2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

January 2020

HAPPY new year 2020

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

DIRTY R-NEWS

Which factors matter most when selecting a radiation training system?

By Steven Pike

Source: https://www.argonelectronics.com/blog/selecting-radiation-training-system

Dec 20 – The first half of the twentieth century represented a period of major advancement in the harnessing of nuclear science and technology, which in turn fueled the urgency to safely utilise, manage and contain these powerful radiological materials.

Different types of radiation possess varying amounts of energy, with gamma rays being by far the most penetrating.

The ability with which personnel are able to accurately localise and detect a gamma radiation hazard is therefore crucial in reducing the risk of harmful health effects caused by exposure.

Portable hand-held radiation survey meters have a wide variety of applications in detecting gamma radiation - from their use in defence, law enforcement and emergency first response to border control, nuclear medicine and non-destructive testing.

Similarly, their simulator detector equivalents can play a considerable role in facilitating the training and education of CBRNe, HazMat and radiation protection personnel.

Creating realistic training experiences

Wherever possible, radiation safety training exercises should be able to recreate the uniquely demanding characteristics of the potential incidents that may be encountered - be it a radionuclide spill, a damaged source containment, a radiological dispersal device or a major reactor release.

Ideally too, these scenarios should include the hands-on use of the instrumentation that will be deployed in a live incident.

What is especially important from a radiation safety training perspective, is that students are afforded the opportunity to experience, and to recognise the significance of key factors such as shielding and inverse square law.

Trainees need to understand the ways in which their readings will change as they approach a source, and which in turn will inform how far they will need to go (and how quickly they will need to move) in order to keep themselves and those around them safe.

Whilst realistic hands-on training is always preferable, integrating the use of actual radiation detection equipment in radiation training exercises is only very rarely a viable option.

Firstly, there is the issue that a real radiation detector is only able to respond to the presence of an actual live source. Lower levels of a live radionuclide may be insufficient to deliver meaningful readings - whilst higher levels of radioactive sources have inherent safety considerations.

Secondly, even in locations where the use of quantities of radionuclides is allowable for training purposes, strict regulatory and administrative controls can make the cost of carrying out such exercises prohibitively expensive.

Thirdly, there is the very real issue of the sheer amount of time that is required to not only prepare and implement these live-source training exercises, but to make an area safe once an exercise has come to an end.

Assessing simulator detector technology

When working with any type of live radioactive source simply isn't practical, the use of simulator radiation detector equipment can provide a compelling and authentic alternative.

In selecting the correct simulator instrumentation however, the quality, fidelity and consistency of the simulation will be vital in ensuring that both trainee and trainer have confidence in the readings that are obtained.

In particular, the technology that underpins the design of a simulator detector will be pivotal.

Some of the common techniques that are used in gamma simulation for example, can lead to fluctuations in the readings obtained - even in situations where the source remains stationary and the environment remains the same.

When using radio waves alone, as has been standard, one of the difficulties to overcome is that there can be fluctuations in the radio wave (due to multipath reflections) which in turn impact on the indication that the student sees in the simulation.

Certain forms of ultrasound simulation enable personnel to monitor the strength of the signal and to calibrate it, so as the ultrasound signal increases it is possible to correlate a simulated radiation reading.

But while this method can work well in open spaces, the manner in which the simulator is implemented can sometimes mean that there is an unwanted directional response.

The human body can also have an impact when using ultrasound simulation methods - for example, when an individual is standing between the simulated source and the simulator detector - which can result in a noticeable reduction in the signal.

There are however new simulator technologies, such as that used in Argon's RadEye simulator, that are able to more realistically simulate the tissue loss that occurs as the result of exposure to a gamma radiation source, which in turn provides a higher quality simulation.

Whatever the environment, it is vital that personnel are trained to use their radiation detector equipment with confidence, that they understand the significance of the readings that they obtain and that they are able to take appropriate responsive action.

Simulator detectors have a vital role to play in cementing this understanding.

But in selecting the best tools for the job it will be important to scrutinise the technology that underpins the instrumentation - and the likely effect that this will have on the fidelity, quality and consistency of the readings obtained.

What are the safety risks when transporting radioactive materials?

By Steven Pike

Source: https://www.argonelectronics.com/blog/radiological-risks-transporting-radioactive-materials

November 2019 – Radioactive materials have a wide variety of applications within the fields of medicine, power generation, manufacturing and the military - and just as with any other product, there are times when these materials may need to be moved from one location to another.

In the US, the Environmental Protection Agency (EPA) estimates that there are around three million shipments of radioactive materials to, from or within the US every year.In the UK meanwhile, Public Health England (PHE) has reported that somewhere in the region of half a million packages containing radioactive materials are transported to, from or within the UK annually.

Regulation of transport of radioactive materials

Ensuring the safety and security of the transport of radioactive material - whether be it by road, rail, air or sea - is understandably a major priority and one that is highly regulated, depending upon the type, and the quantity, of radioactivity that is being transported.

Materials that are deemed to be low in radioactivity may be able to be shipped with no, or very few, controls.

Materials that are considered to be highly radioactive will be subject to controlled routes, segregation, additional security and specialist packaging and labelling measures.

The UK's Office for Nuclear Regulation (ONR) has a primary role to play in advising on the safe and secure transportation of radioactive substances across a wide of sectors - from the movement of decommissioned nuclear reactors or the carriage of irradiated nuclear fuel to the shipping of medical radio-pharmaceuticals, or the transport of sealed radioactive sources used within the construction or oil industries.

What constitutes a radiation transport event?

The normal transport of radioactive materials can result in transport workers (and sometimes even members of the public) being exposed to small radiation doses.

The strict regulatory conditions of transport however are designed to minimise these exposures.

Accidents and incidents can occur for a variety of reasons - from seemingly minor administrative errors, to problems arising from insufficient packaging, mishaps that occur during loading or unloading of consignments or the theft or loss of a radioactive material being carried.

When such events do occur, there is the risk of radiological consequences not just for those transport workers in the immediate vicinity but for emergency responders, HazMat personnel and the wider public.

According to the Radioactive Materials Transport Event Database (RAMTED) there were a total of 16 accidents or incidents involving the transport of radiological materials in the UK in 2012.

These included the receipt of a flask from a nuclear power station where one of the lid-chock locking bolts was found to be loose; the failure of lifting equipment when removing a type 30B uranium hexafluoride cylinder from its protective shipping packaging; and an incident involving the stealing of pipes and plates from a scrap meal facility that were found to have traces of orphan radioactive sources.

Public Health England differentiates radiation transport events into one of the five following categories:

1. **A transport accident (TA)** - which is defined as any event that occurs during the carriage of a consignment of radioactive

material and that prevents either the consignment, or the vehicle itself, from being able to complete its journey.
2. **A transport incident (TI)** - comprising any form of event, other than an accident, that may have occurred prior to or during the carriage of the consignment and that may have resulted in the loss or damage of the consignment or the unforeseen exposure of transport workers or members of the public.
3. **A handling accident (HA)** - encompassing any accident that occurs during the loading, shipping, storing or unloading of a consignment of radioactive material and that results in damage to the consignment.
4. **A handling incident (HI)** - defined as any handling event, other than an accident, that may occur during the loading, shipping, storing or unloading of the radioactive consignment.
5. **Contamination (C)** - defined an an event where radioactive contamination is found on the surface of a package or where the conveyance of a radioactive material is found to be in excess of the regulatory limit.

The role of radiation safety training

When formulating a radiation training strategy, it is vital that personnel are adequately trained to handle the hazards and the risks associated with incidents involving radioactive materials.

Radiation safety training and development programmes should ideally provide personnel with both the knowledge they need and the practical skills that they will rely on in order to carry out their duties safely and effectively.

While most radiation detection equipment is relatively easy to use, the key lies in ensuring that trainees understand the significance of the readings that they get, that they can recognise the implications of changes in units of measurement and that they have the opportunity to train in as life-like a setting as possible.

What Are EMPs and How Are They Used in Warfare?

Source: https://interestingengineering.com/what-are-emps-and-how-are-they-used-in-warfare

Dec 29 – EMPs, or electromagnetic pulses, are intense bursts of electromagnetic energy that can be utilized to damage electronics. Man-made nuclear EMPS are impressive weapons of war that are sparingly used due to their highly destructive nature.

There are natural EMPs that can be caused in small form due to lightning or in large form due to geomagnetic storms. Man-made EMPs are generally created through nuclear explosions.

Essentially, these weapons emit a pulse that damages or destroys the electronic systems in an object due to damaging current and voltage surges.

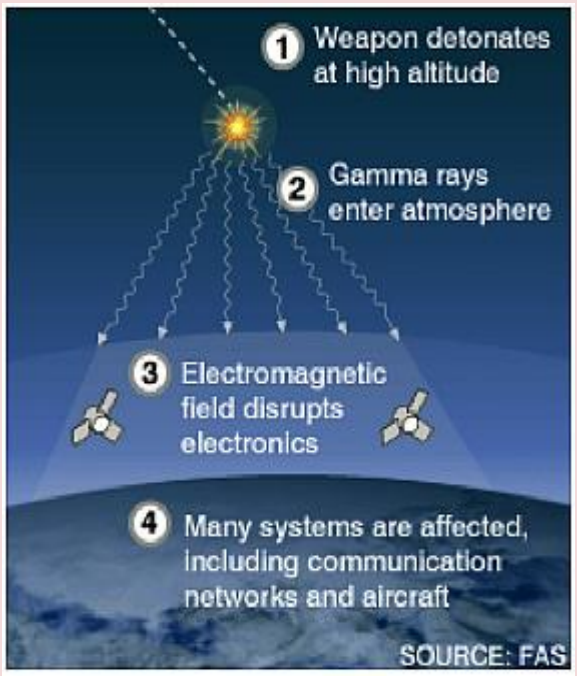
History of man-made EMPs

Man-made EMP capabilities were first discovered as the world's superpowers started nuclear tests. Notably, the Starfish Prime test in 1962, where a **1.4 megaton bomb** was detonated above the Pacific, resulted in damage to electrical equipment more than **1,400 kilometers** away.

During the height of the Cold War, EMPs were investigated as weapons of mass destruction quite extensively by the US and the USSR. During this investigation, multiple low earth orbit satellites failed, which caused both countries to realize just how damaging the weapon they had stumbled upon was.

In warfare, the use of a nuclear EMP weapon is regarded in the same realm as nuclear attacks. They have the potential of destroying an entire region's electronics, which, in the modern information age, would practically be the end of life as we know it.

Aside from nuclear EMPs, military engineers and researchers have been exploring ways to create non-nuclear EMPs essentially since the birth of nuclear EMPs. Non-nuclear EMPs are now a reality for militaries around the world, but these weapons are much more localized than their nuclear counterparts.



Non-nuclear electromagnetic pulses

Focusing in on NNEMPs, these weapons are much less powerful, ranging from hundreds of meters of effectiveness up to several kilometers. These much more targeted ranges and

effects make NNEMPs highly effective non-life-threatening military weapons. In other words, they can do significant damage to a localized region without affecting structures or human life.
The way that NNEMPs are traditionally delivered to a target is rather unique, though. It's not through a vehicle carrying a NNEMP device, but rather there are NNEMP missiles and bombs that are mounted to aircraft and drones. For example, Boeing has built and effectively tested the CHAMP missile.
NNEMP technology is also not a highly complex one, which means that countries of varying sizes, capabilities, and military prowess have the technology in their arsenal. When NNEMPs are implemented in bombs or missiles, they are referred to as e-bombs. Notably, the US used an e-bomb in 2003 in an effort to knock out Saddam Hussein's propaganda network.

Practical military uses of EMP technology
Due to their non-physically destructive nature, NNEMPs can be used against a variety of targets, depending upon their intended effect. Society and military structure are built heavily upon the use of electronics, meaning that the effectiveness of EMPs as weapons are essentially endless.
In war-fighting situations, they could knock out naval ships, disable communications networks, jam tanks, kill radar networks – you name it. If it's electronically based, it can probably be knocked offline by an EMP device.
While all of that may sound a little scary, militaries, and even you have the ability to protect against EMP attacks, though due to the restrictivity of the protection, it's not widely used unless absolutely necessary.
Covering electronics in a faraday caging material keeps the electromagnetic pulses from overloading the circuitry in the systems. Faraday cages are the most effective means of protection for electronics, but unfortunately, they also keep signals from exiting the cage, not just entering. This means that while you could protect a connected device from an EMP attack using a faraday cage, it would only work on network local to the inside of the faraday caging.

The Dirty Bomb Threat That Could Make Your City Uninhabitable — Tomorrow

By Selwyn Duke

Source: https://www.thenewamerican.com/usnews/crime/item/34488-terrorism-the-dirty-bomb-threat-that-could-make-your-city-uninhabitable-tomorrow

Jan 01 – One supposed difficulty terrorists' have effecting dirty-bomb mayhem is obtaining the radioactive material — but it turns out that this may not be so difficult after all.
For that material is as close as your local hospital.
At issue is radioactive cesium-137, which is "commonly found across the United States," reports the *Los Angeles Times*. "Hospitals, blood banks and medical research centers use it in devices called irradiators, which sterilize blood and tissue."

The cesium used is a dry, talc-like substance that remains radioactive for three centuries and could easily be dispersed via dirty bomb detonation. Just four teaspoons of it, experts say, could contaminate 6,400 acres of Manhattan, rendering it uninhabitable for months or even years.

Moreover, a federally commissioned study by the National Academies of Sciences (NAS) warned in 2008 that the "several thousand devices containing high-activity radiation sources" in the United States do present opportunities for terrorists to create dirty bombs. The NAS's experts rated cesium their main concern, in fact. Yet to this day not only has no remedial action been taken — the problem has actually gotten worse.
To be clear, a "dirty bomb" is not a classic nuclear weapon of the kind whose mushroom-cloud detonations we've all seen on TV. The former would not function by way of fission (the splitting of atoms), but would employ conventional explosives such as a fertilizer bomb, TNT, etc. It would, however, contain some radioactive substance that could be dispersed via the detonation. Its danger lies not in the massive heat and shock wave that, let's say, a hydrogen bomb

generates, but in its capacity to contaminate a wide area.
The cesium in question would be an ideal substance for this purpose, too, "because its fine particles disperse easily and can migrate through air ducts and bind tightly to porous surfaces, including concrete," the *Times* also informs.
The upshot? A "dirty bomb packed with cesium would not kill large numbers of people," the paper points out. "Instead, it would be a weapon of 'mass disruption' — leaving areas uninhabitable for months or even decades and increasing long-term cancer risks for people who come in contact with it, atomic experts say."
Illustrating this point, WND writes "that last May, a small amount of cesium was spilled in a [Seattle] research facility.... Months later, 'much of the building remains unusable,' the [*Times*] report said."
An even greater object lesson could be taken from a 1987 incident in Goiania, Brazil, when two men entered an abandoned site of a clinic that had utilized cesium and took metal equipment in the hopes of selling it as scrap.
"That evening, both men began to vomit," related the *Times*. "It wasn't until two weeks later — after the equipment and the strangely glowing material inside it had changed hands through two scrap yards and become a source of fascination for adults and children — that a local physicist persuaded authorities to take action."
"A monitoring station set up in a local stadium **screened more than 112,000 people** for possible cesium contamination. Forty-nine houses were demolished or decontaminated and about **4,500 tons of soil** were hauled away, according to the International Atomic Energy Agency," the paper continued.
"In the end, four people died and hundreds had to be decontaminated."
So, since an ounce of prevention is worth more than a pound of cure in this case, what should be done? The *Times* tells us that the NAS "panel's warning in 2008 came with blunt recommendations: The government should stop licensing new cesium-based blood irradiators, and existing ones should be withdrawn from use. Safer devices that use X-ray technology worked just as well; the panel found." And, in fact, several developed countries have already "converted away from cesium," the paper further informs.
Yet despite this and while the Nuclear Regulatory Commission (NRC) has the power to take remedial action, it declined to do so after protests from hospitals. Moreover, the NRC has played down the risk, claiming the system has "no significant gaps."
The "Department of Energy [DOE], however, is actively trying to eliminate the threat, replacing so far 108 of the [cesium] devices with substitutes," relates WND. As the DOE put it in an April report to Congress, "Every irradiator that is replaced represents one fewer opportunity for a terrorist."
And, predictably, terrorists have already expressed interest in obtaining cesium. An example is Anders Breivik, who'd registered such a desire before killing 77 Norwegians via conventional means in 2011.
As to this danger, no one has to convince Washington State health physicist Mark Henry, who helped manage the aforementioned Seattle cesium contamination. "If you think that somebody couldn't get ahold of material like this and make a weapon of mass disruption," he warns, "then I think you need to review that again." Note that the consequence of the quite small cesium release in Seattle is, he said, a "dead building."
Yet speaking volumes is that the media and politicians aren't too interested in this story. Since unlike gun control, cesium control cuts across partisan lines, it's just not as appealing as disarming law-abiding patriots in Virginia.

***Selwyn Duke** has written for* The New American *for more than a decade. He has also written for The Hill, Observer,* The American Conservative, *WorldNetDaily, American Thinker, and many other print and online publications. In addition, he has contributed to college textbooks published by Gale-Cengage Learning, has appeared on television, and is a frequent guest on radio.*

Could Planet Earth Survive A World War 3 That Worsens the Climate Crisis?

Source: https://in.mashable.com/science/10057/could-planet-earth-survive-a-world-war-3-that-worsens-the-climate-crisis

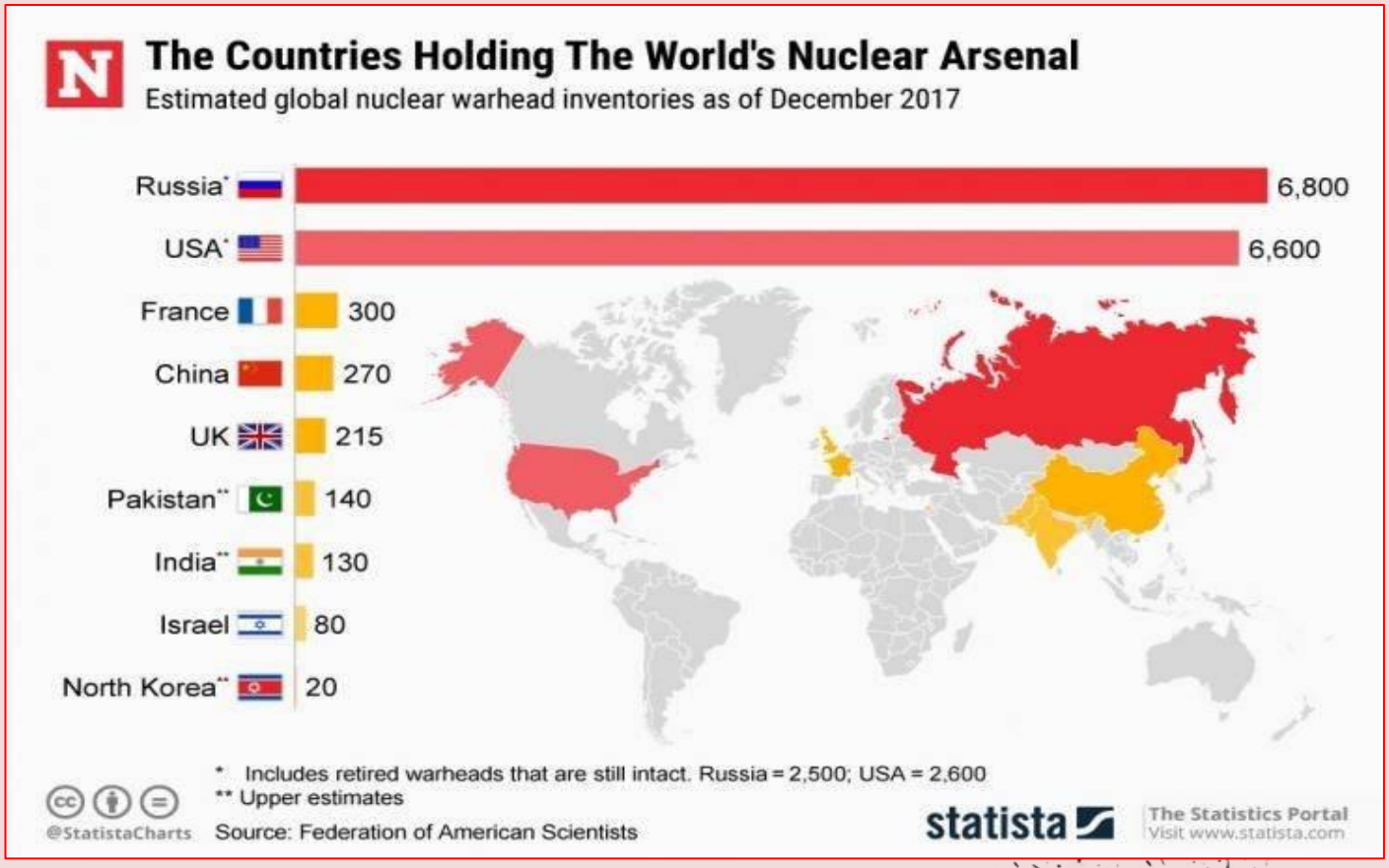
Jan 03 – A famous quote from Albert Einstein says, *"I do not know with what weapons World War III will be fought, but World War IV will be fought with sticks and stones,"* dating back to the 1940s when the first nuclear weapons were being developed. Although the famed physicist didn't actually develop the atomic bomb, he was well aware of how nuclear weapons could affect the world.
The President of the United States, Donald Trump's vow to hit Iran and make it 'pay a very big price' comes after the fiasco of the attack on 6,000 demonstrators at the U.S. embassy in Baghdad, Iraq. In an equally brutal retaliation, Trump ordered an airstrike that killed top Iranian general Qassim Suleimani in Baghdad. If not anything, the counter-strike is an unveiled threat to unleash America's most potent weapons of mass destruction onto the Middle Eastern country and has erupted scares of World War III across the globe.
Considering how close Iran is to developing its own weapon of mass destruction, it won't even take an educated guess to predict that the next World War, if it does happen between

these two countries, will be fought with nuclear weapons. Reportedly, most U.S. weapons are 10 to 50 times stronger than the bombs that brought Hiroshima to a standstill. So, you can just imagine how such a strategic nuclear war would impact the Earth, posing an existential threat to humanity regardless of the scale of its severity.

Take, for example, a relatively new research that models the indirect effects of nuclear detonations on the environment and climate in case of a limited regional nuclear war between India and Pakistan. The combines arsenals of both the nations equal to more than 220 nuclear warheads. Such an event will cause fires to ignite over a large area which would inject large volumes of soot and debris into the stratosphere. This would thus block out the sun and cause a significant drop in average surface temperature and precipitation across the globe, with effects that could last for more than a decade.

According to this particularly convincing report, a bomb can now be manufactured which will be 2,500 times as powerful as the one that destroyed Hiroshima. Such a bomb, if exploded near the ground or under water, could send radioactive particles into the upper air. They would sink gradually and reach the surface of the earth in the form of deadly dust or rain. It was this dust which infected the Japanese fishermen and their catch of fish. No one knows how widely such lethal radioactive particles might be diffused, but the best authorities are unanimous in saying that a war with H-bombs might possibly put an end to the human race.

The culture of war mongering that's especially endorsed by major world leaders like Trump off late is scary. One just cannot overlook their attitude on the idea of a nuclear war as a dramatic rhetoric of global humanitarian disaster because this a more plausible scenario now than ever, given the time we stand in. Nuclear war is also a war on the environment and its indirect repercussions are to be borne by the generations to come and also the geological space around us. It's about time authorities realize the gravity of the situation and put our planet before any international conflict.



A graphic provided by Statista shows the estimated stockpiles of the nine known nuclear weapons powers as estimated by the Federation of American Scientists.

Iran Does Not Have Nuclear Weapons, But Here's Why Its Program Is at the Heart of the Crisis

Source: https://www.newsweek.com/why-iran-does-not-have-nuclear-weapons-1480355

Jan 03 – Iran is not believed to possess nuclear weapons and officially has never sought them—although its top foes the United States, Israel and Saudi Arabia are among those who argue that the Islamic Republic has always secretly wanted such a weapon of mass destruction. This dispute has been at the heart of a worsening Middle East crisis that flared up with the Pentagon's killing of a top Iranian military leader.

A picture taken on November 10, 2019, shows an Iranian flag at Iran's Bushehr nuclear power plant, during an official ceremony to kick-start works on a second reactor at the facility. Bushehr is Iran's only nuclear power station. It is currently running on imported fuel from Russia and is closely monitored by the UN's International Atomic Energy Agency. ATTA KENARE/AFP/Getty Images

The assassination of Revolutionary Guard Quds Force commander Major General Qassem Soleimani along with top Iraqi militia figures Thursday in Baghdad came amid a series of deadly, tit-for-tat escalations that has worsened since President Donald Trump pulled out of a 2015 nuclear deal in May 2018. The accord granted Tehran billions of dollars in sanctions relief in exchange for severely restricting its nuclear activities. The agreement has since begun to unravel, with European powers struggling to normalize trade ties under threat of U.S. sanctions and Iran reducing its own commitments in response.

While Soleimani's death may be the most dramatic salvo in the U.S. and Iran's feud in some time, it was not at all the first blood shed throughout the two nations' complex, tortured history.

Officially, nuclear weapons have been banned by Iran because Supreme Leader Ayatollah Ali Khamenei has deemed them to be forbidden under Islam; since 2003, the U.S. accused of Iran of seeking to develop them. That same year, Khamenei issued a fatwa—an Islamic legal opinion—allegedly dating back to beliefs he expressed for nearly a decade, opposing the manufacturing of weapons of mass destruction.

While Iran's nuclear activities continued, officials consistently argued—and have to this day—that the work was purely for energy purposes.

The idea of weapons of mass destruction being un-Islamic has repeatedly surfaced in the Islamic Republic over the years, with Khamenei saying as recently as June that "religious verdicts prohibit building nuclear weapons." Iran also publicly opposes chemical and biological weapons, owing to Iraq's use of mustard gas and nerve agents during their 1980s war in which Washington backed Baghdad and at times bombed both Iranian troops and civilians.

Still, the United Nations Security Council remained unconvinced as Iran refused to stop enriching uranium, and began targeting Tehran with sanctions in 2006. That same year, James Risen published his book *State of War* that included the account of CIA operative Jeffrey Sterling, who detailed a secret operation to sabotage Iran's nuclear program. The operation was described as "hopelessly botched, and possibly backfiring by giving the Iranians blueprints that could be useful to them if they sorted out the good information from the errors."

As international restrictions against Tehran tightened in 2010, a computer virus known as Stuxnet was uncovered that crippled Iran's centrifuges. Also that year, a series of targeted attacks began that killed four Iranian nuclear scientists and wounded another.

Iran blamed both Israel—which itself is widely believed to possess nuclear weapons—and the U.S. for the operations. Israel has neither confirmed nor denied its involvement in either, but has been widely attributed both with the U.S. assisting in the latter.

The finalization of the Iran nuclear deal—officially known as the Joint Comprehensive Plan of Action—in 2015 was largely hailed as a diplomatic landmark by the international community. Though opposed by hardliners in both Washington and Tehran, the agreement officially held Iran's nuclear program under the scrutiny of International Atomic Energy Agency monitoring and opened up the country's economy.

Trump, who came to office in early 2017, felt it did no go far enough, however, in curbing what he believed to be Iran's nuclear weapons ambitions, as well as its support for militant groups abroad and its ongoing missile development. He has since applied a "maximum

pressure" strategy in hopes of reining in the Islamic Republic, though the security situation across the Middle East has deteriorated significantly.
For one year, the International Atomic Energy Agency reported that Iran abided by the deal, even without any U.S. or full European commitment. On the first anniversary of the U.S. exit from the nuclear deal last May—and just days after the White House announced the deployment of additional troops to the Persian Gulf region—Iran, however, officially began stepping away and has continued to do so.
Fellow signatories China, the European Union, France, Germany, Russia and the United Kingdom all continue to support the accord. But all parties have raised their doubts as to its success should tensions continue to worsen.

France: Iran Could Have Nuclear Weapon within One to Two Years

Source: http://www.homelandsecuritynewswire.com/dr20200110-france-iran-could-have-nuclear-weapon-within-one-to-two-years

Jan 10 – **French Foreign Minister Jean-Yves Le Drian has warned that Iran could have nuclear weapons in one or two years if Tehran continues to violate a landmark nuclear accord with world powers.**
The country's top diplomat made the statement ahead of a 10 January emergency meeting of European Union foreign ministers, which comes amid mounting tensions between Iran and the United States following the killing of top Iranian commander Qasem Soleimani in an air strike in Baghdad last week and a subsequent Iranian missile attack on U.S.-led forces in Iraq.
Under the Joint Comprehensive Plan of Action (JCPOA), Tehran pledged to curb its nuclear ambitions in exchange for international sanctions relief. The agreement between Iran and the United States, Britain, France, Germany, Russia, and China as well as the European Union was signed in October 2015 in Vienna.
However, Tehran has taken what it has described as "steps toward" abrogating the JCPOA since President Donald Trump announced in 2018 that the United States was withdrawing from it and reimposing tough sanctions on Iran.
"If they continue with unraveling the Vienna agreement, then yes, within a fairly short period of time, between one and two years, they could have access to a nuclear weapon, which is not an option," Le Drian said on German radio station RTL on 10 January.
Iran insists its nuclear program is for civilian purposes only, and the JCPOA allows the country to run reactors to generate power.
Trump said the agreement was insufficient and should be renegotiated because it didn't address Iran's ballistic missile program or its involvement in regional conflicts.
Meanwhile, the reimposition of sanctions has taken a toll on Iran's economy, and sent its currency into a downward spiral.
The EU has said it will "spare no effort" to keep the nuclear deal alive, despite the escalating tensions between Washington and Tehran.
Before the 2015 agreement, some experts estimated that Iran was within five to six months of being able to produce a nuclear bomb, while others said that could happen within two to three months.
With the JCPOA safeguards in place, the break-out time was estimated to be more than a year.
But after the U.S. withdrawal from the deal, Iran has breached its main limitations, exceeding the stockpiles of heavy water and uranium allowed, the number and types of centrifuges it can operate to enrich uranium, and the purity of uranium.
The agreement caps uranium enrichment at 3.67 percent, a level that can fuel a commercial nuclear power plant. Weapons-grade uranium enrichment must reach 90 percent.
However, scientists say that, once the capacity to enrich uranium has reached around 20 percent, the time needed to reach 90 percent is halved. Prior to the agreement, Iran enriched uranium to 20 percent.
After the U.S. withdrawal from the agreement, Iran last year boosted its enrichment purity to 4.5 percent.
Following Soleimani's assassination by the United States, Tehran announced what it said was its fifth and final step in violating the JCPOA and said it no longer will abide by any limitation to its enrichment activities.

A guide to radiation safety training terminology for first responders

By Steven Pike
Source: https://www.argonelectronics.com/blog/radiation-safety-training-terminology-first-responders

Jan 14 – All emergency situations present some element of risk for first responders - however an incident can be further complicated by the presence of ionising radiation.
In some scenarios, having familiarity with the different locations where radioactivity is used can provide responders with some forewarning of the hazard that they are about to encounter - for example, in the case of a vehicular accident involving the transportation of a radiological source, or an incident that takes place within a hospital's nuclear pharmacy.

In other situations though, the radiological hazard may not be suspected, expected or immediately apparent.
Radiation safety has formed part of emergency responder training for several decades - encompassing a broad range of topics from awareness, detection and recognition of radiological hazards to technical knowledge, time-distance-shielding, and environmental safety.
The impact of radiological events can be significantly reduced through a combination of comprehensive emergency planning, the conducting of structured radiation safety training programmes and the allocation of appropriate radiological surveying equipment.
From a practical perspective, the instrumentation used in radiological surveying is itself fairly simple to use. It is also important however to ensure that essential hands-on skills are supported by an understanding of the basic principles that underpin the subject of radiation.
In this blog post, we've pulled together some of the key terms that are specifically relevant to the understanding of radiation dose.

Dose

- When measuring ionising radiation, there are two units that need to be classified: the radioactivity of the source (measured in becquerel or curie) and the dose of ionising energy that is absorbed by a person (expressed in sieverts/grays or Rem/Rad). As radiation moves through the body it dislodges electrons from atoms and disrupts molecules, gradually losing energy until it escapes from the body or disappears. How many molecules are disrupted depends on the energy deposited - or the dose.

Dose Limits

- Dose limits protect radiation workers, first responders and members of the public by balancing the risk of exposure with the benefits of using, or coming in to contact, with ionising radiation.

Dose monitoring

- The process of recording and assessing the potential radiation exposures that a person may receive - whether due to occupational exposure or an accidental release.

Cumulative dose

- A measurement of the total energy (or absorbed dose) that is deposited (accumulated) in the body as the result of prolonged, continuous or repeated exposure to ionising radiation.

Dose rate

- The radiation dose delivered per unit of time, usually per hour.

Dose equivalent

- The quantity that combines amount of radiation absorbed with the impact, or medical effect, of that particular type of radiation on human tissue. The dose equivalent is calculated by multiplying the absorbed dose by the quality factor (the difference in effect of different types of ionising radiation.) In the case of gamma and beta radiation the dose equivalent is equal to the absorbed dose, whereas for alpha and neutron radiation the dose equivalent is larger than the absorbed dose.

Effective dose

- A calculated quantity, measured in mSv / mRem that takes into account the absorbed dose to all organs of the body, the relative harm level of the radiation and the sensitivities of specific organs to different types of radiation.

Collective dose

- A calculation of the potential health effects of an area, a region or a large number of people exposed to a source of ionising radiation - expressed as "person-rem" or "person-sieverts".

External dose

The dose received by a person standing near or in the vicinity of a gamma or high-energy beta-emitting source. External exposure will stop once a person moves away from the location of the source.

Internal dose

A dose received through the ingestion or inhalation of a radioactive material. The effects of internal exposure will continue until the material either decays or is flushed from the body.

Dose coefficient

The factor that is used to convert radionuclide intake to dose (for example sieverts per becquerel).
For anyone who is tasked with responding to an incident involving a radiological source, the confidence and accuracy with which they are able to locate, measure and monitor levels of ionising radiation is key.
Given the comparative rarity of major radiological incidents, it is perhaps not surprising that there can sometimes be gaps in knowledge when it comes to the fundamentals of radiation terminology.

Providing first responders with a solid theoretical framework, in combination with regular opportunity for practical hands-on training, will ensure they are confident in handling the operational challenges presented by ionising radiation incidents.

The Costs of Closing Germany's Nuclear Power Plants

Source: http://www.homelandsecuritynewswire.com/dr20200114-the-costs-of-closing-germany-s-nuclear-power-plants

Jan 14 – Many countries have phased out production of nuclear energy because of concerns related to nuclear waste and the risk of nuclear accidents. A new study explored the impact of the shutdown of roughly half of the nuclear power plants in Germany after the 2011 Fukushima accident in Japan. The study found that the resulting reductions in nuclear power were replaced primarily by production from coal-fired sources and reductions in net electricity exports. The authors show that the switch to fossil fuel-fired power resulted in considerable increases in pollution at an estimated annual social cost of about $12 billion.

The study was conducted by researchers at Carnegie Mellon University; the University of California, Berkeley; the University of California, Santa Barbara, and the National Bureau of Economic Research (NBER). It was published as an NBER working paper.

"Although numerous reports have recommended that nuclear power be part of the global solution to climate change because it produces minimal carbon emissions, many countries have slashed their share of energy production from nuclear sources, primarily due to safety concerns," explains Akshaya Jha, assistant professor of economics and public policy at Carnegie Mellon University's Heinz College, who contributed to the study. "One might conclude from this that the expected costs of nuclear power exceed its benefits. But few studies have quantified the full range of economic and environmental impacts of phasing out nuclear production."

In their study, researchers sought to document the short- to medium-term impact of the phase-out of nuclear power in Germany on multiple market and environmental outcomes. In particular, the study focused on the shutdown of 10 of the 17 nuclear reactors in Germany between 2011 and 2017, following the Fukushima accident. Germany plans to shut down all of its remaining nuclear reactors by 2022. Researchers examined hourly data on power plant operations, including electricity demand, local weather conditions, and energy and fuel prices. They also developed a machine learning framework that predicted the quantity of electricity produced by each power plant in Germany under two scenarios—one with the nuclear phase-out and one without it.

CMU notes that the study found that nuclear energy production due to the phase-out of the nuclear plants was replaced primarily by coal-fired production and by imports of electricity from surrounding countries. The move from nuclear power to fossil fuel-fired power resulted in substantial increases in emissions of global and local air pollution. In addition, electricity prices rose due to the phaseout of nuclear plants, so electricity producers benefitted but German consumers had to pay more, the study found.

Researchers estimated the social cost of the phase-out in the initial years at approximately $12 billion per year, with more than 70 percent of the cost coming from the increased risk of mortality (an estimated 1,100 excess deaths annually) associated with exposure to air pollution emitted by burning fossil fuels.

Closing nuclear plants had benefits: reducing the risk of nuclear accidents and decreasing the costs associated with storing nuclear waste. But even the largest estimates of the benefits of the nuclear phaseout were likely far smaller than $12 billion a year.

"It's clear that German citizens care deeply about climate change yet are distinctly anti-nuclear," says Stephen Jarvis, a PhD candidate at the University of California, Berkeley, the study's lead author. "Concerns about air pollution have tended to receive less attention in this debate, perhaps because the risks associated with nuclear power are much more prominent than the costs of air pollution associated with fossil-fuel-fired production."

Among the limitations of the study noted by the authors are that plant-level data on electricity production were unavailable prior to 2015, and economic factors that changed during the course of the study may have affected findings in ways independent of those studied.

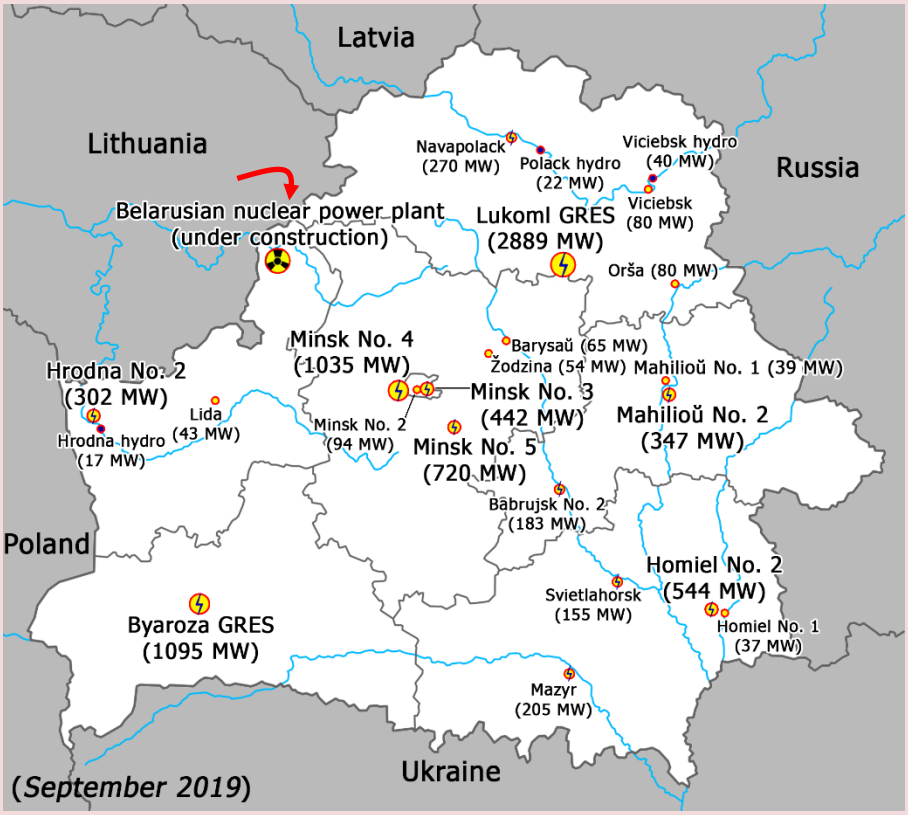
"Policymakers around the world face a difficult tradeoff," says Olivier Deschenes, professor of economics at the University of California, Santa Barbara, who also contributed to the study. "As countries shift away from nuclear production, despite the substantial increases in operating costs and air pollution costs that could be associated with this policy, it is essential for policymakers and academics to convey the relative costs of climate change and air pollution versus nuclear accident risk and waste disposal to the voting public."

Lithuania: New Belarusian Nuclear Plant Hasn't "Learned Lessons of Chernobyl"

By Matthew Luxmoore

Source: http://www.homelandsecuritynewswire.com/dr20200114-lithuania-new-belarusian-nuclear-plant-hasnt-learned-lessons-of-chernobyl

Jan 14 – Belarus is launching its first nuclear reactor without completing all stages of a "stress test" — an EU risk-and-safety assessment of a plant's ability to withstand damage from hazards. Because of its location downwind from Chernobyl, Belarus bore the brunt of that fallout. Its own plans for a nuclear power plant, announced in the 1980s, were shelved as the Soviet leadership and society at large grappled with the consequences of the tragedy. Now, critics say Belarus's decision to forge ahead with the plant near Astravets is a testament to the country's failure to draw conclusions from its past.



Mikalay Ulasevich was running in municipal elections in July 2016 when a local resident alerted him to a major accident at a nuclear power plant under construction close to this town in northwestern Belarus.

Workers had dropped a 330-ton reactor vessel from a height of several meters while attempting to install it, he was told, and officials were trying to keep the incident under wraps.

"Everybody knew about it, or almost everybody, but no one dared reveal it publicly," Ulasevich recalled recently at his house in the nearby village of Varnyany, with the plant's gargantuan cooling towers visible on the horizon. "They'd be putting themselves in the firing line."

As a member of the opposition United Civic Party and an outspoken critic of authoritarian President Alyaksandr Lukashenka, Ulasevich was campaigning on a promise to thwart the controversial project funded by a subsidiary of Russian state nuclear energy monopoly Rosatom.
But it wasn't until two weeks after he learned of the incident that he decided to share the news. In a Facebook post questioning the project's safety record, he asked whether Belarusian officials had notified the International Atomic Energy Agency (IAEA) of the accident or told neighboring Lithuania, whose capital, Vilnius, lies a mere 40 kilometers from the Astravets plant.
It's likely the small Baltic country was already aware. Since the project was announced by presidential decree in 2008, backed by a $10 billion loan from Moscow, Lithuanian officials have waited with trepidation for Minsk to declare construction complete. Now, with its delayed launch slated to take place within months, their campaign to scupper those plans has shifted into high gear.
"This is a threat to our national security, public health, and environment," Lithuanian Energy Minister Zygimantas Vaiciunas told RFE/RL in an interview in Vilnius. "The key question is the site selection, which was done politically — geopolitically."

Lessons Learned?

Eastern Europe knows that nuclear power can be both a blessing and a curse. The April 1986 explosion of Reactor No. 4 at the Chernobyl plant, just south of Belarus in Ukraine, reverberated with catastrophic consequences as tainted clouds spread deadly radioactive particles across the region. The Soviet leadership restricted information about the accident and acted sluggishly, holding off evacuation of the local population for 36 hours. Another nuclear disaster at Fukushima, Japan, in 2011, the deadliest since Chernobyl, exacerbated global fears over the double-edged sword of atomic energy.
Because of its location downwind from Chernobyl, Belarus bore the brunt of that fallout. Its own plans for a nuclear power plant, announced in the 1980s, were shelved as the Soviet leadership and society at large grappled with the consequences of the tragedy. Now, critics say Belarus's decision to forge ahead with the plant near Astravets is a testament to the country's failure to draw conclusions from its past.
"The lessons that were given 30 years ago in Chernobyl have not been learned," Vaiciunas said.
Three years before the disaster in Ukraine, the Soviet Union opened a nuclear plant in Lithuania, near the Belarusian border, with the same RBMK-type reactors that served Chernobyl. It was there that parts of HBO's five-part series on the nuclear disaster were filmed. Lithuania agreed to close it as a condition for its accession to the European Union in 2004, with the final reactor decommissioned in December 2009.
But in the past decade, nuclear-reactor design has advanced markedly, with an increased focus on accident prevention and a substantial improvement in safety records worldwide. And the Belarusian Nuclear Power Plant, as the project is officially known, is no copy of Chernobyl or Fukushima.
The site near Astravets will run third-generation pressurized-water reactors distinct from earlier models used in Japan and Ukraine and equipped with safety measures aimed at precluding the kind of accidents that happened there: from so-called passive safety systems capable of triggering an automatic shutdown to a "core catcher" device installed in a concrete pit beneath the reactor that would trap molten fuel in case of overheating and make it nearly impossible for radiation to infiltrate the environment.
The same Russian-made VVER-type reactors that will be used near Astravets are slated for installation in a range of other countries including Finland, where Rosatom — which has emerged as the world's leading nuclear reactor supplier — is building another power plant amid a global push to install more than 30 of its reactors in deals worth over $100 billion.

Geopolitics in Play?

But while the Finnish regulator has imposed strict safety criteria pending approval of the project, Lithuania says, Belarus is launching its first reactor without completing all stages of a "stress test" — an EU risk-and-safety assessment of a plant's ability to withstand damage from hazards.
But supporters of the project say that since Belarus is not an EU member, it is not obliged to complete the stress test, and the checks it did carry out were done voluntarily. The Astravets plant has also hosted visits from experts at international bodies, including the IAEA.
Although it's up in arms over what it says is Minsk's secrecy over the project, Lithuania doesn't so much dispute the technology used. It's the proximity to its population centers, and a history of seismic activity in the area, that rankles officials in Vilnius. In a 2017 resolution, the Council of Europe called on Belarus to suspend construction of the power station, citing a "lack of respect for international standards for nuclear safety" and "major incidents during the construction of this plant," which it asserted was being built on "an unsustainable site."
"Safety depends not only on the design — it depends also on the site," said Darius Lukauskas, deputy head for radiation safety at Lithuania's nuclear energy regulator. "You have to answer three questions: where the plant is, what kind of facility it is, and how it is constructed."

The plant lies 140 kilometers from Minsk on Belarus's border with the European Union, and Vilnius suspects its location is part of a Kremlin push to retain a foothold on the European energy market and ensure the region's continued reliance on Russian hydrocarbon supplies. As Russia accelerates its push for closer integration with Belarus on Moscow's terms, neighbors also fear that Minsk will be beholden to Russia's geopolitical whims once the plant goes online.

The administration of the Astravets power plant denies that. "Any talk of Belarus building a nuclear plant here to spite or harm someone — be it Lithuania, the EU, or anyone else — is wrong, and has always been," said Eduard Svirid, a spokesman for the nuclear plant. He said the site near the Lithuanian border was chosen after preliminary excavations at several locations in the country's east exposed a layer of chalkstone that rendered the ground unsafe for a power plant, and said past seismic activity in the region is exaggerated.

On a recent afternoon, Svirid showed an RFE/RL reporter around the project's visitor center in Astravets, some 15 kilometers from the plant itself, where he uses touchscreens and model reactors to outline the precautions the administration promises to have in place. He said the plant organizes four or five press tours of the site each year and was "unprecedentedly open toward the media and the general public."

In e-mailed comments to RFE/RL, Rosatom said that "it is practically impossible to conceal any event on the site, as key works are being regularly inspected by watchdogs."

"We are committed to the highest standards of transparency and have always provided the national regulator, international watchdogs, and all other stakeholders with any and all information they require on the design and progress of the project," it said.

"A Bone in the Throat"

But access to the plant itself and the surrounding area are strictly controlled, with a dedicated security detail stopping people who take photos and occasionally detaining journalists. Two Belarusian journalists said they were followed by plainclothes officers and taken to a police station for questioning when they tried to visit the site in 2013 along with Ulasevich and other opposition politicians. During a recent visit, an RFE/RL reporter was detained by the plant's security service, whose officers demanded that he delete all photos of the plant. Svirid defended the actions, warning that photos can be used by terrorists.

Lukashenka, meanwhile, has vehemently defended the project and smeared its opponents. In a speech before university students in the provincial capital, Hrodna, in 2013, the strongman president suggested that critics of the plant were "a fifth column" that had been "paid off." He called the Astravets plant and one under construction in the Russian exclave of Kaliningrad "a bone in the throat of the European Union and the Baltic states," adding, "They'll be forced to buy electricity from us and from Russia."

Lithuania has sought to upend those plans. In April 2017, it announced a boycott on the import and transfer of electricity from Belarus, in an apparent bid to dim the Astravets plant's economic prospects. But Lithuania's electricity grid links up with Belarus and Russia, and while it plans to reorient to the EU's network, it acknowledges that process will take several more years.

In the meantime, its government is already preparing for a potential disaster. It has bought up 900,000 euros ($1 million) worth of iodine tablets in the event of a radiation leak, which Vilnius says could affect a third of Lithuania's population of 2.8 million. And it's holding drills across the country to test its readiness and ability to evacuate citizens should the unthinkable happen.

"It depends on the speed of the wind, [but] we could have only a couple of hours after a release to make decisions — for example, to evacuate," said Lukauskas of the nuclear-safety regulator, one of the many state institutions involved in the drills. "And until the release reaches the Lithuanian border."

A Suspicious Secrecy

Back across the border, official opinion polls suggest that Belarusians are divided over the benefits of harnessing nuclear power in their country and over the construction of the Astravets plant. According to a December 2018 poll by the state Sociology Institute, support for the plant was at its highest in the Astravets district itself, with more than 71 percent in favor — though the accuracy of such surveys is hard to gauge in the tightly controlled country.

A continuing influx of workers from Russia and other parts of Belarus is expected to almost double the town's population within the next five years, to over 22,000, with new housing blocks springing up on the outskirts. An active outreach campaign by authorities in Astravets since 2008 has also helped sway local opinion in favor.

But for Ulasevich, a geologist by training and one of the project's few outspoken critics in Belarus, it is the apparent secrecy around it that is most jarring. When the reactor vessel was dropped in July 2016, it wasn't until after his Facebook post that Belarusian officials confirmed publicly that the accident had taken place and pledged to replace the damaged vessel. (Svirid contended that the reactor shell was not dropped, but rather titled during transportation in a way that caused one end to hit the ground.)

On a recent drive from his house in Varnyany to the nuclear plant, Ulasevich pointed out military installations that have emerged near Belarus's western border in recent years, part of what Lithuania suspects is a build-up aimed in part at protecting the strategic facility but

also a symbol of growing tensions between the EU and Russia, which has close military ties with Belarus and leads a security alliance that includes its smaller western neighbor. Despite warming relations between Brussels and Belarus, which Lukashenka has sought to balance between Moscow and the West, the country's ties to Russia remain strong.

"This is a military-political project, not an economic one," Ulasevich said of the nuclear plant. "These tracking stations and army bases have been sprouting up like mushrooms after a summer rain."

In Vilnius, officials acknowledge they have no way of preventing the plant's launch, or strong-arming Belarus into making concessions over its sovereign territory. But Vaiciunas hopes that the country's continued vocal opposition will encourage countries and companies to boycott the project, just as it has done.

When the Chernobyl catastrophe struck, he said, "the key problem was not the accident itself, but the fact nobody was talking about it."

"That's the fear for us," he said. "You can't trust a country which is not communicating with you."

***Matthew Luxmoore** is a Moscow-based correspondent for RFE/RL.*

Securing Radiological Sources on the Go

Source: http://www.homelandsecuritynewswire.com/dr20200121-securing-radiological-sources-on-the-go

Jan 21 – Radioactive materials are a critical tool in a number of industrial applications, particularly oil and gas drilling and welding. While these sources are safe and well-regulated for their intended use; if lost or stolen the materials could be used by terrorists to make dirty bombs. The Department of Energy's Pacific Northwest National Laboratory developed and licensed a technology system to keep track of and secure radiological material on the road or at jobsites. Golden Security Services of Miami, Florida, will produce and deploy the Mobile Source Transit Security, or MSTS, system starting at several sites in Latin America.

Industrial radiographer

"The system is a first line of defense against radiological terrorism and provides situational awareness if the material is tampered with or moved from where it is supposed to be," said PNNL MSTS project manager Brian Higgins.

According to the Nuclear Regulatory Commission, most radiological dispersal devices would not release enough radiation to kill people or cause severe illness. But they certainly could create fear and panic, contaminate property and require potentially costly cleanup. The National Nuclear Security Administration sponsored PNNL to develop the MSTS system to help protect such material from theft, loss, or tampering.

PNNL notes that radiological sources are commonly used in the oil and gas industries. These sources help determine and log geological features of an oil well, such as porosity or proximity to oil. Other devices with radiological material are commonly used for industrial radiography, where devices are used to inspect welds on jobsites. PNNL used its extensive radiological and radio frequency expertise to develop the MSTS system, which consists of detection devices and radiofrequency tags specifically designed to track the devices that house this radiological material.

"Technology transfer to industry is an important mission of the Laboratory, especially in the area of nuclear security where the consequences can be severe," said Kannan Krishnaswami, who manages commercialization of national security technologies for PNNL. "Partnering with industry allows for such security solutions to be commercially deployed, allowing PNNL to refocus its efforts on the next generation of scientific and technical challenges."

United States nuclear forces, 2020

By Hans M. Kristensen and Matt Korda

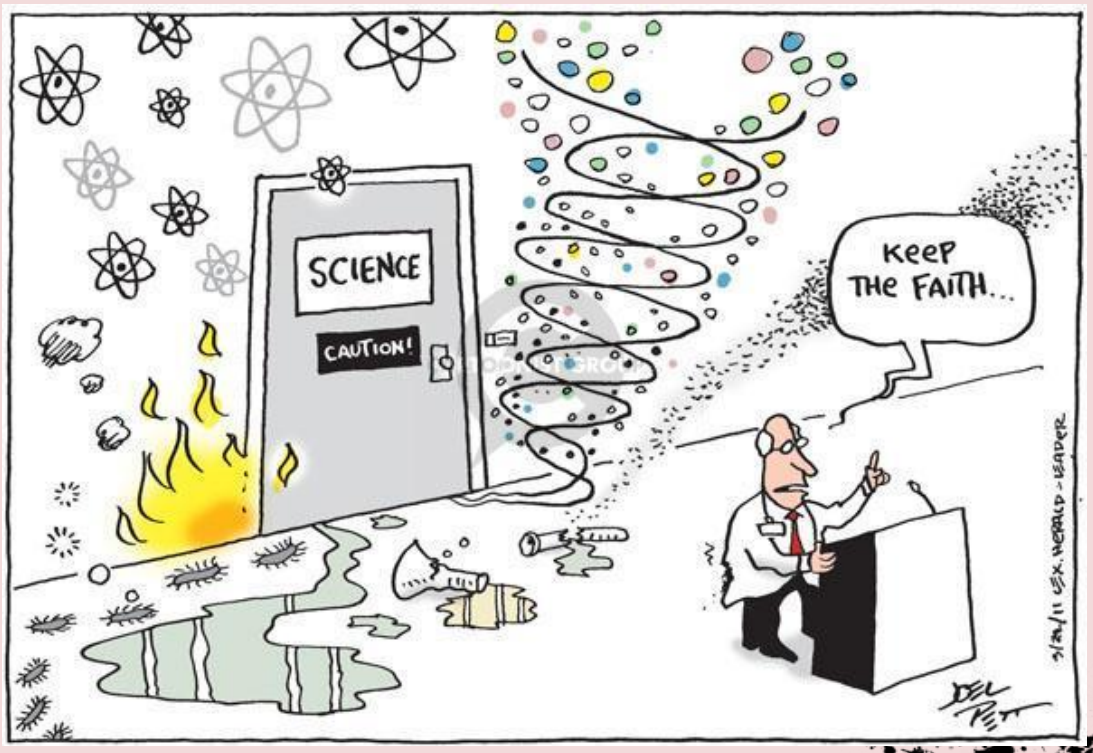
Source: https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1701286

Jan 21 – The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Matt Korda, a research associate with the project. The Nuclear Notebook column has been published in the *Bulletin of the Atomic Scientists* since 1987. This issue examines the status of the US nuclear arsenal. The US nuclear arsenal remained roughly unchanged in the last year, with the Defense Department maintaining an estimated stockpile of approximately 3,800 warheads. Of these, only 1,750 warheads are deployed, while approximately 2,050 are held in reserve. Additionally, approximately 2,000 retired warheads are awaiting dismantlement, giving a total inventory of approximately 5,800 nuclear warheads. Of the approximately 1,750 warheads that are deployed, 400 are on land-based intercontinental ballistic missiles, roughly 900 are on submarine-launched ballistic missiles, 300 are at bomber bases in the United States, and 150 tactical bombs are at European bases.

▶▶ Display Table

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

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



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

EXPLOSIVE NEWS

Intercepting Explosive Drones – World First Technological Solution Developed by Israel Police

Source: https://i-hls.com/archives/97552

Dec 26 – A world-first technological solution was developed in response to the threat of explosive drones and incendiary balloons and kites, frequently launched from Gaza into Israel territory. The laser-based **Lahav Or system** was developed by MAFAT – Israel Police Department for the Development of Technological Systems, which is part of the Police's Computer Directorate, as well as the Israeli company Optidefense, and Israel Border Police.

▶▶ Read more at source's URL.

The US has decided to stop sending bomb-sniffing dogs to two Middle Eastern countries after many of the animals died

Source: https://www.businessinsider.com/us-stops-sending-bomb-sniffing-dogs-egypt-jordan-deaths-2019-12

Dec 21 – The US has made the decision to temporarily stop sending explosive-detection dogs to Jordan and Egypt after discovering that a lot of the animals had died as a result of poor treatment, a report from the Department of State's Office of the Inspector General revealed.

The department watchdog, which had previously pushed the Department of State to stop sending dogs to these countries after an earlier investigation uncovered a number of animal deaths and other serious problems, wrote that it had "received notice of additional canine deaths that warrant immediate department action."

The report released Friday said that two dogs sent to Jordan died in June and September of this year of "non-natural causes." Specifically, one died from hyperthermia (heatstroke), and the other died after being poisoned by insecticide that was sprayed in or near the kennel.

Another dog was found in October to be suffering from leishmaniasis, a preventable disease transmitted by sand flies.

The Office of the Inspector General also found that three of the ten dogs provided to Egypt, which has been uncooperative with department officials, died from lung cancer, a ruptured gall bladder, and hyperthermia.

The latest report follows an IG evaluation released in September that examined the state of the program in Jordan, a US ally in the counter-terrorism fight.

That report, which characterized the conditions the animals were living in as "disturbing," found that "at least 10 canines had died from various medical problems from 2008 through 2016 while others were living in unhealthy conditions."

At that time, the Office of the Inspector General recommended that the Department of State put a hold on the Explosive Detection Canine Program (EDCP) for Jordan until the country could demonstrate that it was able to provide proper care, but the department refused, citing national security concerns.

The Department of State assured inspectors that it was taking steps to improve the situation and provide better care for the dogs. "The death of two canines from non-natural causes — namely, hyperthermia and poisoning — since June 2019 raises serious questions about the Department's contention that it has taken adequate steps to protect their health and safety," the latest Office of the Inspector General report said.

The IG report also noted that the previously-unreported deaths in Egypt, which barred State Department officials from visiting the areas where the dogs were living and working, were also cause for concern.

While the Department of State initially refused to stop sending dogs, the latest findings by the department watchdog appear to have led the department to change its mind.

In August, the Department of State repossessed ten dogs from Morocco because they were not being used for their intended purpose, the IG report revealed.

Somalia car bombing: 'Heinous act of terror' leaves at least 79 dead

On 28 December 2019, a suicide truck bomber killed at least 84 people at the Ex-Control Afgoye police checkpoint in Mogadishu, Somalia. More than 150 others were wounded and, as of 30 December, 24 people remained missing. There was no immediate claim of responsibility. The attack was the deadliest in Somalia in more than 2 years since the 14 October 2017 Mogadishu bombings, which killed 587 people.

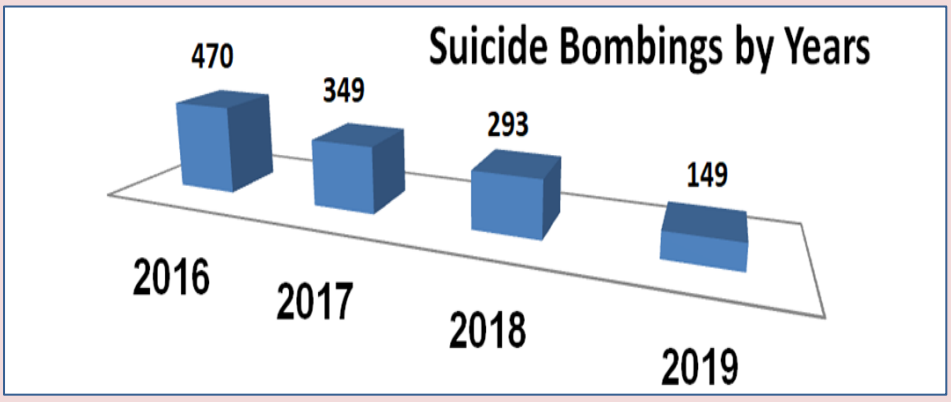
Attack
The attack occurred at a busy intersection on the western outskirts of Mogadishu, at a police checkpoint during local rush hour. The major intersection connects Mogadishu with the rest of southern and southwestern Somalia. The Ex-Control Afgoye checkpoint is located near a tax office, and is used by vehicle entering Mogadishu from nearby Afgooye town. The truck bomb explosion caused massive damage to the surrounding areas, and left many of the dead burned beyond recognition. At least 15 of those killed were university students returning to class at Benadir University, whose minibus was demolished in the explosion. Many others were wounded. Two Turkish engineers, who were constructing a road from the checkpoint into the city, were also killed in the bombing.

ESRI Terrorist attacks
Source (interactive): https://storymaps.esri.com/stories/terrorist-attacks/

Suicide Bombings Worldwide in 2019: Signs of Decline following the Military Defeat of the Islamic State

By Yoram Schweitzer, Aviad Mendelboim, and Dana Ayalon
Source: https://www.inss.org.il/publication/suicide-bombings-worldwide-in-2019-signs-of-decline-following-the-military-defeat-of-the-islamic-state/

Jan 02 – Suicide bombings in 2019, despite a sharp decline in number from the previous year, remained one of the most effective tactics available to terrorist groups. The drop in number is in keeping with an ongoing (albeit more modest) decline seen in recent years, but the figures of 2019 can be attributed to the final military defeat of the Islamic State. Therefore, while the Islamic State and its affiliates - the organizations that since 2015 have committed the most suicide bombings – remain the groups primarily responsible for suicide bombings, the actual number of attacks plummeted. According to collected data in 2019, 149 suicide bombings were carried out in 24 countries by 236 suicide bombers, among them 22 women. In these suicide bombings, 1,850 people were killed and 3,660 were wounded.



Read the full report

In 2019, around 149 suicide bombings were carried out worldwide (compared to around 293 in 2018 - a decline of around 49 percent). For the second consecutive year, the most active arena in this regard was Asia, where around 68 suicide bombings were carried out – primarily in Afghanistan - accounting for 45.5 percent of all suicide bombings globally. In the Middle East, around 47 suicide bombings were carried out in 2019, accounting for around 31.5 percent of all suicide bombings. In Africa, around 33 such attacks were carried out in 2019, accounting for around 22 percent of attacks during the year. Latin America saw a sole, rare attack, launched in Colombia, by the National Liberation Army, killing 21 people.
All suicide bombings listed and analyzed by the Terrorism and Low Intensity Conflict Program at the Institute for National Security Studies (INSS) are based on at least two

independent sources. Combined assaults on multiple adjacent targets simultaneously, or as part of deliberate advance planning, are considered a single attack.

The Sharp Decline in Attacks by the Islamic State and its Affiliates

The gradual military defeat of the Islamic State intensified over the last two years, eliminating the entity's control over swathes of Iraq and Syria and culminating with the loss in March 2019 of its last stronghold, al-Baghuz, in eastern Syria. In its stead, the ISIS organization remains operational in the Levant and cooperates with allied groups worldwide that still identify with and use the brand name Islamic State.

Despite the sharp decline in 2019 in the number of suicide bombings carried out by the Islamic State and its global affiliates - some 60 percent - it remained the main element perpetrating such attacks. The Islamic State/ISIS and their affiliates were responsible for some 69 suicide bombings, which constituted some 46 percent of all such attacks globally. These attacks killed around 850 people; in 2018, the Islamic State and its affiliates were responsible for around 172 attacks that caused the deaths of around 1,930 people. In parallel, 2019 also saw al-Qaeda and its affiliates - the rivals of ISIS in the Salafi-jihadist movement for the leadership of the global jihad camp - carry out around 52 attacks that comprised around 35 percent of all suicide bombings. Together, these organizations were unquestionably responsible for more than 80 percent of all suicide bombings worldwide.

2019 saw approximately another 17 suicide bombings, (accounting for around 11.5 percent of suck attacks) where the identity of the group responsible is not known, but given the locations of the attacks it most likely that at least 14 of them were carried out by members of the Salafi-jihadist movement. Additional suicide bombings were carried out by other groups that are identified with the Salafist-jihadist movement even if they do not formally belong to one of the two major camps. Overall data thus indicate that terrorist groups identified with the Salafi-jihadist movement were responsible in 2019 for some 97 percent of all suicide bombings.

In contrast to the dominance of the Middle East, particularly Iraq, as the region where most suicide bombings were carried out for some 15 years (with the exception of 2009-2012), for the last two consecutive years it has been Asia – primarily Afghanistan – that was the main arena. In Asia overall, a total of around 68 suicide bombings were carried out in 2019 - a sharp decline of some 40 percent relative to the previous year (113 attacks). Afghanistan remained the most frequent site for suicide bombings, with around 43 suicide bombings in 2019 - a drop of around 48 percent relative to 2018. Khorasan Province, an Islamic State affiliate in Afghanistan depicted by the United States as the deadliest organization today, carried out around 6 suicide bombings in 2019 (a sharp decline of 83 percent from the previous year, when the group carried out around 35 such attacks). By contrast, the Taliban organization, al-Qaeda's main partner and patron in Afghanistan, remained active, conducting around 28 suicide bombings in 2019 compared to around 25 in 2018. Around 10 suicide bombings were carried out in Pakistan in 2019 (compared to around 22 the previous year, a drop of some **54.5** percent). Additional attacks were carried out in Indonesia (4 compared to 2 last year) and the Philippines (3 compared to a single one in 2018), while Bangladesh, China, India, and Iran each suffered one such attack. Four suicide bombings were carried out in Sri Lanka in 2019, the first such instances in many years. Previously, for more than a decade while in the midst of an ethnic conflict, Sri Lanka was a main arena for suicide terrorism by the Tamil Tigers. Before 2019, no suicide bombings by Islamist groups identified with the Salafi-jihadist movement occurred there. In 2019, a series of suicide bombings carried out by a local group in the name of the Islamic State killed around 270 people and wounded around 500.

Despite the reduction in the number of suicide bombings in the Middle East, the region remains a central arena for this tactic. In 2019, some 47 suicide bombings were carried out there, making up some 31.5 percent of all such attacks globally. This is in contrast to the previous year, when around 98 of suicide bombings took place in this region - a drop of around 52 percent. Syria was the site of the most suicide bombings in 2019 in the Middle East - around 29 - occurring amidst the ongoing civil war and the campaign to oust the Islamic State from territories in its control. Around 8 suicide bombings were carried out in Iraq - a reduction of around 76.5 percent over 2018 - with all attributed to the Islamic State. Additional such attacks in the Middle East took place in Egypt - 4 compared to 5 the previous year. Libya and Yemen each suffered 2 such attacks, which represents a sharp decline in suicide bombings: Libya saw around 13 such attacks in 2018 (a reduction of around 84.5 percent); around 7 were carried out in Yemen (a reduction of around 71.5 percent). In Lebanon and the Gaza Strip, one suicide bombing each was carried out in 2019. Since 2015, the Islamic State has remained the dominant force in the execution of suicide bombings in the Middle East, and in 2019 the Islamic State and its affiliates were responsible for around 34 suicide bombings that accounted for around 72.5 percent of all suicide bombings in the Middle East.

Some 33 suicide bombings were carried out in Africa in 2019, compared to around 81 the previous year prior - a reduction of around 59 percent - and these account for around 22 percent of all suicide bombings globally. The highest number of attacks occurred in Somalia - some 13 attacks, versus around 25 attacks in 2018, a decline of around 48 percent. Like Asia, Africa is targeted for infiltration by organizations supported by the Islamic State, chief among them Boko Haram, which is active mainly in Nigeria as well as Chad and Niger, and al-Shabaab, affiliated with al–Qaeda which is active mainly in Somalia and Kenya. These groups carried out the sweeping majority of suicide bombings on the continent. Around 6 additional attacks were documented in Nigeria, compared to around 39 the year before - a sharp decline of around

84.5 percent; in Mali, there were around 5 compared to 6 the year prior; in Niger, there were around 4 such attacks; in Tunisia, there were around 3, compared to around 2 in 2018. Chad and Kenya each suffered one such attack, compared to 2018, when no suicide bombings took place in either country.
Female suicide bombers: in 2019, around 22 women took part in around 14 suicide bombings that were executed in 9 countries. These attacks killed around 98 people and wounded approximately 230. In 2018, around 84 women took part in around 38 such attacks, causing the deaths of around 160 people. The 2019 figure thus represents a decline of around 74 percent in the number of female suicide bombers. Around 19 of the female suicide bombers belonged to the ISIS organization, either directly or indirectly, and in 2019, as with the year prior, it was the affiliated Boko Haram group that dispatched most female suicide bombers: around 15 women carried out around 7 suicide bombings, compared to around 74 women sent by the group to carry out around 31 suicide bombings in 2018.
In conclusion, despite the sharp decline in their number, suicide bombings remain a useful and effective modus operandi in the service of terrorist groups. In 2019, around 21 different organizations conducted suicide bombings, the sweeping majority of them adherents of the Salafi-jihadist movement. Thus, for example, in 2019 suicide bombings killed an average of around 12 people each, but in more than a dozen attacks the death toll was much higher. A salient example is the outcome of the simultaneous attack in Sri Lanka on April 21, 2019, in which around 253 people were killed.
Among the main factors in the reduction in the number of suicide bombings in 2019 was the military defeat and ongoing decline of the Islamic State, especially in the last two years, which led to a total loss of control over territory as well as a sharp erosion in income and, in the absence of new recruits, of operatives. Indeed, foreigners who joined the Islamic State carried out most suicide bombings in its name in the Levant. The decline of the Islamic State in 2019 has been felt on all fronts where it was active, especially in Iraq, which for many years was the main arena for operations of this kind, as well as in two other main operational theaters: Nigeria and Afghanistan.
The elimination of the caliph Abu Bakr al-Baghdadi, notwithstanding the appointment of a successor caliph, alongside the loss of Islamic State strongholds, prompted a period of regrouping and retrenchment for ISIS in the Levant and efforts to strengthen its ties to global partners. ISIS and its affiliates, and in parallel also al-Qaeda and its affiliates, see in suicide bombings not just an effective tactic but also a shared emblem of religious and moral values that proves their dedication to the "path of God." They are thus not expected to stop using it as a main means of fighting their enemies. The scope and frequency of future such activity will be affected to a decisive degree by the pace of their recovery, internal organizational circumstances, and the situation within countries where they operate. ISIS, which has remained active in Syria and Iraq, is already proving its survivability and capacity to carry out terrorist and guerrilla attacks, mainly with tactics other than suicide bombings, though at a lower rate than in the past.
Against this backdrop, and despite the decline noted in 2019 in the number of suicide bombings worldwide and specifically those by the global jihad, a renewal of momentum for terrorist attacks – including suicide bombings – within and outside the Middle East can be expected. A resurgence of this activity may be based on fighters who are still in various areas in Syria and Iraq, assisted by reserve fighters who are in detention camps and displaced-persons camps in Syria, alongside the many hundreds of fighters who are affiliated with the Salafi-Jihadist movement and are now concentrated in Idlib province and may to leave Syria. Thus, the decline in the number of suicide bombings in 2019, as a continuation of the trend noted in previous years, does not necessary attest to this tactic being any less alluring for groups that are disposed to use it and believe in its effectiveness. A regrouping the global jihad camp is thus liable to be manifested in a renewal of suicide bombings, and even perhaps an increase in their frequency.

Yoram Schweitzer *is the head of the Terrorism and Low Intensity Conflict research program at INSS.*
Aviad Mendelboim *is a research assistant in the program.*
Dana Ayalon *is an intern on the program who is responsible for the subject of suicide bombings.*

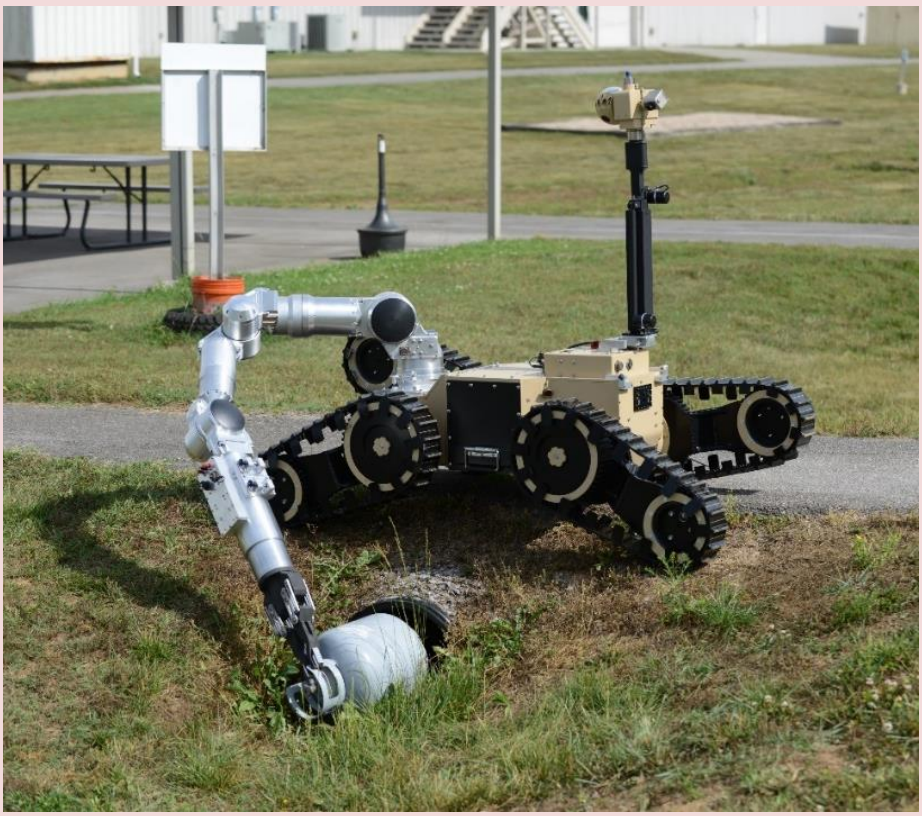
Andros FX: Next-Gen Solution for Explosive Ordnance Disposal

Source: https://i-hls.com/archives/97730

Jan 01 – H.B.A. System Integrators, an Israeli homeland security company with over 30 years of experience in the fields of anti-terror, border checkpoint technology, robotics, and perimeter defense, are providing the newest robotic member for fleets of EOD (Explosive Ordnance Disposal) robots, the **Andros FX**, manufactured by Remotec of Northrop Grumman.
The Andros FX fully leverages H.B.A.'s 30 years of experience with managing and integrating autonomous and unmanned robotic systems for land based and underwater operations. With a diversified fleet of unmanned EOD robots and years of experience working alongside the most experienced bomb disposal experts in the Israeli Defense Force and Israeli law enforcement, H.B.A. has established the EOD fleet of law enforcement bomb

disposal departments, while also providing complete turnkey solutions for worldwide customers. H.B.A. truly aims, and succeeds, at minimizing human exposure to explosives and other harmful materials, all while providing first responders with the most advanced and accurate tools to dispose of such dangerous materials.

The heavy-duty Andros FX has been built from the ground up to supply the system's operator with the most versatile and user-friendly experience possible. Weighing in at 383 kilograms, the EOD robot utilizes an advanced combination of ruggedness, mobility, and high dexterity in order to defeat the most complex threats. Andros FX's ruggedness and large number of operational tools and payload capabilities expands the operator's ability to complete a wide range of missions with more confidence and in less time.

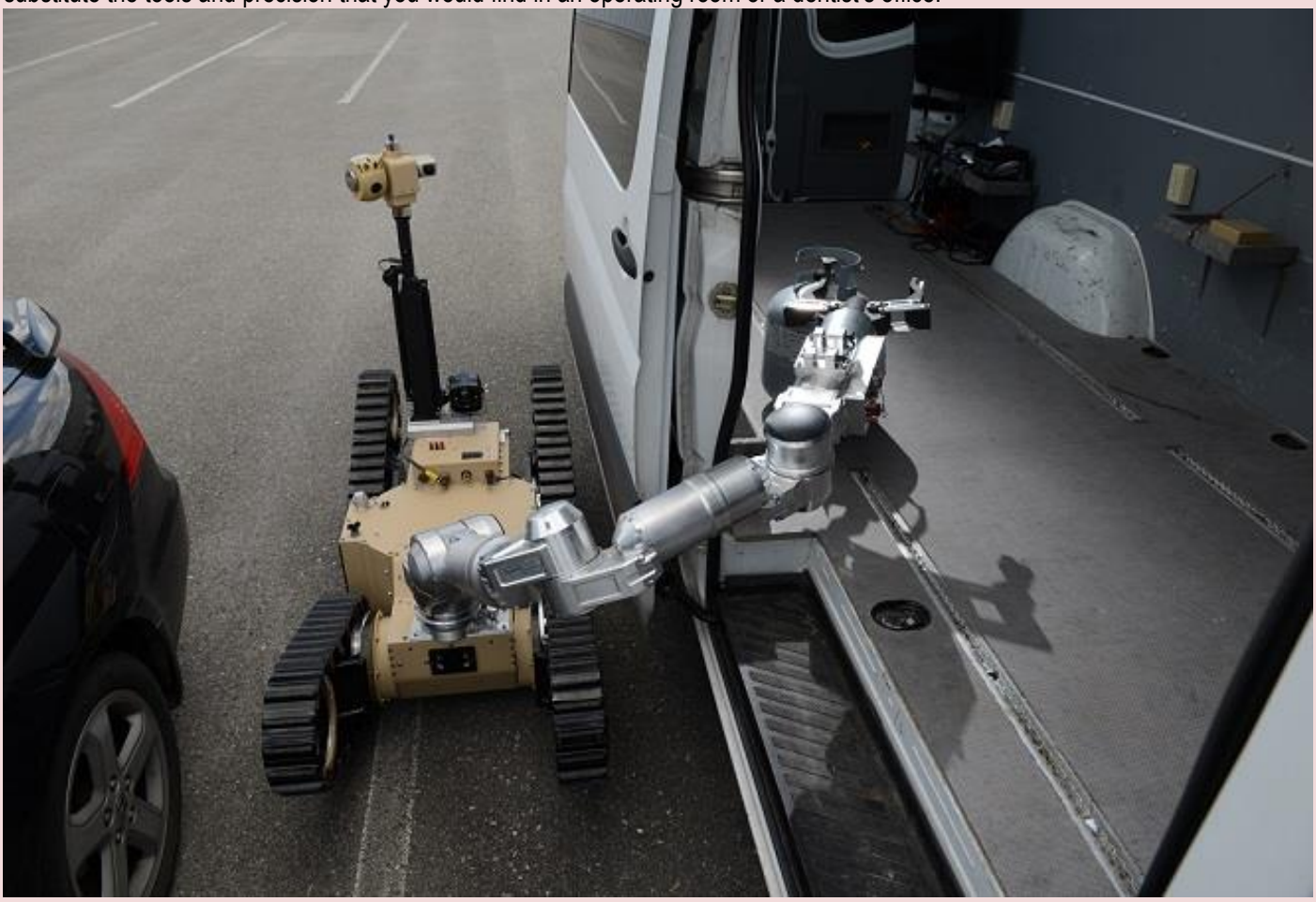


The system can be controlled manually by an operator and it could also have a preset route and set of tasks uploaded for automatic operation. Andros FX's control system displays 3D images of the robot to help the operator visualize the robot's settings and payloads. Furthermore, the robot's maintenance information is also displayed via touch screen graphics to help the operator gain the best understanding of the robot's condition.

With a quad track mobility system, the Andros FX is capable of maneuvering to and through pretty much any type of terrain. Each track has its own motor and can be controlled independently from the other tracks in order to increase the operator's flexibility to control the robot. This allows the EOD robot to go up and down stairs, overcome the toughest obstacles, and cross rough terrains. Furthermore, the tracks could re-angle themselves in order to give the Andros FX another 14 inches in height for increased reach and observation capabilities.

Yet, an effective EOD robot needs more than just advanced mobility, the Andros FX utilizes a long, strong, and smart manipulator for its operations. Similar to the robot's track system, Andros FX's manipulator can also be controlled joint by joint for flexible and accurate maneuvers. The manipulator allows the robot to carry up to 61 kilograms when the arm is fully extended. The robot is capable of carrying even more weight, up to 124 kilograms, when the arm is only partially extended. Andros FX's manipulator grant the robot

a vertical reach of 3.2 meters, when the arm is fully extended and the robot is "standing" on its tracks.
At the end of the robot's manipulator is its gripper. The gripper is capable of extending an extra 6 inches for fine and accurate movement. The gripper also comes equipped with an IR sensor, lights, and camera installed in its "palm" for maximum precision.
The Andros FX is also compatible with a second manipulator for extreme precision. Based on the Jaco robotic arm, which is used to assist people with upper-body disabilities, the second manipulator is for more "surgical" operations that require fine and precise movements and has already been provided to US bomb disposal departments.
"The focus is precision," said Manuel Bar-Gil, a senior manager at H.B.A. to iHLS. "[Andros FX] provides a solution that could substitute the tools and precision that you would find in an operating room or a dentist's office."



Ideal for vehicle-borne IED (Improvised Explosive Device) disposal, the Andros FX's design supplies a solution for a wide array of threats stretching much farther than EOD missions. Any threat involving carrying, cutting, drilling, precise movements, and even negotiation can be neutralized by H.B.A.'s newest robot integrations, since the robot also comes equipped with a two-way speaker/microphone system.
"Using the knowledge and expertise obtained from bomb disposal experts, we have developed a set of tools that supply an end solution for the bomb disposal expert in the field," said Bar-Gil.
The system comes equipped with a set of cameras and sensors in order to ensure maximum situational awareness. A weapon's camera and laser sighting system can also be attached to the system for additional targeting assistance.
With several units already expected to be delivered to the IDF in the beginning of 2020, H.B.A. System Integrators are the only suppliers of the Israeli police and military forces that work alongside U.S. federal agencies, such as the Department of Homeland Security. This does not come as much of a surprise considering the company's record and experience with innovation and technologies in the defense and homeland security sectors.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

CYBER NEWS

Report highlights risk of cyberattacks and terrorism during Tokyo Olympics

Source: https://www.japantimes.co.jp/news/2019/12/20/national/japan-cyberattacks-terrorism-tokyo-olympics/#.Xf5JofzQDIU

Dec 20 – The Public Security Intelligence Agency has warned against cyberattacks in an annual report with the 2020 Tokyo Olympics and Paralympics just around the corner.

In the report released Thursday regarding the security situation in Japan and overseas, the agency said that **cyberattacks** may interfere with Olympic operations as prior host nations have become targets of such attacks in recent years.

In addition, the report said that the Summer Games are "the perfect opportunity for terrorists to gain global attention."

It stressed the need to watch out for terrorist attacks on competition venues, as well as public transportation and accommodation facilities, during the games between July and September next year.

On North Korea, the report said that while the leaders of the United States and North Korea have held three meetings, the future of bilateral negotiations on the dismantling of Pyongyang's nuclear weapons program is still unclear.

The report warned that North Korea may engage in military provocations, including conducting nuclear tests and firing intercontinental ballistic missiles.

On the now-defunct doomsday cult Aum Shinrikyo, the report said that former cult leader Chizuo Matsumoto still has deep influence over the successor cults even after his execution in July 2018.

Matsumoto, who went by the name of Shoko Asahara, was executed for his involvement in a series of crimes committed by Aum, including a deadly sarin attack in Tokyo's subway system in 1995.

Iran Spent Years Building a Cyber Arsenal. Will It Unleash That Arsenal Now?

Source: http://www.homelandsecuritynewswire.com/dr20200108-iran-spent-years-building-a-cyber-arsenal-will-it-unleash-that-arsenal-now

Jan 08 – In 2007, a computer virus crippled centrifuges at Iran's uranium enrichment facility in Natanz, setting back its nuclear program by years. Chris Meserole writes in Lawfare that the Stuxnet attack—not uncovered until a few years later—taught the revolutionary regime in Tehran a valuable lesson about how effective cyber weapons can be, prompting Tehran to invest heavily in cyber capabilities of its own. "The results speak for themselves: Iranian hacking groups have graduated from conventional distributed denial of service (DDoS) and domain name system (DNS) attacks to more sophisticated operations against critical infrastructure and industrial control systems," Meserole writes, adding:

> *In the wake of Qassem Soleimani's killing last week, the question of how Iran aims to use its cyber arsenal has acquired a newfound urgency. Tehran will need to respond forcefully to Friday's attack, as well as related recent strikes. Iran's cyber weaponry would seem to offer a ready-made option for high-impact, low-cost retaliation, as Iran's national security chiefs have apparently recognized.*
>
> *Yet fears of a devastating Iranian cyberattack are premature. The coming days and weeks will almost certainly bring an uptick in Iranian activity, as always happens when the two countries are engaged in brinksmanship. But it would be surprising if Tehran's promised retaliation leveraged cyber operations alone.*
>
> *Consider Iran's three options going forward: a response that escalates the conflict further, a strike that maintains the status quo, and an attack that "saves face" while de-escalating the conflict. In each case, cyber weapons would not be able to signal Iran's preference effectively.*

As Suzanne Maloney has noted, Iran is likely to take some time to evaluate its options — and in the interim, it will want a low-cost way of probing for vulnerabilities while signaling to the White House that it fully appreciates the seriousness of what has just taken place. Cyber operations are ideally suited for such a task.

"The U.S. and its allies would do well to prepare for heightened cyber activity from Iran. But they would do better to prepare for military force more" Meserole concludes.

How Real Is the Threat of Cyberwar Between Iran and the U.S.?

By Vasileios Karagiannopoulos

Source: http://www.homelandsecuritynewswire.com/dr20200110-how-real-is-the-threat-of-cyberwar-between-iran-and-the-u-s

Jan 10 – The world shook at the news in early January that a U.S. drone strike had killed Iran's top military general, Qassem Soleimani, outside Baghdad's airport. According to the Pentagon, the attack was conducted as a decisive defensive action at the direction of President Donald Trump to protect U.S. personnel abroad.

The supreme leader of Iran, Ayatollah Ali Khamenei called for "severe revenge" for Soleimani's death and on 8 January, Iran launched missiles against U.S. military bases in Iraq in retaliation.

There are widespread concerns that these events might fuel further conflict between the two countries. Considering the importance of information networks and cyberspace for our everyday lives, there is also concern that this conflict might not only take place in the physical world but could take the form of cyber-attacks. These could have serious consequences, particularly since Iran has demonstrated an increase in its cyber-capability in the past decade.

Cyber Capabilities

The most memorable cyber-attack between Iran and the U.S. was the Stuxnet virus which infected Iranian uranium enrichment facilities and caused their centrifuges to malfunction in 2010. Although no country claimed responsibility, it is widely considered to be the work of state-supported U.S. and Israeli experts.

At the moment, U.S. cyberwarfare capabilities are multifaceted, organized and of a very high level. In October 2019, U.S. officials told Reuters the U.S. had launched a secret cyber-operation against Iran's propaganda infrastructure following an alleged Iranian drone and missile attack on Saudi Arabian oil facilities.

On the other side, it was discovered in 2013 that Iranian hackers who allegedly perform work for the Iranian government had penetrated the computer controls of a small dam north of New York city. These same hackers also launched cyber-attacks against dozens of large financial institutions and blocked customers from accessing their accounts online.

In the current climate, Iran could consider using its cyber-attack capability as part of its retaliation for the killing of Soleimani. Acknowledging the possibility of a spate of cyber-attacks from Iran-affiliated parties, U.S. Homeland Security warned U.S. companies to consider and assess the possible impact such an attack could have on their business.

Contrary to these concerns, Iran's capability to launch major cyber-attacks that could affect a large part of the U.S. population has been downplayed by some cybersecurity experts. Others have argued that cyber-attacks might not be aggressive enough retaliation for Iran, which is more vulnerable than it is capable online.

It's one thing to talk about cyber-attacks by hackers with a political or nationalist motivation – of which there has been a reported increase in the wake of Soleimani's death. But it's another issue altogether to talk about acts that are so forceful and monumental that they could amount to cyberwar.

Cyberwarfare is far more serious and could amount to taking control of critical infrastructure to disable military targets or seriously harm sections of the public. Acts of war involve states and relate to actions led by governments or military forces. But it's often difficult to attribute a certain cyber-attack to a particular government. Attacks can be perpetrated at a distance and by hacker groups not openly employed by the government involved.

Under international law, countries can legitimately defend themselves if they come under armed attack – which could include an equally serious cyber-attack. The U.S. has explicitly reserved the right to respond to cyber-attacks with military force. But the

justification for any counter-strike would be weakened if it's unclear whether the state accused of being behind a cyber-attack had explicit knowledge that the attack was going on.

From Cyber to Physical Attacks

In the current climate, there is a serious concern that a cyber-attack – even if it's not successful – could lead to physical retaliation. The memory of an Israeli missile attack in May 2019 against Hamas hackers, accused by the Israeli Defense Force of attacking Israeli targets, is still fresh.

If the U.S. believed that Iran was imminently about to target critical infrastructure in a cyber-attack, this could provide legitimate justification under international law for a pre-emptive physical strike against Iranian targets. But judging when an attack is imminent in cyberspace is challenging: a serious cyber-attack could be planned well in advance or be executed very quickly.

Although the immediate threat of further military violence between the U.S. and Iran seems to be diffusing, the fallout from the strike on Soleimani is taking place in a new era of modern warfare, where basic notions of war and international law are constantly evolving.

Although the world is yet to see a government admit to launching a cyber-attack so grave that it's been considered an act of war by the target country, the potential for such attacks does exist. Even if such capabilities are not used, the threat of them could provide justification for physical counterattacks with destructive results in future conflicts.

***Vasileios Karagiannopoulos** is Reader in Cybercrime and Cybersecurity, University of Portsmouth.*

The 5 Biggest Cybersecurity Trends In 2020 Everyone Should Know About

Source: https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/#762154e37ecc

Jan 14 – The vital role that cybersecurity plays in protecting our privacy, rights, freedoms, and everything up to and including our physical safety will be more prominent than ever during 2020. More and more of our vital infrastructure is coming online and vulnerable to digital attacks, data breaches involving the leak of personal information are becoming more frequent and bigger, and there's an increasing awareness of political interference and state-sanctioned cyberattacks. The importance of cybersecurity is undoubtedly a growing matter of public concern.

We put our faith in technology to solve many of the problems we are facing, both on a global and personal scale. From smartphones and AI personal assistants to space travel, curing cancer, and tackling climate change. But as the world becomes increasingly connected, the opportunities for bad guys to take advantage for profit or political ends inevitably increases. Here's what will be top of the agenda when it comes to cybersecurity over the coming year:

1. Artificial intelligence (AI) will play an increasing role in both cyber-attack and defense

AI is the new arms race, but unlike earlier arms races, anyone can get involved – there's no need for the sort of resources that were previously only available to governments.

This means that while AI is undoubtedly being researched and developed as a means of crippling an enemy state's civil and defense infrastructure during war, it's also easily deployable by criminal gangs and terrorist organizations.

So rather than between nations, today's race is between hackers, crackers, phishers and data thieves, and the experts in cybersecurity whose job it is to tackle those threats before they cause us harm. Just as AI can "learn" to spot patterns of coincidence or behavior that can signal an attempted attack, it can learn to adapt in order to disguise the same behavior and trick its way past our defenses.

This parallel development of offensive and defensive capabilities will become an increasingly present theme as AI systems become more complex and, importantly, more available and simpler to deploy. Everything from spam email attempts to trick us into revealing our credit card details to denial-of-service attacks designed to disable critical infrastructure will grow in

frequency and sophistication. On the other hand, the tech available to help us avoid falling victim, such as deep learning security algorithms, automation of systems that are vulnerable to human error, and biometric identity protection, are getting better too.

2. Political and economic divisions between east and west lead to increased security threats

As it appears to most people, the internet and the online world is an international entity – relatively free of borders or restriction on the free movement of information and ideas. It's been built that way because its architects understand the importance of international cooperation when it comes to accessing talent and resources. But that's really all just an illusion. The corporations, networks, and associations which provide the infrastructure behind the scenes are legal entities obliged to comply with national laws and regulations. With no end in sight to the "trade war" between the world's superpowers, talk of fracturing among international organizations like the UN or EU, and an ongoing tech-driven arms race among nations that are economic competitors, that illusory veneer is being stretched thinner and thinner. And that could have very scary consequences.

Just a few weeks ago, Russia announced that it had tested an 'unplugged' internet, basically a country-wide alternative to the global internet, which could give their Government control over what citizens can access on the web. Countries like Iran and China are already censoring content and block access to external information.

In 2019, we also saw the US government effectively embargoing partnerships between US tech firms and the Chinese mobile giant Huawei, due to fears over the close links between Huawei and the Chinese state. If more barriers like these go up, it could easily have the effect of preventing international cooperation on both the technological and regulatory challenges of cybersecurity, and that's only likely to benefit the bad guys.

3. Political interference increasingly common and increasingly sophisticated

Targeted disinformation campaigns aimed at swaying public opinion have almost become an accepted feature of democracy today. With a US presidential election coming up in 2020, it seems certain that they will make headlines once again.

So far, cybercrime targeting elections has taken two forms. The first involves the spreading of "fake news" and false narratives – usually designed to slur a candidate – via social media. The second is direct attacks against candidates' or digital electoral infrastructure.

Countering the false narratives means building systems, either automated or manual, that can sift out lies, propaganda, and bad-faith by analyzing both content and metadata – where the information originates from, and who is likely to have created it. Facebook and Google have both invested in technology designed to determine whether or not political messaging fits patterns that suggest it could be part of a targeted "fake news" campaigns. This is because of the overwhelming evidence that these tactics are being increasingly adopted by state actors with the aim of causing political unrest. The Chinese government has been suspected of attempting to push a pro-China narrative around elections in Taiwan and civil protests in Hong Kong using fake social media accounts, and candidates' private emails were hacked and released in both the 2016 US elections and the 2017 French elections.

Both forms of digital electoral interference are likely to become a growing problem over the next 12 months, partly due to the fact that they have proven to be highly effective up until now. Consequently, we can expect more investment in technology designed to counter them, as well as efforts to raise public awareness of the issue.

4. The cybersecurity skills gap continues to grow

During 2020, research suggests the number of unfilled cybersecurity jobs will increase from just 1 million in 2014 to 3.5 million. This deficit of skills is likely to become a growing matter of public concern during the early part of this new decade.

The threats we face in cyberspace today, from thieves attempting to clone identities to carry out fraud, to political disinformation campaigns designed to alter the course of democracies, will only become more intense unless there are sufficient people with the skills to counter them coming through the pipeline. Without investing in training existing staff on how to prevent or mitigate cyberattacks in their field, as well as hiring experts with the skills to spot new threats on the horizon, industry stands to lose hundreds of millions of dollars. The current average cost incurred by a company in the US that suffers a data breach stands at $8.19 million. Amongst organizations that have implemented fully automated cybersecurity defenses, that cost drops to $2.6 million. Of course, implementing these mature defenses requires access to a skilled, experienced cybersecurity workforce – something that is likely to increasingly become a challenge in coming years.

5. Vehicle hacking and data theft increases

Even before we get into the subject of self-driving cars, vehicles today are basically moving data factories. Modern cars are fitted with an array of GPS devices, sensors, and in-car communication and entertainment platforms that make them an increasingly profitable target for hackers and data thieves.

Criminals have learned to piggyback into private networks through connected home appliances and smart devices, thanks to the lack of security standards among the thousands of device manufacturers and service providers. Likewise, the automobile is likely to increasingly become the backdoor of choice in the coming years thanks to the growing amount of data they collect and store about our day-to-day lives. Attackers will have the choice of targeting either the vehicles themselves, perhaps using them to access email accounts and then personal information, or the cloud services where our data is routinely sent for storage and analysis. Large scale harvesting and resale of this data on the black market is highly lucrative for cybercriminals.
Another very real danger is that malicious actors could learn to compromise the digital controls and safety features of modern vehicles. The idea of hijacking autonomous cars and taking over their controls may seem far-fetched right now, but it's a threat that's being taken seriously by the automotive industry as well as lawmakers. During 2020, we're likely to see more debate over this aspect of the safety of self-driving vehicles, as the regulatory framework that will allow them to operate on our roads continues to take shape.
For more on this topic, have a look at my conversation with cybersecurity expert Professor Kevin Curran, in which we discuss the biggest cybersecurity challenges and how to tackle them:

Top 10 Cybersecurity Courses In India: Ranking 2020

Source: https://analyticsindiamag.com/top-10-cybersecurity-courses-in-india-ranking-2020/

Jan 14 – Indian enterprises — be it larger companies or smaller enterprises — are always on the hunt for skilled cybersecurity professionals to augment their digital infrastructure and safeguard their data from unwanted intrusions. Although there are several job vacancies in the country, recruiters are still facing a big challenge to find the right resources for the positions.
According to a report, the increasing cyber-attacks and data protection laws are expected to create 1 million jobs and $35 billion opportunities for India by 2025. So, this could be an opportunity for individuals interested in cybersecurity as a career option.
As the country is creating massive opportunities, enterprises are desperate to hire people for a lucrative pay scale; however, a significant amount of upskilling is required. Here's our first-ever ranking of Cybersecurity courses in India.
A primary survey which was conducted a few months back was taken into consideration to understand the preferences of candidates, based on their experience. The survey helped to invalidate the data and providing a rationale for the ranking, wherever required. Students feedback and expert advice were also accounted for the overall ranking process. The courses that have not been mentioned in the ranking either did not participate or did not make it to the top ten.

1. Master Certificate in Cyber Security (Red Team) – Jigsaw Academy with HackerU

Jigsaw Academy is a global award-winning training provider headquartered in Bengaluru, India. Founded by the duo of Gaurav Vohra and Sarita Digumarti, Jigsaw Academy has been instrumental in shaping the careers of over 50,000 learners in 30+ countries by helping them build a successful career in emerging technologies with specialised industry oriented courses. The domain experts and educators at Jigsaw Academy offer meticulously structured courses with industry-relevant curricula. Jigsaw Academy trains professionals in the areas of analytics, data science, big data, machine learning, business analytics, and more recently, cybersecurity and cloud computing.
Flagship Cybersecurity Program: Jigsaw Academy's Master Certificate in Cyber Security (Red Team) in association with HackerU
Duration Of The Program: 600 Hours (20 Hours of Live Online Instructor-Led, and 40 Hours of In-person Classroom – Basic and Fundamental Program + 4 Months-Main Program)
Cost Of The Program: ₹2,80,000 + Taxes (Scholarships available up to ₹70,000)
Cities Of Operation: Bengaluru
Course Content And USP Of The Program: Jigsaw Academy's Master Certificate in Cyber Security (Red Team), is the only program on offensive technology in India. The program is intensive in delivery and extensive in technology coverage and is delivered in collaboration with/by HackerU, Israel's premier cybersecurity training institute. HackerU has more than 20 years of experience in providing cybersecurity solutions and training in the US, Singapore, Russia, Australia, and other geographies in the US and European market. The course covers more than 14 modules in 3 different phases focusing on network fundamentals, Windows, Linux Administration, applicative hacking and penetration testing on emerging technologies like IoT.

2. Stanford Advanced Computer Security Program – Great Learning

Great Learning is a technology-enabled online and blended-model learning organization that offers high-quality, impactful and industry-relevant learning programs to working professionals. The programs help learners master 'hard' competencies such as business analytics, data science, big data, machine learning, artificial intelligence, cloud computing,

cybersecurity, digital marketing and digital business. Great Learning's analytics programs have been ranked #1 in India for five years in a row, and its professional learning programs have delivered over 6 million hours of impactful learning to over 10,000 learners.
Flagship Cybersecurity Program: Stanford Advanced Computer Security Program
Duration Of The Program: 6 Months
Cost Of The Program: $2,495 or ₹1,74,650 (approximately)
Cities Of Operation: Online for India, UK, South East Asia, Australia and other international locations
Course Content And USP Of The Program: Advanced Computer Security Program is created by Stanford University, and is taught by distinguished faculty from Stanford's Computer Science and Engineering departments. The comprehensive program covers all the essential areas in cybersecurity from a practitioner's perspective. Some of the salient features of the program are:

1. A certificate of achievement from Stanford Engineering
2. Regular mentorship from industry experts in cybersecurity
3. Hands-on practice through a series of labs and projects that allows participants to put what they learned to practice.

This program is aimed at aspiring security and system architects and provides a holistic understanding of the various moving parts within cybersecurity. The range of topics covered in the program includes web applications security, network security, mobile security, cryptography, writing secure code, and other emerging threats and defences.

---

3. PGP in Cybersecurity – Praxis Business School

Praxis Business School is committed to playing a significant role in creating a strong pool of resources who understand the interplay among data, technology and business and can contribute significantly to the exciting Digital Future. Praxis is well known for the quality of the faculty team that it has been able to build. Faculty members with impeccable academic pedigree and enormous industry experience design and deliver programs that are relevant and effective. Thus, Praxis programs have been well received by the industry and the Data Science program has been consistently ranked as one of the top 3 programs in data science in India by prominent publications.
Flagship Cybersecurity Program: PGP in Cybersecurity
Duration Of The Program: 9 months and 525 Hours (It does not include self-study, group discussion, R&D, practice, seminar/workshop, etc.)
Cost of the program: ₹3,00,000
Cities of Operation: Kolkata, India
Course Content And USP Of The Program: On successful completion of the course, the students will learn how to detect a cyber attack and respond during an attacked scenario, identify, assess and mitigate cyber risk, assess the cybersecurity posture of the any enterprise, find technical vulnerabilities of any ICT infrastructure, be a strategist in cybersecurity roadmap creation, identify legal, regulatory and statutory requirements impacting cybersecurity, build a cyber safe IT and OT (Operation Technology) environment, become a digital forensics investigator, conduct cybersecurity audit, and become a compliance manager. All the programs can be done by any individual who has completed their graduation (both three years and four years duration) in engineering, science or any other stream and wants to pursue his/her career in the field of cybersecurity.

---

4. Certified Ethical Hacker and Certified Information System Security Professional – Simplilearn

Simplilearn enables professionals and enterprises to succeed in this fast-changing digital economy. The company provides outcome-based online training across digital technologies and applications such as big data, machine learning, AI, cloud computing, cybersecurity, digital marketing and other emerging technologies. Based out of San Francisco, CA, Raleigh, NC and Bengaluru, India, Simplilearn has helped more than one million professionals and 1,000 companies across 150 countries in getting trained, acquiring certifications, and reaching their business and career goals. The training industry-recognized Simplilearn as a Top 20 IT Training Company for 2017-2019.
Flagship Cybersecurity Program: Certified Ethical Hacker (CEH), andCertified Information System Security Professional (CISSP)
Duration Of The Program: 40 hrs for CEH program, and 32 hrs for CISSP program
Cost Of The Program: ₹35,999 for CEH and ₹24,999 for CISSP.
Cities Of Operation: Bengaluru, Hyderabad, Pune, Mumbai, Gurugram, Noida, Singapore and the US
Course Content And USP Of The Program: The EC-Council Certified Ethical Hacker course verifies your advanced security skill-sets to thrive in the worldwide information security domain. Many IT departments have made CEH certification a compulsory qualification for security-related posts, making it a go-to certification for security professionals. This certification provides learners with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse the learner into a "hacker mindset" to teach how to think like a hacker, and better defend against future attacks. It also offers a hands-on training environment

employing a systematic ethical hacking process. The course covers five phases of ethical hacking, diving into reconnaissance, gaining access, enumeration, maintaining access, and covering your tracks. Simplilearn's CISSP certification training is aligned to the (ISC)² CBK latest requirements. The course trains you in the industry's most recent best practices which will help you pass the exam in the first attempt. The certification helps you develop expertise in defining the architecture and in designing, building, and maintaining a secure business environment for your organization using globally approved Information Security standards.

---

5. PG Diploma/M.Tech in Cybersecurity – Reva University

REVA Academy for Corporate Excellence (RACE), is an initiative of REVA University, which offers a range of specialised, techno-functional programs in emerging technology areas, custom-designed to suit the needs of working professionals to enhance their careers. These programs bring in the latest tools, techniques and skill sets which are in sync with the futuristic demands of the industry. All our programs have a blended learning model with flexible contact classes and a robust online learning management system with 24/7 support.

Flagship Cybersecurity program: PG Diploma/M.Tech in Cybersecurity(Powered by AforeCybersec and in association with IBM).
Duration Of The Program: 12 months PG Diploma and 24 months M.Tech Program
Cost of the program: 12 months PG Diploma is ₹3,50,000 and 24 months M Tech program in ₹4,50,000 lakhs.
Cities Of Operation: Bengaluru
Course content and USP of the program: PG Diploma/M. Tech in cybersecurity is a 12/24 months program in cybersecurity for working professionals that provides in-depth knowledge and skillsets in cybersecurity to monitor, prepare, predict, detect and respond to cyber-attacks and manage enterprise security. This program is designed and delivered by industry experts. It focuses on providing in-depth knowledge and skills on information security, application security, cloud security, identity and access management, vulnerability and penetration testing, incident management, and SOC operations. This program extensively runs on the virtual environment provided by Cyber Range incorporating hyper-realistic emulators, including traffic generators. To enhance the real-time learning, a state-of-the-art, futuristic Security Operations Centre is built at REVA University with the capabilities of Security Analytics and Security Orchestration, Automation and Response (SOAR). The SOC is a 12- seater with four visual displays and has LogRhythm as the SIEM is Python and Spark-based indigenously developed, security analytics platform.

---

6. Post Graduate Diploma in Cybersecurity – Amity Online

Amity University is India's leading research and innovation-driven university. It is recognized by UGC – a statutory body of higher education in India and accredited by National Assessment and Accreditation Council (NAAC) with "A+" Grade. Careers of Tomorrow is an initiative by globally accredited Amity Education Group to offer high-end niche programmes to upskill students and working professionals for future and emerging industry requirements in the Technology space.

Flagship Cybersecurity Program: Post Graduate Diploma in Cybersecurity
Duration Of The Program: 11 months
Cost of the program: ₹1,55,000 (with flexible EMI options)
Cities of Operation: Online – They have students from Bengaluru, Noida, Hyderabad, Chennai, Pune
Course Content And USP Of The Program: Enterprises across the globe are increasingly realizing the vitality of cybersecurity. Amity's Post Graduate Diploma in Cybersecurity will equip you with the skills needed to become an expert in this rapidly growing domain. You will learn a comprehensive approach of securing your IT Infrastructure, building intelligence for threat detection, executing cybersecurity operations, understanding ICS Security, architecting cloud-based security and achieving compliance. Not only will you learn the interdependence of Blockchain, Machine Learning and IoT with Cybersecurity but also you get real-world insights from our leading industry experts. The best-in-class Diploma fosters practical experience by learning in group projects and assignments to help you become a Cybersecurity expert.

---

7. Cybersecurity Certification Course – Edureka

Edureka is a global e-learning platform for live, instructor-led training in trending technologies such as AI, data science, big data, cloud computing, blockchain, and cybersecurity. They offer short term courses supported by online resources, along with 24×7 lifetime support. Edureka has an unwavering commitment to helping working professionals keep up with changing technologies. With an existing learner community of 750,000 in 100+ countries, Edureka's vision is to make learning easy, enjoyable, affordable and accessible to millions of learners across the globe.

Flagship Cybersecurity Program: Cybersecurity Certification Course
Duration Of The Program: 4 weeks (weekend batch)
Cost of the program: ₹14,995
Course content and USP of the program: Edureka's Cybersecurity Certification Course will help learners master the basic concepts of cybersecurity along with the methodologies

that must be practised to ensure information security of an organization. Starting from the Ground level security essentials, this course will lead one through cryptography, computer networks and security, application security, data and endpoint security, idAM (Identity and Access Management), cloud security, cyber-attacks and various security practices for businesses. This course is designed to cover a holistic and a wide variety of foundation topics in cybersecurity which will prepare freshers as well as IT professionals for the next level of choice such as ethical hacking/ audit and compliance / GRC/ Security Architecture and so on. This course is designed as a first step towards learning Cybersecurity.

---

8. Post-Graduation Program in Cybersecurity – IIDT

International Institute of Digital Technologies (IIDT) is an Institute set up under APEITA (Andhra Pradesh Electronics and IT Agency), an autonomous society of the Government of Andhra Pradesh to promote Information Technology and Electronics industry registered under the Andhra Pradesh Societies Registration Act, 2001. The purpose of this unique initiative is to ensure that the student community across India/Globe is empowered with the niche emerging technologies as well as to make the state of Andhra Pradesh a leader in India in establishing this prestigious Institution.

Flagship Cybersecurity Program: Post-Graduation Program in Cybersecurity (PGP)
Duration Of The Program: 11 Months
Cost Of The Program: ₹5,25,000
Cities of Operation: Tirupati and Andhra Pradesh
Course content And USP Of The Program: IIDT has three differentiators:

1. The pedagogy, which is based on academic and industry collaborations for the course content creation as well as delivery
2. The advanced Cyber Range Lab with the creation of Centers of Excellence (CoE), to give deep-digital exposure, through real-life use-cases and projects
3. Global mentor-network, to strengthen the industry exposure to the students

The Govt. of Andhra Pradesh has chosen Gujarat Forensic Sciences University (GFSU) as the Academic Partner to deliver the one-year full-time postgraduate program in cybersecurity at IIDT. GFSU, with expertise in conducting widely acclaimed Cybersecurity program for the past six years, has designed the curriculum, is delivering the program and collaborating with IIDT for placements. IIDT is setting up Cyber Range Lab operational along with 3 Centers of Excellence (COE)'s in collaboration with CISCO, Kii Corporation, T4U.

---

9. Cyber Pro Track – PurpleSynapz

PurpleSynapz is a hyper-realistic research and training lab designed to pave the way for the next-gen cybersecurity professionals. It aims at building the pipeline of cybersecurity talent to dent the shortage of required professionals in India. PurpleSynapz features Modern Curriculum crafted by India's leading infosec practitioners and consultants, Cyber Range, and Innovation Sandbox that focuses on promoting the next-gen cybersecurity entrepreneurs.

Flagship Cybersecurity Program: Cyber Pro Track
Duration Of The Program: 6 Months Classroom-Based Program (Including 2 Months of Hands-on Internship)
Cost Of The Program: ₹3,00,000 + GST
Cities Of Operation: Bengaluru
Course Content And USP Of The Program: Cyber Pro Track is a six-month full-time certification course designed by one of the Industry's leading Infosec practitioners and consultants. The program features a modern curriculum spread in 14+ different modules and a hyper-realistic simulation lab (Cyber Range) that allows participants to fight real-life cyber attacks in a controlled environment. The range offers a catalogue of training scenarios, including incident response, pen-testing, OT security, and individual skill-building. Program Overview includes 14+ modules covering networking, checkpoint, deep packet inspection, firewalls, SIEM, incident response, cyber range and many other latest technologies, along with two months internship, and free access to Cyber Range.

---

10. Certified Information Security Consultant – Institute of Information Security

The Institute of Information Security is one of the most trusted sources of hands-on training in information security, providing excellent unmatched practical training to individuals and corporates around the globe for over a decade. With the backing of our brilliant technical team providing consulting services for the past 18 years under the brand name of Network Intelligence, they are here to train, mentor and support your career in cybersecurity. Keeping in mind the requirements of the industry, our training programs are designed to prepare the candidates/professionals attending our training to meet the challenges they will be facing in real-life situations.

Flagship Cybersecurity Program: Certified Information Security Consultant
Duration Of The Program: 6 months

Cost of the program: ₹1,30,000 + tax for weekday batches, and ₹1,45,000 for weekend batches
Cities Of Operation: Dubai, Mumbai, Pune, Bengaluru, Chandigarh, Delhi, Hyderabad**Course Content And USP Of The Program**: Course content includes fundamentals, network security, coding, server security, web application security, mobile security, digital forensics, and compliance. The CISC training is designed to make you an expert in the domain of cybersecurity. While most certification programs are geared towards purely technical know-how, the CISC also arms you with the necessary consulting skills to help you make your mark in this exciting field. CISC covers a wide variety of topics, starting right from the basics, and then leading up to compliance standards, and even forensics and cybercrime investigations. CISC includes over 45+ sessions, including the fundamentals as well as advanced concepts. These 45+ sessions will be divided into four quarters, all of which will be covered in 6 months. Each session will be further broken down into 15-20 modules.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

A Drone for Any Application

Source: https://i-hls.com/archives/98033

Jan 10 – **What do the agriculture, defense, mapping, and construction industries all have in common?** They all significantly benefit from the use of innovative UAVs. Whether it be heavy duty drones, capable of carrying sprayers and spraying crops with pesticides, or small lightweight drones used for tunnel and pipe inspections in tight, confined places, drones offer a wide range of solutions to a wide range of industries.

A French drone making company is working to capitalize on the world's demand for drones. Drone Volt has been at work developing and manufacturing a wide fleet of drones for a variety of different applications.

One of the company's drones is the Hercules 20 heavy lift drone. Its carbon fiber frame and anodize aluminum fasteners make the drone durable and resistant to various extreme flight conditions. It also allows the drones to carry payloads weighing **up to 20 kilograms**.

The heavy-duty quadcopter is very versatile. The done is fully customizable, so if you're using it to spray your crops, survey areas, or simply lift objects to higher levels in a construction site, you could find a matching payload for the Hercules 20 to help with your task.

The company offers a range of professional payloads and sensors for surveillance, inspection, construction, and agriculture. The drone can be attached with a gyro stabilized gimbal that has both an electro-optic and infrared camera installed. Both cameras have 360 degrees of rotation, with the electro-optic camera offering 30x optical zoom and the infrared camera offering 4x zoom.

Other payloads include a crop sprayer and an electromagnet for lifting.

Going from large to small, the company also offers a mini-UAV for confined spaces inspection. The Inspector drone is a mini professional drone for indoor inspections of extremely confined environments. The drone's small size and protective 360 degrees carbon sphere allows the operator to explore and inspect the tightest places while also reducing risk to humans near the drone.

The Inspector is capable of live video streaming and recording. It comes with powerful LED lights to brighten up dark confined spaces. The drone could also be used for military and police applications. Ideal for search and rescue and hostage situations in confined spaces.

The company also manufactures a fixed wing, VTOL capable UAV, the Heliplane. The Heliplane is hybrid quadcopter-fixed wing UAV with five propellers, four acting as quadcopter propellers and one at the nose, acting as a fixed wing propeller.

The VTOL UAV comes in 3 versions for different types of missions. The first variant comes with a dual camera-thermal sensor used for long range surveillance, ideal for military intelligence gathering.

Another variant of the Heliplane is used for mapping operations as it utilizes a LIDAR sensor for high resolution mapping and 3D modeling.

Finally, the third version of the UAV utilizes Real Time Kinematic measurements for obtaining precise measurements.

EDITOR'S COMMENT: What if we add one word in the first sentence (in red) of this article – "**terrorists**" ???

Heathrow Airport Got 5km-Range Drone Detection

Source: https://i-hls.com/archives/98291

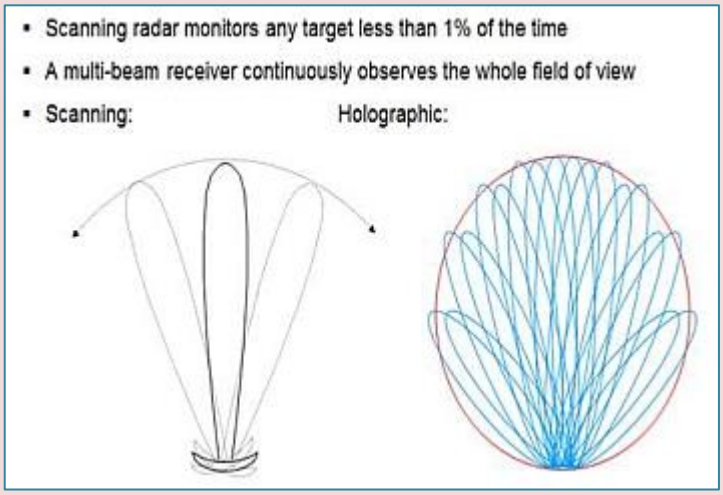
Jan 20 – Illegal drone flights are a growing problem for airports, utilities and factories. London Heathrow Airport has recently deployed a new system aimed at preventing drones from entering its airspace and interrupting operations, following a string of recent attempts that

threatened Europe's busiest travel hub. Heathrow's new detection system is the same one that's already in use at Paris' Charles de Gaulle (CDG) Airport.

Heathrow chose a **holographic radar system** developed by Aveillant, a UK company acquired by Thales SA in 2017. Its technology is now part of the French defense contractor's anti-drone solution, EagleShield.

The system detects and identifies drones when they enter the airspace. The radar system can detect drones as far as **5km away in all directions.** If it detects a drone around the airspace, the airport can then opt to deploy countermeasures. According to bloomberg.com, drone-disabling technology was not part of Thales' contract with Heathrow.

Holographic radars can be deployed in airports to look over specific high-risk areas such as the approach path, or to cover the entire aerodrome and surrounding area to give early warning of any approaching drone. The Holographic radar will improve safety by reducing the risk of an aircraft hitting a drone, and also reduce the potential for serious operational disruption associated with closing a runway after a pilot sighting of a drone.



The Holographic Radar system differs fundamentally from both traditional mechanically scanned radars and from more advanced electronically scanned systems. Holographic Radar forms multiple simultaneous receive beams that fill the illuminated volume. It requires only a very narrow bandwidth, making it very spectrum efficient compared to traditional radars. By dwelling on targets continuously and for long periods, not only is detection performance against multiple targets excellent but a rich data set containing target specific information enables high discrimination performance. The holographic radar can give reliable alerting with low false alarms to a degree not possible using conventional radar, according to Aveillant's website.

In March 2019, legislation took effect that prohibits drones from flying within any Flight Restriction Zone, which extends to 5 km (3.1 miles) from U.K. airports. Drone operators who operate their devices within an airport's perimeter face a prison sentence of up to five years, according to thepointsguy.com.

The introduction of the drone detection technology follows several reports of drones at airports around London, including at Gatwick and Heathrow. In December 2018, Gatwick airport was closed for more than 24 hours around the busy holiday travel season when there were multiple drone sightings near the runway.

New Drone Detection System for Urban Environments

Source: https://i-hls.com/archives/98230

Jan 17 – Drone detection in urban environments in order to minimize risks is a new challenge. Airspace security and defense starts with situational awareness. A new radio frequency sensor expanded capabilities and increased detection range, providing early warning, detection, and classification of drones.

Incorporating an advanced design for urban environments, with a detection range of up to 5 km, the **Dedrone RF-160** offers reliable, actionable analytics of drone activity for organizations to build a threat profile, understand their risk, and begin building resilience in their airspace security program.

It is an upgraded version of the company's the RF-100, and includes new and advanced features such as increased detection range, integrated LTE, etc.

According to suas.com, the system requires **simple installation and fast startup thanks to integrated LTE**. Only needing power supply and a pole, it automatically connects to the Dedrone Cloud via LTE and immediately starts to detect drones. An on-premise server is not required. Users can assess their drone risk quickly and use these insights to act upon drone threats.
A single RF-160 has an average detection range of 1.6 km, and under ideal conditions, up to 5 km for certain drones. This range extends when one or more RF-160s are working together, and even more information on drone activity can be generated when **layering with other detection technologies, including the RF-300, radar, and PTZ-cameras**.
The technology incorporates an advanced design for urban environments: Urban areas have more radio frequency activity from radio communication, televisions, cell phones, GPS, and other technologies. The RF-160 meets the needs of organizations in such environments with a higher potential of RF interference.

Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons

By Zachary Kallenborn and Philipp C. Bleek
Source: https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/

Feb 2019 – Imagine swarms of undersea, surface, and aerial drones hunting submarines hidden in the vastness of the ocean. Or imagine hundreds of airborne drones darting through New York City, seeking out targets and dosing them with nerve agent.
These imaginary scenarios are not yet reality, but they are quickly becoming so.
Drone swarm technology could have a significant impact on every area of military competition, from enhancing supply chains to delivering nuclear bombs. This article examines the implications for chemical, biological, radiological, and nuclear (CBRN) weapons. Some applications are already possible, while others are futuristic, but plausible. Our broader study in the *Nonproliferation Review* on the applications of drone swarms to CBRN weapons offers additional analysis.
Drone swarms offer significant improvements to both nuclear offenses, the ability to successfully deliver a warhead to a target, and defense, the ability to prevent successful

delivery and mitigate consequences. When it comes to chemical and biological weapons, drone swarms can improve both defense and offense, but appear to strongly favor offense by addressing key challenges to delivery. In the future, this could weaken the norms against these weapons and encourage proliferation. U.S. national security agencies should act to combat the threat and take advantage of the opportunities this new technology offers for CBRN weapons.

Military Advantages of Drone Swarms

Precisely defined, drone swarms are "multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, with the platforms and/or weapons autonomously altering their behavior based on communication with one another."

The fact that components of the swarm can communicate with one another makes the swarm different from just a group of individual drones. Communication allows the swarm to adjust behavior in response to real-time information. Drones equipped with cameras and other environmental sensors ("sensor drones") can identify potential targets, environmental hazards, or defenses and relay that information to the rest of the swarm. The swarm may then maneuver to avoid a hazard or defense, or a weapon-equipped drone (an "attack drone") may strike the target or defense. Real-time information collection makes drone swarms well-suited for searching over broad areas for mobile or other hard-to-find units.

But swarming also adds new vulnerabilities. Drone swarms are particularly vulnerable to electronic warfare attacks. Because drone swarms are dependent on drone-to-drone communication, disrupting that signal also disrupts the swarm. As swarms become more sophisticated, they will also be more vulnerable to cyberattack. Adversaries may attempt to hijack the swarm by, for example, feeding it false information, hacking, or generating manipulative environmental signals. Although numerous counter-drone systems are in development, current defenses do not appear sufficient and even promising systems will face scalability challenges, from deployment allocation to training, in the system's use.

Analysts are divided on whether drone swarms offer significant cost benefits. T.X. Hammes has posited in *War on the Rocks* that the future of warfare is "small, smart, and cheap platforms." He highlights swarms of drones as one example, arguing the costs are already low and likely to become lower. But Shmuel Shmuel disagrees, arguing in a skeptical essay that this new technology will be more expensive to operationalize than most think.

Ultimately, the cost and its relevance depend in part on what role the swarm will play and what alternatives are available. Even multimillion-dollar drone swarms can be cost-effective on balance if they meaningfully increase the survivability of more expensive or particularly crucial platforms, such as aircraft carriers or nuclear deterrent forces. Simple, low-cost drones may also fill capability gaps, such as the Marine Corps' interest in small, tactical drones and drone swarms to provide infantry organic close-air-support and reconnaissance.

Nuclear Deterrence

Drone swarm technology has significant implications for both the offensive and defensive sides of the nuclear deterrence equation. Swarms offer new means of defeating traditional nuclear delivery systems — a defensive advantage. They could serve as novel missile defenses, potentially even against hypersonic missiles. Imagine 100,000 cheap, simple drones forming a dome over a high-value target. Any incoming missile, no matter how fast or maneuverable, would likely hit a drone (whether lightweight drones are enough to damage a reentry vehicle or throw it off course is an open question). The same drones could also serve effectively as air mines, colliding with or exploding in the vicinity of incoming bombers. Even small drones can significantly damage airplane wings. This could be especially effective against low-flying bombers because there is less airspace to cover and defenders can use short-range drones. Finally, multi-domain swarms of undersea, surface, and/or aerial drones could search the ocean for adversary submarines. The drones might locate, follow, relay information about, or attack the submarines. They also could draw information from broader sensor networks.

However, drone swarms also offer new means to improve nuclear delivery — that is, nuclear offense. States are already pursuing drone delivery systems for nuclear weapons, and drone swarms can also improve existing nuclear delivery systems without being armed with a nuclear weapon. Just as they may be able to serve as air and missile defenses, drone swarms can be used to defeat, disable, or trick those same defenses. While it's true that air and missile defenses are highly mobile, creating significant challenges for locating and destroying them, drone swarms have the advantage of being able to spread out broadly to search for them. Along the same lines, Israel used drones as decoys to trick Syrian air defenses into believing they were Israeli aircraft. Drone swarms could do the same in larger, more distributed numbers to encourage defenses to hit the drones instead of the delivery systems carrying nuclear, biological, or chemical weapons. Drone swarms would move more effectively as a unit, akin to how groups of actual aircraft would behave.

Swarms may also improve nuclear targeting. Drones can be used to collect information to identify vulnerabilities or previously unknown defenses. Traditional delivery systems such as cruise missiles, while not technically drones, might incorporate drone swarm technology to adjust their approach en route, for instance based on other systems' success or failure in

striking targets. This is especially useful for counterforce strikes against an adversary's military, which hinge on accurate and comprehensive target identification and precise strikes on those targets. Improved targeting is less important for second strikes and countervalue strikes, which target cities and civilians. Additionally, more accurate weapons mean fewer warheads and delivery systems would be needed. Targeting improvements may also lower upkeep or other costs.

In this way, drone swarm technology could make nuclear delivery systems either more or less survivable, depending on who uses the technology and how. Delivery system survivability is critical to nuclear stability. A nuclear threat is less credible if the threatened state believes it can reliably defeat the nuclear system. And on the other hand, if a state believes its nuclear delivery systems can be defeated, it may develop and deploy more nuclear weapons and novel delivery systems, as well as act more aggressively in crises and conflicts. Such concerns underlie Russia's objections to U.S. ballistic missile defenses. This was also a key reason the United States and others have pursued multiple means of delivering nuclear weapons: to ensure nuclear weapons could always survive a first strike.

Will drone swarms ultimately improve nuclear offense more than they would improve nuclear defense? It's unclear. But theoretically, emerging technologies that improve the ability to defeat nuclear weapons are more disruptive to overall nuclear competition than improvements to delivery. Nuclear weapons already inflict such significant damage that delivery improvements are unlikely to fundamentally alter the character of nuclear warfare. If North Korea can significantly deter the United States with a small, simple nuclear arsenal, for instance, delivery systems improvements seem unlikely to alter the fundamental dynamic. Therefore, while drone swarm technology could aid attacking states, the improvements for defenders are likely to matter more.

Chemical and Biological Weapons Proliferation

Drone swarm technology is likely to encourage chemical and biological weapons proliferation and improve the capabilities of states that already possess these weapons. Terrorist organizations are also likely to be interested in the technology, especially more sophisticated actors like the Islamic State, which has already shown interest in drone-based chemical and biological weapons attacks. Drone swarms may also aid counter-proliferation, prevention, and response to a chemical or biological attack, but those applications appear less significant than the offensive applications.

Indeed, swarms have the potential to significantly improve chemical and biological weapons delivery. Sensor drones could collect environmental data to improve targeting, and attack drones could use this information in the timing and positioning for release, target selection, and approach. For example, attack drones may release the agent earlier than planned based on shifts in wind conditions assessed by sensor drones.

Dispersed attacks also allow for more careful targeting. Instead of spraying large masses of agent, drones could search for and target individuals or specific vulnerabilities such as air ventilation systems. This also means the drones would not need to carry as much agent.

Moreover, drone swarms enable the use of combined arms tactics. Some attack drones within the swarm could be equipped with chemical or biological payloads, while others could carry conventional weapons. Chemical or biological attack drones might strike first to force adversary troops into protective gear that inhibits movement, then follow up with conventional strikes. Although combined arms tactics are possible with current delivery systems, drone swarms allow much closer integration between conventional and unconventional weapons.

These improvements in chemical and biological delivery could conceivably weaken both the military and moral justifications for the relative marginalization of weapons in international politics (with some key exceptions). As far as military utility goes, chemical and especially biological weapons are often unreliable modes of attack. Environmental and territorial conditions such as precipitation, wind, humidity, and vegetation reduce the efficacy of the agent, while protective gear may significantly or wholly mitigate the harm they cause. But drone-based environmental sensors could make these weapons much more reliable, while combined arms tactics could mitigate the impact of, or even gain advantage from, adversary use of protective gear.

The moral opposition to chemical and biological weapons has much to do with their indiscriminate nature and the consequential risk of collateral harm. In 1968, wind blew a cloud of VX nerve agent from the Dugway Proving Grounds in Utah into a nearby farm, killing thousands of sheep. Public opposition to the event helped catalyze the Nixon administration's review of the U.S. chemical and biological weapons programs, culminating in an end to the bioweapons program. With improved targeting, including employing drone-based environmental sensors, it's possible to imagine less error-prone, more discriminate chemical and biological weapon delivery systems that might be less morally objectionable.

Of course, just because these weapons are more usable does not necessarily mean they will reemerge. Modern chemical and biological weapons emerged in a different security environment. Various international laws may constrain rearmament and significant usage, as might popular opinion or political leadership. Still, it's worth considering how advances in technology could make previously indiscriminate weapons more discriminate.

At the same time, drone swarms may also help prevent and respond to chemical and biological weapon attacks. Drone swarms could aid counter-proliferation efforts by, for example, coordinating searches for previously unknown chemical and biological facilities to secure stockpiles after a war. They could similarly coordinate searches along national borders to identify potential smuggling activity, including CBRN material smuggling, or searches through cities to search for gaseous plumes. Notably, swarms could serve as mobile platforms for chemical or biological detectors with different types of sensors to mitigate false positives. If an attack is successful, drones could coordinate mapping of affected areas to help guide responders. Drones could even have sprayers to help clean up after an attack, without risking harm to humans. But given the rarity of chemical and biological weapons attacks and the technical uncertainty of creating reliable, drone-based CBRN detectors, these applications appear less significant than the improvements to offensive capabilities.

Conclusion

How should the United States government address this still-nascent threat? Several agencies have clear equities in this area and should consider how to respond to the technology's emergence.

First, the Commerce Department's Bureau of Industry and Security should adopt new rules restricting the export of swarming-capable drones and related technologies. These rules should especially focus on technology with the potential to improve chemical and biological weapons delivery.

The Defense Department should expand its ongoing research and development into drone swarms to include CBRN-relevant uses. Current DoD research appears to focus on fundamental drone swarm capabilities, but not CBRN-specific applications. The department should also conduct red-team analysis to identify in which that drone swarms could support adversary capabilities in this area, especially chemical and biological weapons delivery.

The Department of Homeland Security should fund research and development into drone swarms for CBRN detection and response. This research should focus on three separate, but related lines of research: detectors, decontaminators, and platforms. Detectors and decontamination systems need to be small enough to effectively mounted on small drones. Drone swarm platforms need to effectively coordinate actions when broadly dispersed and require control systems for detectors and decontaminators.

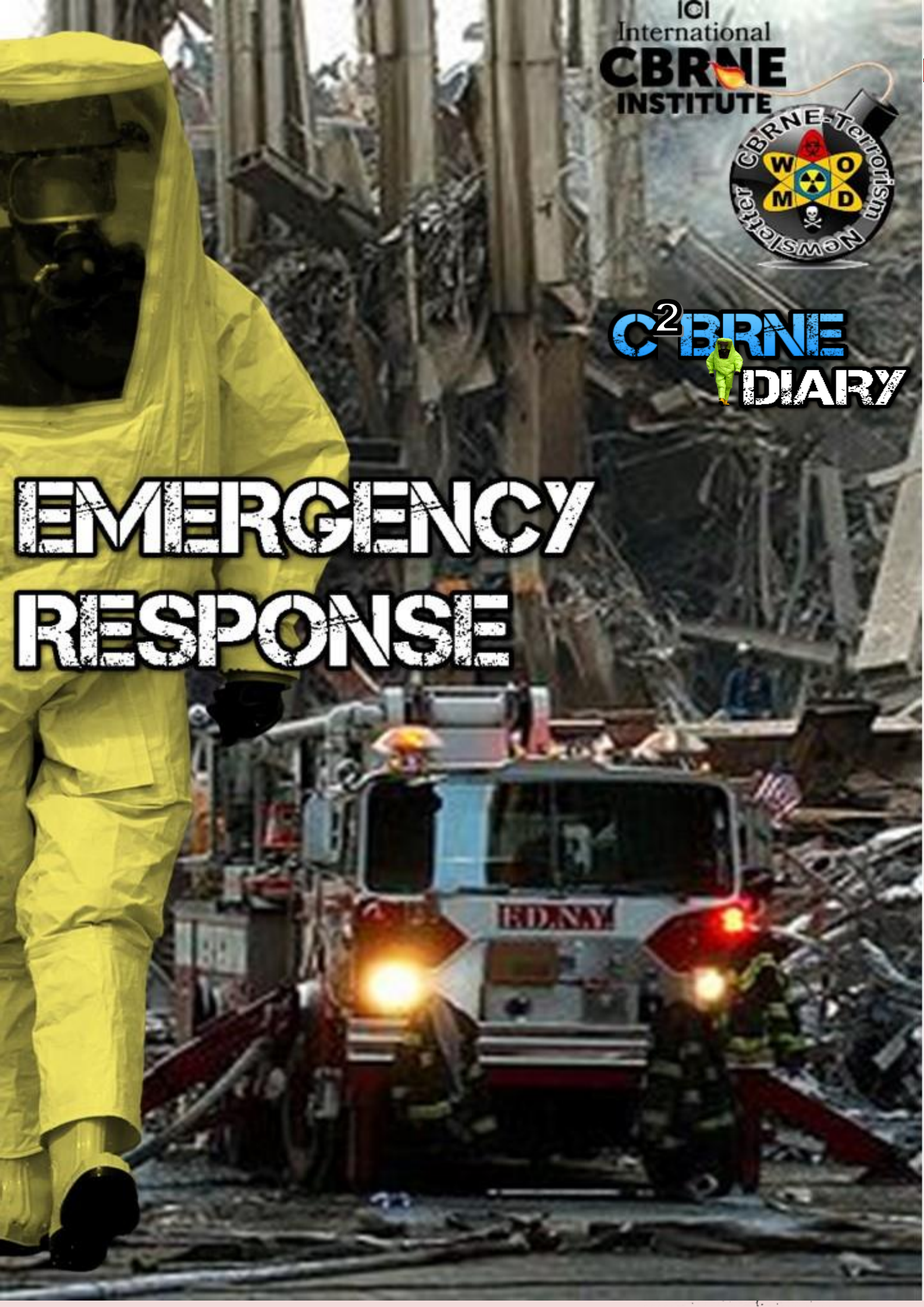
The State Department should evaluate whether and to what extent existing international treaties are sufficient to discourage proliferation of CBRN-relevant drone swarm technology. Particularly, the department should consider whether and how to account for swarming technology in the Missile Technology Control Regime, which restricts individual drones.

Lastly, the intelligence community should collect information on adversaries' interests in and experimentation with drone swarms, including those related to CBRN. The potential applications of drone swarms are extremely broad, and adversaries may identify novel, disruptive applications. The intelligence community should pay particular attention to China's drone swarm research, as the Chinese have shown considerable interest in the technology.

As the technology underlying drone swarms matures and spreads, the barriers to entry will almost inevitably fall. After all, when reading about drones in 2010, how many readers would have thought that an organization such as Islamic State would have mounted hundreds of drone attacks in a single month or that commercial drones would shut down airports?

Zachary Kallenborn *is an independent national security researcher/analyst specializing in CBRN terrorism, CBRN weapons, radical environmental terrorism, and drone swarms. His work has been published in Studies in Conflict and Terrorism, the Nonproliferation Review, Modern War Institute at West Point, Defense One, and other outlets.*

Philipp C. Bleek *is an Associate Professor in and Acting Program Chair of the Nonproliferation and Terrorism Studies Program, and a Fellow at the James Martin Center for Nonproliferation Studies, both at the Middlebury Institute of International Studies at Monterey. He previously served as Senior Advisor to the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs. Kallenborn and Bleek are the authors of "Swarming Destruction: Drone Swarms and CBRN Weapons" in the Nonproliferation Review.*


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE

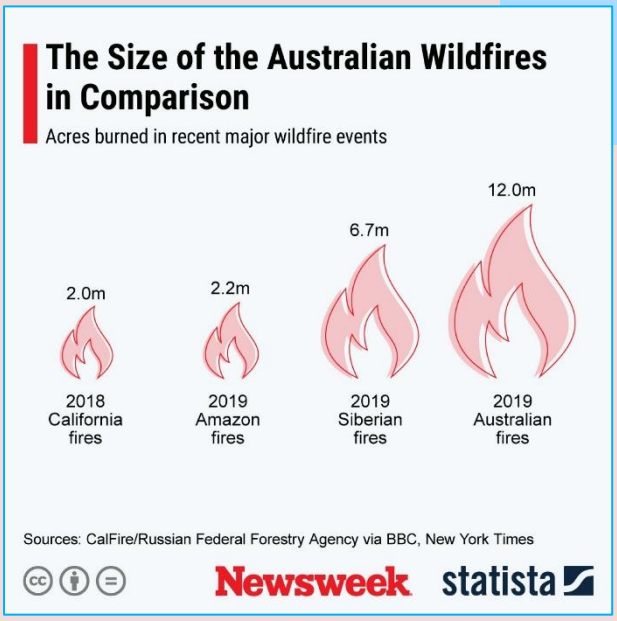
The Lessons from Australia's Fires

Source: http://www.homelandsecuritynewswire.com/dr20200114-the-lessons-from-australia-s-fires

Jan 14 – The *Economist* writes that "You might think that Australia is particularly vulnerable to forest fires. But that would be a mistake. Many other countries share the same conditions that have set Australia ablaze, physically and politically, including similar terrain and a leadership that has yet to wake up fully to the new reality that climate change is creating."

Worldwide, fire seasons are getting longer and more damaging. The *Economist* notes that the areas at risk include America's west coast, the Mediterranean, southern Africa and swathes of Central Asia. If that sounds alarmist, remember that in 2018 California had the deadliest forest fires in its history, killing more than 80 people and causing parts of Los Angeles to be evacuated, while more than 100 people died in wildfires in Greece.

As a result, the lessons from Australia's tragedy are important. One is that climate change is making infernos more likely. It is true that forest fires are a long-standing part of some territories' ecology. But as the world gets hotter and drier, their incidence and severity are rising. In 2019 Australia's mean temperature was the highest since records began in 1910, 1.5°C above the long-run average. The amount of rainfall, meanwhile, was 40% below the long-term average and at the lowest level since 1900. For at least a decade climate models, sometimes derided by sceptics, have accurately predicted worsening droughts and infernos in Australia.



....

The last lesson is that, as the costs of climate change stop being just about abstract temperature forecasts and start being something you can smell in your nostrils, the politics surrounding it will change, too.

The next mega disasters that could happen at any moment (and kill us all)

Source: https://www.foxnews.com/science/the-next-mega-disasters-that-could-happen-at-any-moment-and-kill-us-all

From supervolcanoes to mile-wide asteroids, here's a look at potential mega disasters that could happen at any moment and devastate life on Earth.

As wildfires so hot that images can be seen from space ravage Australia — creating toxic smoke that clogs the country's major cities, killing over 25 people, burning 18 million acres and slaughtering up to a billion animals — many around the globe are wondering what catastrophe is next?

Due to climate change, human activity and other factors, "natural" disasters are becoming more common. But some could be worse than others …

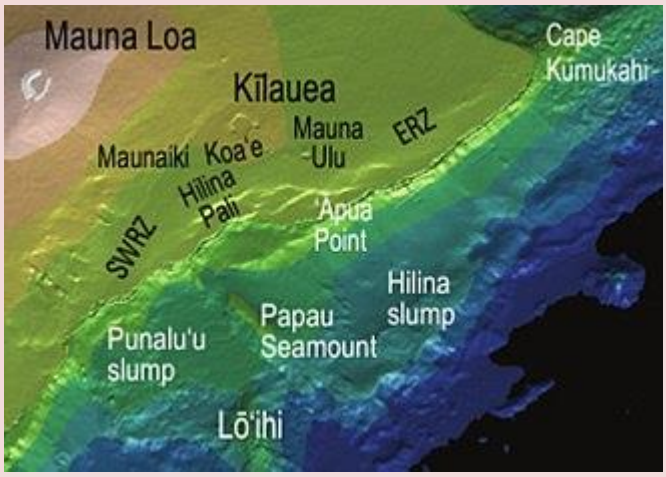
The eruption of the Yellowstone supervolcano

Yellowstone National Park quietly sits on top of a supervolcano that is 44 miles wide. Even scarier, it's still active and could blow at any time. Its last big eruption was 630,000 years

ago, but as "End Times" author Bryan Walsh wrote in an op-ed in The New York Times, an eruption of this supervolcano "would be like nothing humanity has ever seen" and be an "ultra-catastrophe" that "could lead to global devastation, even human extinction. … There will probably never be a year in which no one dies in an aviation accident, but there will definitely never be a year in which 10% of the global population dies in a single plane crash. Yet that could happen with a supervolcano." Walsh wrote. As it's located in America, we'd be the first to go.

The Lake Toba supervolcano, on the Indonesian island of Sumatra

The land of volcanos, Indonesia is no stranger to eruption — with Mount Merapi last exploding in 2018. But there's a bigger threat to the countries of Southeast Asia: The Lake Toba Supervolcano — the "forgotten volcano." Lake Toba is a volcanic lake that sits on top of a huge caldera (a volcanic crater) — which is still considered to be in a stage of "resurgence." An eruption 75,000 years ago caused a "bottleneck" effect in human development — in which the world's population dramatically shrank — according to scientists. Conspiracy theorists say this could happen again. To add salt to the wound, as it lies in an island country, any major eruption would also likely cause a mega-tsunami.



The Hilina slump

On the south slope of Hawaii's Big Island lies the infamous Hilina Slump — where every now and then there is a landslide that creates horrid tsunamis. According to The Independent, "there is evidence that a similar collapse at nearby Mauna Loa around 120,000 years ago generated a tsunami with a run-up height of over 400 meters. Even as recently as 1975, movement of the Hilina Slump generated a smaller, yet destructive tsunami that reached California."

Mega hurricanes

Hurricanes Irene, Katrina, Wilma and Sandy did a number on the East and Gulf Coasts of America, causing billions of dollars in damages and claiming countless lives. To make matters worse, due to climate change, the frequency of these monster storms is expected to increase. Once a phenomenon that happened only every so often, they now occur almost every year — with worsening consequences. As coastal cities grow, the devastation is expected to increase and Science Focus cites them as one the "next big natural disasters."

The Big One in California, Oregon and Washington

The San Andreas Fault has caused havoc and devastation in the past — and it's predicted to do so again. The United States Geological Survey has increased the probability of the likelihood of a magnitude 8.0 or larger earthquake hitting California within the next few decades — and let's not forget the volatile Cascadia Subduction Zone that covers most of Oregon and Washington state. Due to massive population increases in these states over the last decade — and a love of highrises in their major cities — when the Big One hits, it's going to be bad. Real bad.

A Chilean 'Megathrust'

Another West Coast earthquake disaster waiting to happen is in Chile, on the west coast of South America. According to volcanologist website Temblor, "it is clear to many of us that the Coquimbo region [in central Chile] has an unusual, increasing seismicity that may be preparing the area for a very large earthquake near the end of the present century." As with the North American quake, scientists also predict the Megathrust would be accompanied by a devastating tsunami.

Rising oceans

As arctic glaciers melt at alarming speeds, scientists have predicted that "some 150 million people are now living on land that will be below the high-tide line by midcentury," according to The New York Times. Major population areas affected by this direct result of climate change are the East and West Coasts of America, China, Thailand and almost the entire country of Vietnam. The Maldives, an island nation in the Arabian Sea, are also under serious threat as the country comprised of low lying islands is predicted to disappear entirely by 2045.

Caribbean tsunami

An unstable volcano in the Canary Islands, located off the northwestern coast of Africa, is directly threatening most of the Caribbean. According to the BBC: "Dr. Simon Day, of the

Benfield Greig Hazard Research Centre at University College London, UK, believes one flank of the Cumbre Vieja volcano on the island of La Palma, in the Canaries archipelago, is unstable and could plunge into the ocean." This is expected to cause a mega tsunami which would wipe out the many island nations.

Major solar storm

In 2012, Earth narrowly missed being hit by a massive solar storm — the most powerful in over 150 years. The last major incident was in 1859, which created "intense geomagnetic storms (and causing) global telegraph lines to spark, setting fire to some telegraph offices and thus disabling the 'Victorian Internet,'" according to NASA. Daniel Baker, of the University of Colorado, told the organization's website, "In my view, the July 2012 storm was in all respects at least as strong as the 1859 event. The only difference is, it missed. … If it had hit, we would still be picking up the pieces." A similar storm would be "catastrophic" — wiping out the internet and almost all communications — and cause trillions in damages.

Asteroid hits Earth

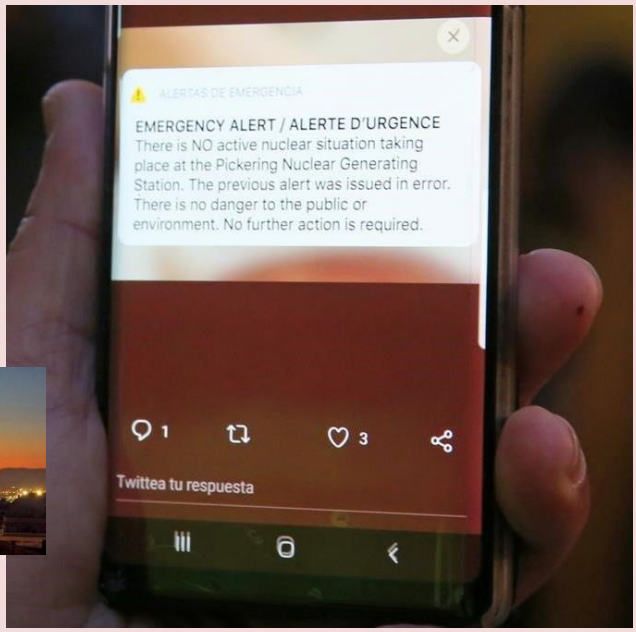
However, the dinosaurs died — they're gone — and many scientists attribute this extinction to an asteroid striking the earth. If one were to hit us today, it would have similarly devastating effects. According to How Stuff Works, "In 2028, the asteroid 1997XF11 will come extremely close to Earth but will miss the planet. If something were to change and it did hit Earth, what you would have is a mile-wide asteroid striking the planet's surface at about 30,000 mph. An asteroid that big traveling at that speed has the energy roughly equal to a 1 million megaton bomb. It's very likely that an asteroid like this would wipe out most of the life on the planet."

Contagion

It used to be communicable diseases were contained by natural borders of rivers, oceans and mountains. But in the modern age, airplanes have caused these natural borders to become moot. Due to porous borders and airports, the Ebola epidemic of 2014 wiped out as many as 12,000 people and spread to several continents within months. This week, the Coronavirus that originated in China spread to Japan and Thailand. While the world is getting better at containing these outbreaks, it's only a matter of time before one break through and causes global devastation.

Spain finalizes mass emergency plan for acts of terrorism, mass murders, natural disasters and explosions

Source: https://www.euroweeklynews.com/2020/01/18/spain-finalises-mass-emergency-warnings-for-acts-of-terrorism-mass-murders-natural-disasters-and-explosions/#.XidIQiPQDIU



Jan 18 – In the event of a serious incident taking place in Spain, the Government and Civil Protection Unit are finalizing the roll-out of a mass warning system. This will alert people of the danger posed in a specific area and the actions that should be taken to ensure their safety.

Sources close to the Ministry indicate that data will be collected from telephone providers where in the case of an emergency, an alert will be sent through SMS to mobile phones. This would include situations such as acts of terrorism, bombs, chemical explosions and mass murders.

Texts with messages such as '*Detected chemical accident in XX. Stay at home with the windows closed until further notice*' would be received by registered mobile phone users shortly after the incident occurs.

The innovative emergency alert system is already used in European countries such as the Netherlands and Belgium as well as in Japan, the United States and Canada.

Currently, Spain uses a siren system, however much criticism was made on its application after the chemical explosion took place in La Canonja, Tarragona earlier this week. It has

transpired that no warnings or alerts were made to the surrounding community, leaving many unaware of the serious dangers posed in the area.
Miquel Buch, the Minister of Interior condemned the non-activation of the sirens after the chemical emergency, calling on the government to accelerate the implementation of the new warning system. He stated that the new warnings will be very useful in cases such as a natural disaster, terrorist attacks or nuclear explosions.
It is understood that Movistar and Vodafone have already met with state technicians, where the new system will allow messages to be sent out to individuals in a specific area provided that they have signal.
The new mass alert system will be in operation by June 2022 and within that time work will be carried out to ensure its compliance with the European Code of Electronic Communications. It will also be approved by the Congress of Deputies, according to sources from the Secretary of State for Telecommunications.

Lessons Learned From an 'Almost' Evacuation

Source: https://www.domesticpreparedness.com/healthcare/lessons-learned-from-an-almost-evacuation/

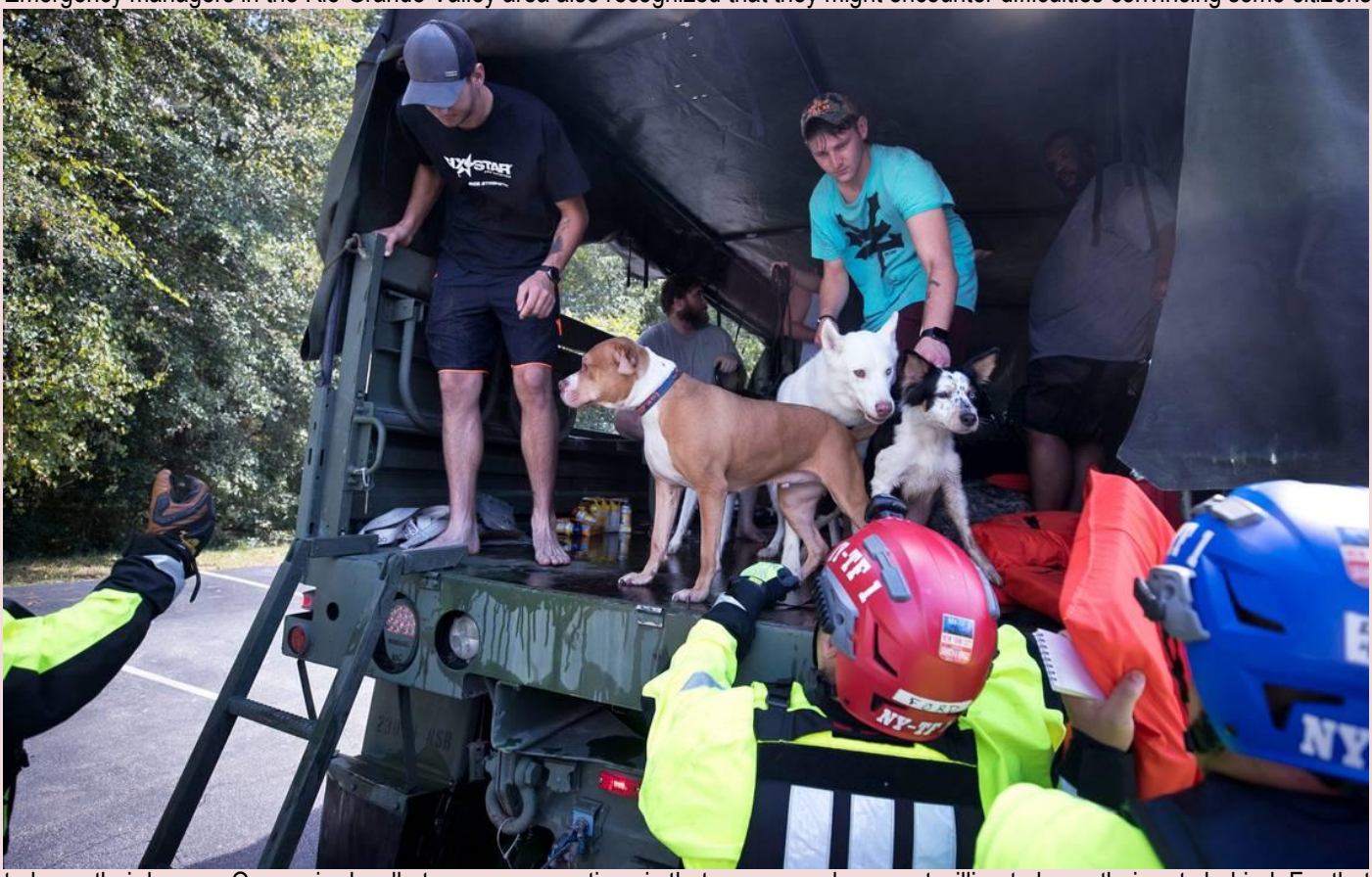
June 2010 – In August 2007, Hurricane Dean gathered strength in the Gulf of Mexico and aimed for the southern coast of Texas. Although the hurricane later changed course and made landfall in Mexico, authorities predicted that Texas could still be hit hard by heavy rains, storm surge, and, possibly, coastal flooding. Before Dean made landfall, President George W. Bush issued an emergency declaration for 32 Texas counties; the presidential order triggered the greatest mobilization of emergency resources in the state's history. Since Hurricane Dean skirted Texas, however, no mass-evacuation order of similar magnitude has been necessary.

Despite the lack of an actual evacuation order, many if not quite all of the state's emergency managers have put their evacuation plans into effect at least once – and have learned several valuable lessons from the potential shortcomings in those plans. The *2007 Hurricane Dean After-Action Report*, developed by the State of Texas Governor's Division of Emergency Management – and available on *Lessons Learned Information Sharing* (LLIS.gov) – details the mobilization efforts carried out throughout the responding regions.
In the Rio Grande Valley, for example, emergency managers took steps to safely evacuate a large number of area residents (and some visitors, of course). Responders were deployed to staging areas, and receiving points, to await the evacuation order – which, unfortunately, did not include enough of the supplies and other resources necessary (e.g., food and sleeping facilities) to support a team of responders during an extended deployment. Because responders stayed longer than expected while waiting for the evacuation order, the supplies at the receiving areas and staging points were severely taxed. The after-action report mentioned above recommends that emergency managers stock receiving areas and staging points in quantities sufficient to accommodate extended deployments, especially when responders' schedules are unpredictable.

Dogs, Cats, Building Materials & Other Impedimenta

As the evacuation plans proceeded, the Texas Department of Transportation assured emergency managers in the Rio Grande Valley District's Disaster Center that all construction materials on planned evacuation routes would be removed. As it turned out, although much of the construction materials were in fact cleared, especially in the Alamo area, not *all* routes were cleared. To resolve a repetition of this problem the after-action report recommends that the State Department of Transportation continually review infrastructure improvements to quickly identify and clear construction-related impediments to traffic flow in times of an actual or potential disaster. The report also recommends that all road work should stop – preferably at least 72 hours before the onset of a severe storm that could require evacuation.

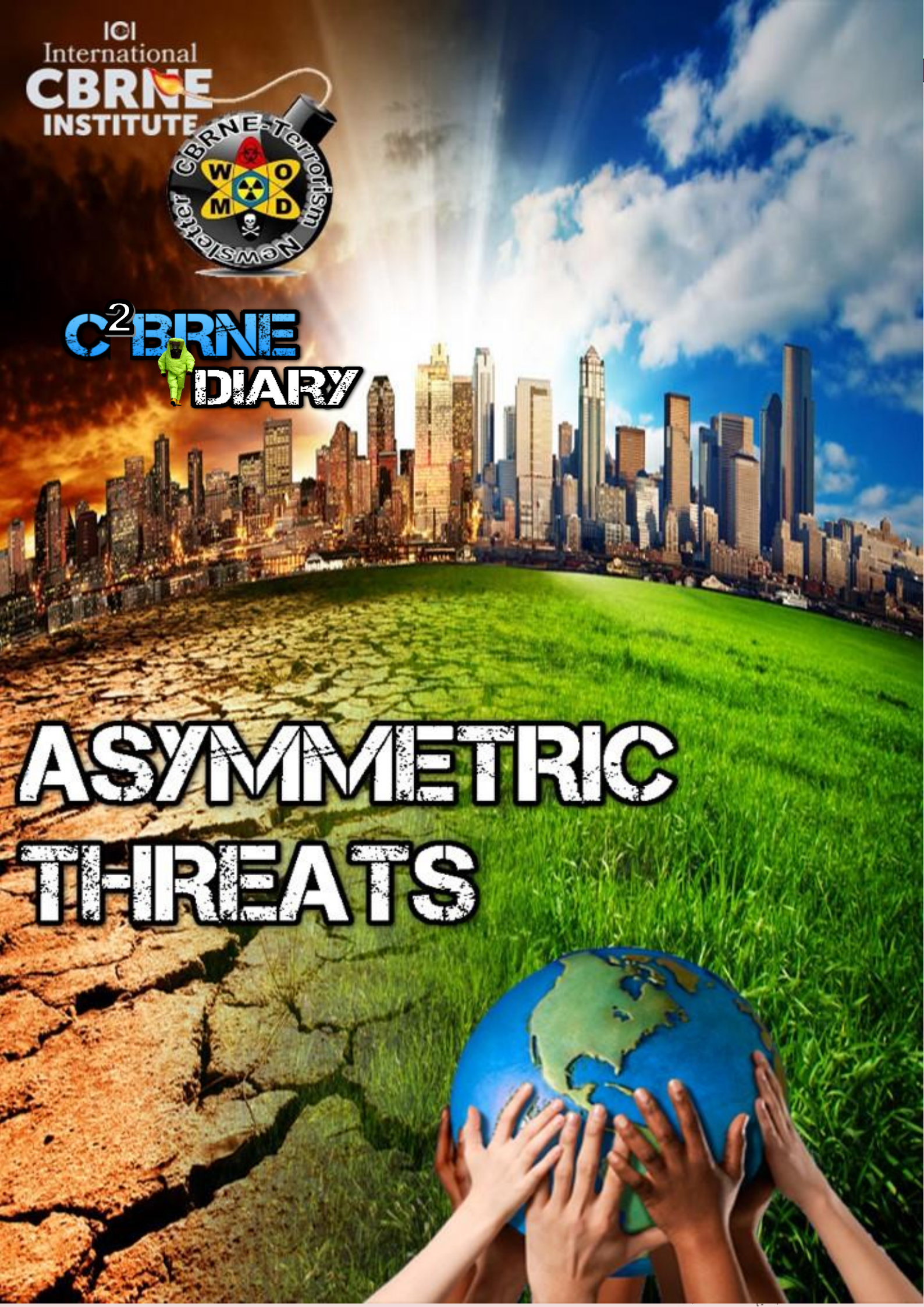
Emergency managers in the Rio Grande Valley area also recognized that they might encounter difficulties convincing some citizens



to leave their homes. One major hurdle to mass evacuations is that many people are not willing to leave their pets behind. For that reason, the Pets Evacuation and Transportation Standards Act of 2006 (also available on LLIS.gov), requires states and local communities to include accommodations for pets and service animals in their evacuation plans.

To meet that requirement, public information campaigns in the Rio Grande Valley area encouraged pet owners to help prepare for disasters by purchasing the muzzles and/or carriers needed to transport the pets safely – but emergency managers still expected, reasonably enough, to have to provide many of those necessities. However, when preparing for Hurricane Dean, planners belatedly realized that most if not all local pet stores did not have enough of those items, and other pet supplies, needed to accommodate a mass evacuation. Had an evacuation been required, therefore, the lack of available ways to safely transport pets would have caused difficulties for the emergency responders themselves. To remedy this problem, the after-action report recommends that emergency managers collaborate with private-sector and/or non-profit pet advocacy groups *before* a disaster strikes to arrange for muzzles, pet carriers, and other supplies to be distributed at the pre-determined evacuation hubs.

Although no actual evacuation was necessary in the Rio Grande Valley during Hurricane Dean, the emergency managers documented their evacuation preparations in the *2007 Hurricane Dean After-Action Report* so that other jurisdictions could learn from their experiences. The report discusses those and other lessons in further detail.


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

Asymmetric Warfare

By Raashid Wali Janjua

Source: https://pakobserver.net/asymmetric-warfare/

Dec 24 – He plays a game with which I am not familiar (Bobby Jones) This quote by Booby Jones about Jack Nicklaus' Golf skills encapsulates the whole philosophy of Asymmetric warfare. Several writers nowadays are confusing the terms like fourth, fifth and hybrid Warfare. The United States Joint Forces Command defines a hybrid threat as, any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space. Rather than a single entity, a hybrid threat or challenger may be a combination of state and non-state actors. As per European Centre of Excellence for Countering Hybrid Threats, hybrid threats are methods and activities that are targeted towards vulnerabilities of the opponent where the range of methods and activities is wide including terrorism, lawfare, political subversion and media manipulation.

The fourth generation warfare is defined as an irregular warfare waged by non-state actors against nation states employing irregular tactics. The fifth-generation warfare is based on space age technologies and artificial intelligence employing hi tech weaponry, robotics and unmanned information technology enabled platforms. The fourth generation and hybrid warfare are of essence the same. The Chinese called that the "Unrestricted Warfare" which sometimes is coterminous with the nonlinear warfare. The hybrid or the unrestricted warfare employs all elements of a nation's power potential to leverage an advantage upon a truculent adversary. Dislocation of an enemy's conventional or unconventional force balance to uncover the vulnerability to be attacked is the first logical step followed by an attack on enemy's center of gravity in the repertoires of two adversaries' Grand Strategy.

The soul of all these non-linear strategies and tactics is the Asymmetric Warfare. It is a kind of warfare where a weaker adversary uses tactics, stratagems, and weapon systems that render a stronger adversary's strengths infructuous. Martin Van Creveld called the modern warfare as the province of "unarmed yet unharmed adversary" that uses the very strength of a stronger adversary as its weakness. The decimation of three Roman legions led by Publius Quinctilius Varus in 6 A.D. at the Teutoburg forest by a Germanic tribes' leader Arminius is a classic example of Asymmetric Warfare. Three Roman legions were completely destroyed through an ambush by the lightly armed yet agile Germanic troops who took full advantage of the lack of maneuverability of heavily armed Roman legions in the wooded territory. Another example is the Ali versus George Foreman world heavy weight bout in Congo where Ali used the ropes in ring to absorb the punches.

The mad fury of Foreman's punches was spent like a water current crashing against the rocks. As Foreman tired himself out Ali counter attacked knocking him out. Hybrid Warfare is in fact an "Asymmetric War" that is waged by a state or a non-state actor against a state or a non-state actor. Its scope therefore is limitless and unbounded. When the Chinese use this term, they mean use of all elements of a nation's power potential especially the ones with a comparative advantage over the adversary to render the strengths of an adversary useless. The guerillas using hit and run tactics, the terrorists resorting to terrorism, the intelligence agencies subverting the loyalties and fomenting unrest amongst rivals' social units, and the armies resorting to low tech weaponry to render the cyber war capabilities of adversaries irrelevant are all examples of Asymmetric Warfare. After the nuclear revolution according to Lawrence Freedman and Martin Van Creveld the non -Trinitarian was the new normal.

The Clausewitzean trinity of government, people and the army were replaced by a conflict featuring people and governments as conventional armies receded in background because of the increased irrelevance of the conventional forces due to nuclear balance of terror. In this new warfare system, the asymmetric warriors can operate from the anonymity of their hideouts using cyber as well as information war tools. All over the world in areas covered by the nuclear umbrella the asymmetric warfare employing a hybrid of conventional, sub conventional and unconventional threats have become the norm. Weapons of mass destruction have assumed the status of deux ex machina in contemporary warfare. These have given weak states and non-state actors a hitherto unknown power to inflict grievous damage on stronger adversaries.

The forms of asymmetry include asymmetry of operational thoughts, technology, will and organization. Out of the three forms mentioned above the asymmetry of the will is the most important aspect. In Afghanistan for example the Americans despite obtaining the clear edge in technology and operational thoughts lost badly on the will power front. A badly organized and poorly equipped Afghan Taliban led indigenous resistance is apparently getting the better of the US war machine due to a wide gulf between the will of the Americans and the Taliban. According to the theory propounded by TV. Paul the weak states initiate asymmetric conflicts against superior adversaries based upon four factors, i.e., strategic calculations of cost/benefit, alliance relationship with global powers, acquisition of offensive weapons and domestic political power changes Egypt's

attack against Israel in 1973 and Pakistan's Operation Gibraltar in 1965 can be included in the asymmetric war category wherein Egypt and Pakistan having acquired modern weaponry and international support successfully prosecuted asymmetric wars. The lesson for Pakistan to heed is to to enhance its asymmetric warfare capacity to succeed whenever the opportunity meets preparation in future.

Raashid Wali Janjua is a retired Brigadier and a PhD scholar at NUST, Islamabad.

A MUST-READ DOCUMENT

Millennium Challenge 2002

Millennium Challenge 2002 (MC02) was a major **war game exercise** conducted by the United States Armed Forces in mid-2002. The exercise, which ran from 24 July to 15 August and cost US$250 million (equivalent to about $355M in 2019), involved both live exercises and computer simulations. MC02 was meant to be a test of future military "transformation"—a transition toward new technologies that enable network-centric warfare and provide more effective command and control of current and future weaponry and tactics. The simulated combatants were the United States, referred to as "Blue", and an unknown adversary in the Middle East, "Red", with many lines of evidence pointing at Iran as the red side.

When the Blue Forces issued a surrender ultimatum, **Van Riper** commanding the Red Forces, turned them down. Since the Bush Doctrine of the period included preemptive strikes against perceived enemies, Van Riper knew the Blue Forces would be cominfor him. And they did.

But the three-star general didn't spend 41 years in the Marine Corps by being timid. As soon as the Navy was beyond the point of no return, he hit them and hit them hard. Missiles from land-based units, civilian boats, and low-flying planes tore through the fleet as explosive-ladened speedboats decimated the Navy using suicide tactics. His code to initiate the attack was a coded message sent from the minarets of mosques at the call to prayer.

In less than ten minutes, the whole thing was over and Lt. Gen. Paul Van Riper was victorious.

▶▶ **Read the full report of this unique strategic experiment, here.**

EDITOR'S COMMENT: Despite its size (~700 pages) this report is worth reading and studying! It is the epitomy of asymmetric warfare and can be easily materialized in turbulent modern times (e.g. in SE Mediterranean area). Thinking out of the box it might be the privilege of very few people but learning from the past and implement related solutions is something that even ordinary people can do! Of course, if the box is empty, then history will repeat itself …