C2BRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

January 2019

New year

New challenges

New threats

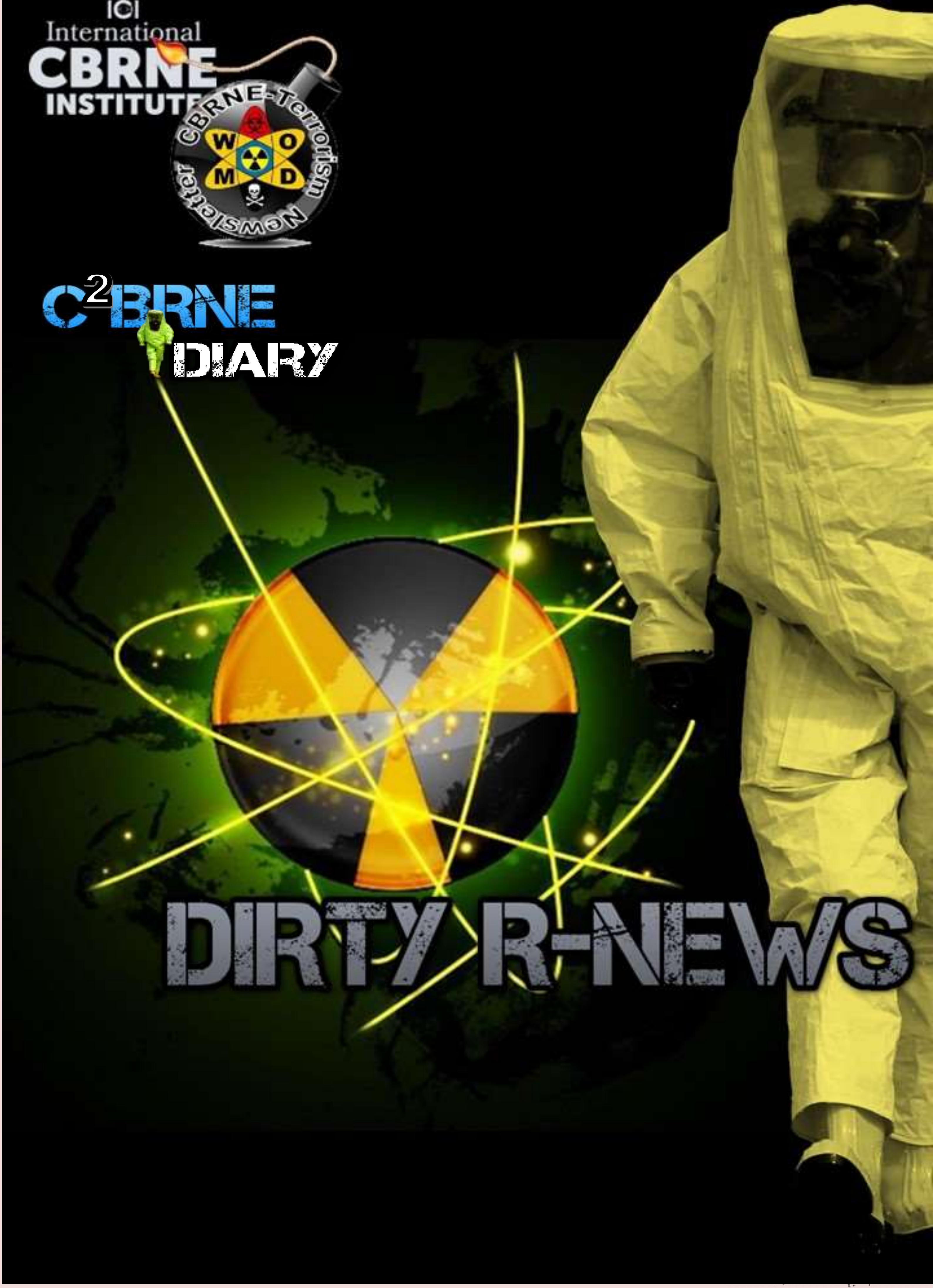
Preserve peace

www.cbrne-terrorism-newsletter.com

ICI
International
CBRNE
INSTITUTE

CBRNE-Terrorism Newsletter

C^2BRNE
DIARY



DIRTY R-NEWS

What Must Be Done Now to Prepare for EMP Strike

By Jack Thomas Tomarchio

Source: https://www.hstoday.us/subject-matter-areas/wmd/perspective-what-must-be-done-emp/

May 2018 – One of the last meetings I had in office was with three scientists from the Commission to Assess the Threat to the United States from Electromagnetic Attack. As they briefed me about the threat and impact of an electromagnetic pulse ("EMP") attack upon our country, it was clear these were desperate men. Working under a 2001 congressional mandate, these scientists were making the rounds at various three-letter agencies sounding a tocsin of warning about the catastrophic consequences of the little-known and poorly understood threat of an EMP attack against our nation.

An EMP is created by the detonation of a nuclear payload in the upper Earth atmosphere. That changes the atomic makeup of oxygen and nitrogen molecules. The electrons released from these molecules as a result of a nuclear explosion can cause a magnetic pulse that produces voltage surges in electric devices that will disable them permanently. In essence, an EMP can, in a nanosecond, fry the insides of most electrical appliances and other electrically powered machines, rendering them permanently useless. What that means to societies thousands of miles from ground zero is a total disruption of electric power from power plants to handheld devices.

EMP events can also occur naturally from changes in the sun's thermal activity. Whether caused naturally by the sun or artificially by the detonation of a nuclear warhead on an intercontinental ballistic missile, the results can be a veritable game-changer for society.

My guests that day educated me on the threat, the impact of a successful EMP attack on our wired society, and what our government was doing to combat the problem. Their discussion of the former topic was detailed and insightful. Their discussion of the latter topic, U.S. response planning for the threat, was brief and alarming. Indeed, what the U.S. was doing to prepare for this threat could be summed up in two words: not much. From the time I had my introduction to the EMP threat in 2008 until today, the United States has remained practically and negligently unprepared to deal with the challenge.

These were desperate men.

For a time, there was some talk that an enemy like North Korea could fire a crude nuclear warhead launched from a submarine in the South Pacific over the southwestern United States and detonate it in the upper atmosphere with the desired effect of eliminating a good portion of our power grid west of the Rockies. Since the North Koreans had yet to perfect a nuclear weapon that could survive re-entry, all they would need to do would be to send it high, detonate it, and let the so-called games begin.

Recent rumors of *rapprochement* with Kim Jong-un's Democratic Republic of North Korea may make that scenario unlikely, but there are still other would-be malefactors who could attempt an attack such as a re-embargoed and nuclear-aspirant Iran. Even if the genesis of an EMP attack is not man-made, but purely a solar phenomenon, the fact remains that our nation is not prepared to address the ramifications of such an attack upon the homeland.

With our nation now inextricably wired at every level, an EMP attack could bring our critical infrastructure to a crashing halt: disconnect us from our computers, cell phones and handheld devices, disable our air traffic control system, cripple our banking and financial system, and paralyze our hospitals, schools and emergency services. The result would be to shut down society as we know it, throwing the country into a pre-Industrial Age dystopian gloom.

Since the day I met with those desperate scientists in 2008, little has changed; they are still desperate. What can and must happen is for the country to become more aware of the threat and to take needed action that will address the problem. What can be done? First, the public needs to be made aware that the dreaded nuclear winter can come just as easily via a low-tech EMP explosion or a solar hiccup as it can from a full-blown nuclear war. Indeed, public awareness of the threat is low with most Americans totally ignorant of it.

The FBI, to its credit, engaged the EMP issue in 2011 by instituting an InfraGard EMP Special Interest Group within its larger InfraGard program. That program seeks to build partnerships between the Bureau and private industry to address various critical infrastructure challenges relating to homeland security. InfraGard's EMP Special Interest Group's work is a step in the right direction, but other than sponsoring a few conferences, the last one in 2014, not much has resulted. Where the InfraGard public-private partnership needs to concentrate its efforts is on Capitol Hill, where more engagement with members of Congress to educate them on the threat is imperative.

Raising public awareness will also kick-start discussion of palliative measures that can be followed to mitigate the impact of an EMP strike. One such measure overdue for discussion is to consider taking critical assets such as military bases and emergency services off the grid. Introducing solar power, wind and geothermal power sources where practical at military bases would ensure that these key facilities would remain up and running should an EMP attack occur.

Another action that needs to be taken now is to increase information-sharing on the EMP threat with state and local governments and the private sector. Just as state and local governments were "read into" counter-terrorism intelligence after the 9/11 attacks, so too should the federal government build up a series of information-sharing protocols with states, cities and private industry on the EMP threat. This isn't rocket science, as most of the work has already been trailblazed by the U.S. intelligence community, the state and locals and the private sector in response to the terrorism threat.

Of course, responders must be trained to deal with this threat. A tabletop exercise built around an EMP hit on the continental United States would not be hard to build and would allow participants from all levels of government to participate. Tabletop exercises often called "war games" are highly didactic and if conducted properly can function like a 3-Dimensional GAP analysis to show where our response to an EMP attack is weak and in need of immediate improvement. We do these every day in the counter-terrorism world, so again the fix is not that hard to do.

Lastly, we need to pay better attention to our missile-defense capabilities. As Americans, we think little of the defense umbrella provided by NORTHCOM. But even this umbrella needs some upgrades. With our anti-missile missiles not yet achieving at least an 80 percent knock-down rate, we need to enhance our ability to detect and shoot down suspicious airborne threats that could be carrying an EMP triggering device. Recently, Congress authorized $13.8 billion for missile defense. This is a good start, but it needs to be followed on in the out years by other appropriations to maintain our lethality in defending the air and the space above the United States.

It's been 10 years since I met with those desperate scientists in my Washington, D.C., office. We needed to address the EMP threat to the homeland in 2008 as we need to address it in 2018. Unfortunately, our government has remained pretty much quiet about the threat, yet those scientists are still desperate. Isn't 10 years too long to live life in quiet desperation?

***Jack Thomas Tomarchio** is the President of Agoge Group, LLC, a strategic consulting firm in Wayne, Pa. He served as Principal Deputy Assistant Secretary of Homeland Security for Intelligent and later Principal Deputy Under Secretary for Intelligence from 2006-2008. He is a Senior Fellow at the George Washington University Center for Cyber and Homeland Security and the Foreign Policy Research Institute.*

What's Happening Behind Scenes to Thwart Radiological Attacks

By Rico Chandra

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/whats-happening-behind-scenes-thwart-radiological-attacks/

March 2018 – Over the course of 2017, the global political landscape shifted significantly. More than one of the developments is likely to have heightened, rather than diminished, the concerns that another large-scale malicious attack on U.S. soil is looming. Just three months ago, a man detonated a pipe bomb in the New York City subway system near Times Square. Thankfully, the explosion did not result in deaths, though a handful of minor injuries were reported. While this appears to be an isolated and amateurish incident, it once more highlights the alarming and potentially tragic consequences of terrorism.

Yet despite tensions growing year by year, our nation has not suffered a single casualty in an act of radiological terrorism. As a reminder, the threat could come in the form of a strong radioactive source the size of a pencil hidden in a packed stadium, invisibly exposing crowds to the point of acute radiation sickness. Or, it could be a rogue nation, whose ballistic missiles might not be quite as reliable as a shipping container destined for Los Angeles.

The absence of radiological attacks on the U.S. homeland is not entirely coincidental. Behind the scenes, a monumental effort is being carried out by multiple U.S. and international agencies. They are working to prevent some deeply troubling scenarios from jeopardizing our way of life. A multi-layered defense has successfully protected U.S. citizens from a radiological attack. Even as the sophistication of terrorist organizations increases rapidly, the government uses technology – including new and emerging technologies – and intelligence to remain one step ahead in this race.

Mitigating threats at the source

In July 2017, the *Washington Post* published an article on how ISIS nearly stumbled upon the ingredients for a "dirty bomb." Indeed, over a prolonged period of time Daesh's territorial control of Mosul made them the unknowing owner of more than one strong radioactive source. It would have taken little skill to repurpose these sources into daunting radiological weapons of terror.

Obviously, Mosul is not the only place on earth where strong radioactive sources exist. Just about every country in the world has strong radioactive sources. Add to that the presence of nuclear material – uranium and plutonium – that if processed the right way are the key ingredients to yield nuclear weapons.

Yet despite the abundance of these radiological threats, we have remained safe from their effects. The United States has worked with international partners to reduce this risk in many ways, starting with reducing the number of such threats and cataloging the ones that cannot be avoided. The National Nuclear Security Administration (NNSA) of the Department of Energy has helped foreign governments secure some of the most dangerous of these materials at the sites where they are stored. Adding onto that a second layer of protection, the NNSA has helped deploy radiation detection equipment to the borders of vulnerable countries, for instance at the periphery of the former Soviet Union. And in yet another building block of this global nuclear detection architecture, radiation detection equipment is installed in most modern seaports, monitoring U.S.-bound maritime containers for radiological signatures.

Regardless of our best-laid plans, we must still assume that nefarious actors will be able to move illicit material to their target location. But the knowledge and logistics necessary to evade the many layers of this detection-net forces adversaries to inform themselves and to plan. Such communication in turn increases the digital footprint of nefarious actors that intelligence services can target.

Prevent at points of entry

Almost every truck or maritime container entering the U.S. passes through a so-called Radiation Portal Monitor (RPM). These highly sensitive systems are mounted on either side of traffic lanes 12 feet high; tall enough to monitor vehicles in their full height. Well over a thousand such devices are installed at the northern land border, the southern land border, and at the seaports of both coasts. The Department of Homeland Security's Countering Weapons of Mass Destruction (C-WMD) office (until recently, the Domestic Nuclear Detection Office) is currently running a technology evaluation with the goal of replacing many of the aged existing RPMs with cutting-edge technology.

The new technology will have a particular emphasis on cybersecurity. While older generations of systems had been integrated in a cyber-secure manner, the new systems will be *cyber-hardened by design*. A higher degree of network integration will result in lower manpower needs of the new systems, allowing personnel tied up babysitting the current systems to be deployed in more effective ways. The new RPMs will have benefited from novel technologies developed over the last decade, making them significantly lower cost to acquire and operate than earlier generations were. Above all, the new systems will be more precise in being able to differentiate between actual threats and benign sources of radiation, an important economic factor. In June 2017, the port at Charleston, S.C., was shut down for hours after a potential "dirty bomb" was suspected upon a docked freighter. Though that particular threat never materialized, it highlighted that even the credible threat of a weapon, without the weapon itself, can have a grave economic impact.

Protect citizens at the local level

The federal government has been supporting state and local authorities in their efforts to protect important cities. In Washington, for example, Metro Transit Police officers are in the process of being outfitted with portable radiation detectors to identify potential dirty bomb threats. Similar efforts are underway in major cities that terrorists are likely to view as high-value targets. Historically, the detection of radiation has relied on equipment that tended to generate too many false alarms to be practical in public spaces. Moving forward, technology has advanced to the point that scalable, highly efficient detectors can be used in concert with pager-sized devices to improve the possibility of finding a source in a large area.

The combination of static and mobile detection, when used in conjunction with data analytics, enabled by the growth of ubiquitous cloud computing, can increase the success of detection as it reduces the overall cost to conduct radiological searches. By affording more radiation detectors that can be interconnected, the United States can develop revolutionary ways of identifying threats, and therefore preventing attacks and protecting U.S. citizens.

Developing the future of radiation detection

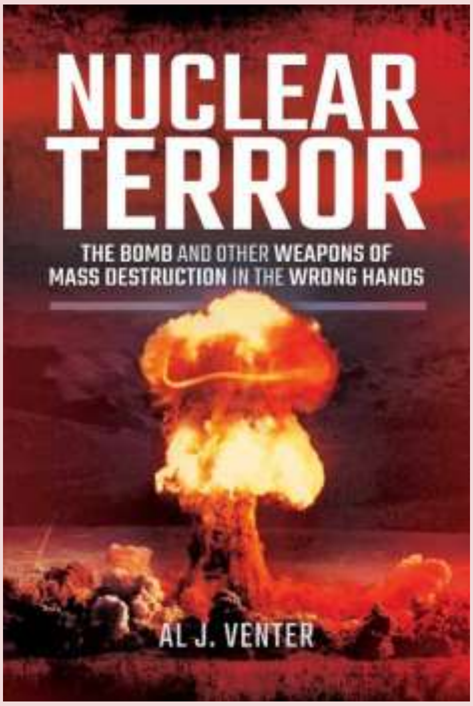
With the help of next-generation radiation detection systems, government agencies including DHS can identify, prevent, and protect against incoming threats caused by radioactive and nuclear materials. Once radiation detection systems have been successfully integrated, regular testing will help strengthen the agency's detection capabilities and overall preparedness. A lot has been invested into building the global nuclear detection architecture, parts of which have been described above. Given that the general public has remained safe from radiological attacks, the strategy of layered protection appears to have served us well. Despite the overwhelming number of radiological threats present in the world, such weapons have not been turned against us. And through continuous investment into development of new technology and deployment of reliable systems, the government has managed to stay one step ahead of the bad guys.

__Dr. Rico Chandra__, CEO and co-founder of Arktis Radiation Detectors, has a PhD from ETH Zurich, awarded for his work in dark matter detector R&D at CERN, Geneva. His experience includes consulting work performed for the European Commission in security questions, strategic consulting of several SMEs, and technology consulting as a council member of the Gerson Lehrman Group.

Dirty Bombs – Terrifying, But Not In The Way That You Think

Source: https://www.forces.net/news/dirty-bombs-terrifying-not-way-you-think

Jan 02 – There is nothing scarier than the prospect of nuclear terrorism. Here, author Al J Venter explains that a 'Dirty Bomb' attack might not be as immediately devastating as generally feared. Equally though, he illustrates that the risks of nuclear material falling into the wrong hands are alarmingly high, and that authorities cannot afford to be complacent.


NUCLEAR TERROR
THE BOMB AND OTHER WEAPONS OF MASS DESTRUCTION IN THE WRONG HANDS
AL J. VENTER

The following is an edited version of an excerpt from his book 'Nuclear Terror'.

Article by Al J. Venter

Among the most consistent debates along the corridors of power in Washington, Whitehall and the Kremlin is whether nuclear, chemical or biological weapons will be the first to be used in upgraded weapons of mass destruction (WMD) onslaughts by Islamic zealots.

For many, the consensus is that nuclear is the most likely of these three, with an RDD – Radiological Dispersal Device – being the delivery method.

What sets the RDD apart from weapons used by other dissident political groupings is that al-Qaeda has shown an unusual and historic interest in these weapons, otherwise known as 'Dirty Bombs'.

In fact, one senior al-Qaeda official captured by the Americans said of his organisation:

"...they know exactly how to do it."

The motivation for such an attack can be found in the writings of Dhiren Barot, a British Hindu convert to Islam.

Writing under the alias of Esa al-Hindi in a book titled The Army of Madinah in Kashmir (Madinah, or more commonly Medina, refers to the second holiest site in Islam) Barot declared that one way to counter what he referred to as 'Western interference in Muslim lands' would be to conduct large-scale attacks with radiological weapons.

But where would the radioactive elements of such a device come from? And how could terrorists get it into the US?

One option al-Qaeda seriously considered was using spent fuel cells from dismantled former Soviet Union nuclear submarines currently being taken apart in Russia's far northern Kola Peninsula.

Once obtained and weaponised, the plan was – and still is - to smuggle a radiological bomb (or pathogens such as anthrax) across the Mexican border, or possibly secreted in a shipping container through a major US port.

The video game 'Dirty Bomb' involves a team of mercenaries dealing with this kind of attack – one hopes that, in this case, life does not imitate art

And having arrived inside the US, a Congressional Research Service (CRS) Report estimated that the impact of an attack from an RDD "would depend on many variables, such as meteorological conditions, type and amount of radiological material, duration of exposure, and method of dispersal". The report goes on:

"...both the threat posed by terrorist RDD use and the magnitude of impact are matters of some contention. Some experts believe that terrorists could, without great difficulty, obtain radioactive material and construct an RDD...others assert that radiation sources intense enough to cause casualties in an RDD attack would be injurious to the terrorists during acquisition and use. Most experts agree that few casualties would be likely to directly result, generally only among those close to the device, but many disagree on how attractive an RDD would be to a terrorist.

"Some assert that the inherent difficulties of handling radioactive material combined with few direct casualties make RDDs less likely terrorist weapons. Other experts claim that terrorists recognize the potential economic and psychological effects of such a weapon and thus more highly value RDDs as terror weapons."

The argument about terrorists falling victim to their own destructive device is viewed by some as superfluous.

Or, as one authority suggested, do those who compile these reports not read the daily newspapers?

Islamic zealots have proved many times in recent years that no matter what the risk – radiation sickness or otherwise – they would be happy to die for the cause in order to achieve their objectives. Suicide bombers are as much a feature of today's fundamentalist Islamic world as their five-times-a-day call to prayer.

But as frightening as this is, RDDs might more accurately be referred to as weapons of mass disruption than weapons of mass destruction.

In a large RDD blast within the confines of a city, there would obviously be a number of casualties, including people exposed to the actual blast who would succumb to the effects of the chemical explosion, as would be the case with a conventional bomb and the shrapnel that it disperses.

Though at the same time, the number of casualties would not be nearly as many as some authorities like to predict: a major bomb in downtown Chicago or Berlin would result in hundreds rather than thousands of casualties, of which only a limited number would die.

Furthermore, according to Dr von Wielligh, who has studied the likely outcome of such an attack, it is extremely unlikely that there would be such a vast amount of radioactive material in the immediate vicinity of an RDD blast that people would die right there from radiation. Acute radiation effects – including death - would only appear in the days, weeks or months that followed the exposure.

The main purpose of an RDD is to contaminate the surroundings and to disrupt normal commercial and other activities for an extended period. Most salient - and the terrorists know it – is the principal objective of detonating a 'Dirty Bomb' to create panic on a massive scale, which would unquestionably happen should the attack take place in the heart of any major city.

Dr Mike Foley is a geologist who has made a career of specialising in nuclear-related issues. He's likewise warned that weapons-radioactive materials "could be used in terror acts as pollutants rather than as fissionables".

In other words, the real issue might not be the explosiveness of such weapons but rather their potential to create multiple no-go areas.

That's because clearing up after an RDD attack is likely to be a formidable task. It might not only take an inordinately long time to counter the effects of serious radiation resulting from such a bomb, but the entire area would have to be quarantined, certainly for many months and, depending on both the nature of radioactive material employed and quantity, possibly for years.

Were it to happen outside the Bank of England in London, for instance, the level of radiation would be the ultimate deciding factor.

Not only buildings, but the entire grid of roads and sidewalks would need to be ripped up and, once the all clear is given, re-laid.

Contaminated debris would be dealt with in the appropriate manner, in and of itself a formidable task on a relatively small group of islands that comprise the United Kingdom.

It is axiomatic that costs would run into billions.

The problem is, preventing a dirty bomb attack is also expensive.

In fact, according to Foley, prevention is not being properly addressed precisely because of the immense cost and scale of the problem:

"All countries would need to expand coverage to everything including radon waste storage sites, medical waste and the rest...there is an incredible amount of radioactive waste about…not all of it safeguarded and in the Former Soviet Union, very badly."

Of significant concern in this regard are the burgeoning numbers of incidents that involve internationally-linked nuclear smugglers. According to the IAEA, these are increasing exponentially by the year.

Prior to his retirement as head of the IAEA in December 2009, Dr Mohamed Al Baradei disclosed that the Vienna-based UN watchdog was aware of hundreds of cases of nuclear smuggling annually (much of it linked to uranium or plutonium.) But this number likely reflects only the one in 10 or 12 cases that come to light.

Simply put, for every smuggling case we know about, there are another dozen or more not detected. In almost every case listed, people of Islamic or Middle East extraction are shown as receiving parties.

It is worth mentioning that IAEA investigators believe that those involved from former Eastern bloc countries are rarely ideologically motivated. Rather, they're interested only in the money and it is of little concern to many of them whether cities or people are contaminated by deadly radiation.

"The fear, essentially, is that the criminals may have no qualms about selling to Jihadist groups", read the IAEA report. Furthermore, the IAEA's smuggling figures did not include radiation sources that had simply gone missing.

"An average of one a day is reported to the US Nuclear Regulatory Commission as lost, stolen or abandoned,' it read.

Also, there were still more than 1,000 radioactive sources unaccounted for in Iraq.

In another case, of 25 sources stolen from the Krakatau steel company in Indonesia in October 2000, only three were ever recovered.

When sources such as these show up, they can appear in some unexpected places:

"In Tbilisi, Georgia, a taxi driver, Tedo Makeria was stopped by police in May 2003 and found to be carrying lead-lined boxes containing strontium-90 and caesium-137. (And in Belarus,) customs officials seized 26 radioactive cargoes between 1996 and 2003, six of them from Russia", the IAEA disclosed.

On the plus side, technology for mitigating the effects of a dirty bomb attack does exist.

There are pagers to detect radiation levels, special anti-radiation protective sprays and a gel designed to suck radioactive particles out of contaminated concrete.

Yet some scientists privately question whether this technology would really be up to the task of coping with a full-scale radiological disaster.

Additionally, as the BBC's Frank Gardner has noted:

"…until terrorists actually detonate a dirty bomb, the funding for dealing with such an attack is (limited)."

In summation, one can look to Washington's Federation of American Scientists, which succinctly analysed the dirty bomb threat and reached three principle conclusions:

1). That "radiological attacks constitute a credible threat… materials that could be used for such attacks are stored in thousands of facilities around the US, many of which may not be adequately protected…"

2). "While radiological attacks would… not result in… thousands of fatalities," they would kill some as well as contaminating large urban areas;

3). "Materials that could easily be lost or stolen from US research institutions and commercial sites could contaminate tens of city blocks at a level that would require prompt evacuation and create terror in large communities even if radiation casualties were low… Since there are often no effective ways to decontaminate buildings that have been exposed at these levels, demolition may be the only practical solution."

The final sentence puts the high (or one might say, comparatively low) cost of prevention into perspective: "If such an event were to take place in a city like New York, it would result in losses of potentially trillions of dollars."

***Al J Venter** has had more than 50 non-fiction titles published in Britain, the US and South Africa, many of them about military and insurgency-related developments in the Middle East and Africa. He is a specialist writer on nuclear warfare.*

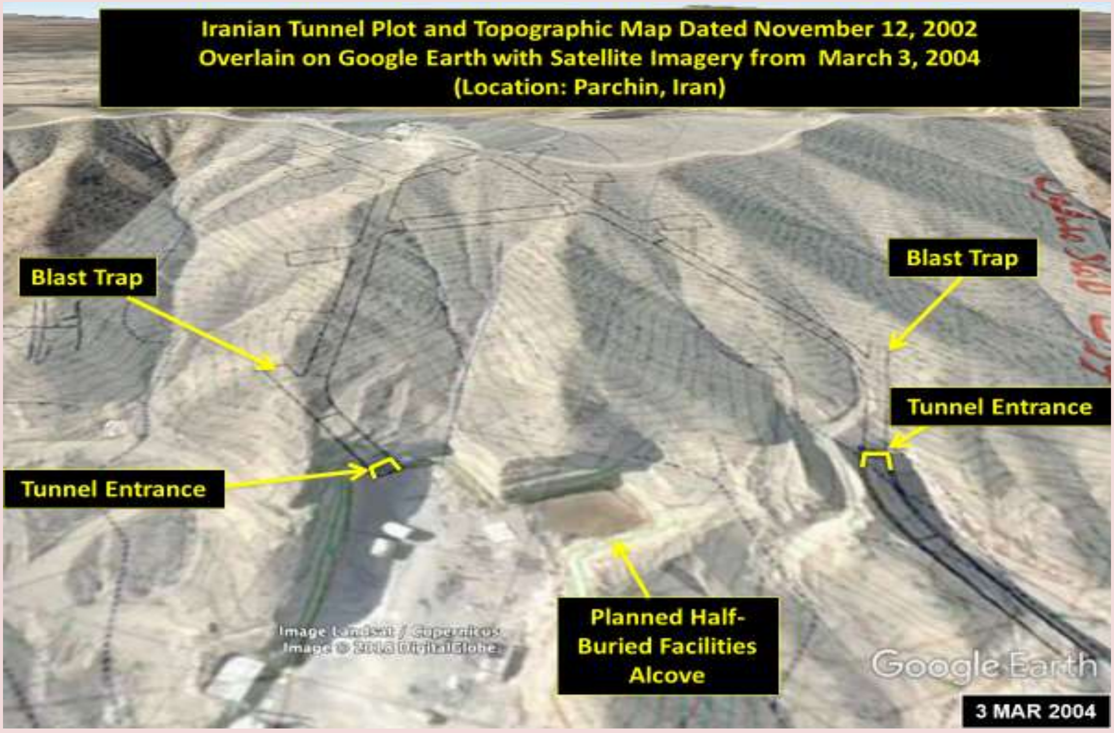
Weapons experts: Archives show that Iran was likely developing nuclear warheads

Source: http://www.homelandsecuritynewswire.com/dr20190118-weapons-experts-archives-show-that-iran-was-likely-developing-nuclear-warheads

Jan 18 – **Documents in the Iranian nuclear archive captured by Israel last year show that Iran built an underground facility, which was likely used for the development of nuclear warheads**, a paper published Friday by the Institute for Science and International Security charged.

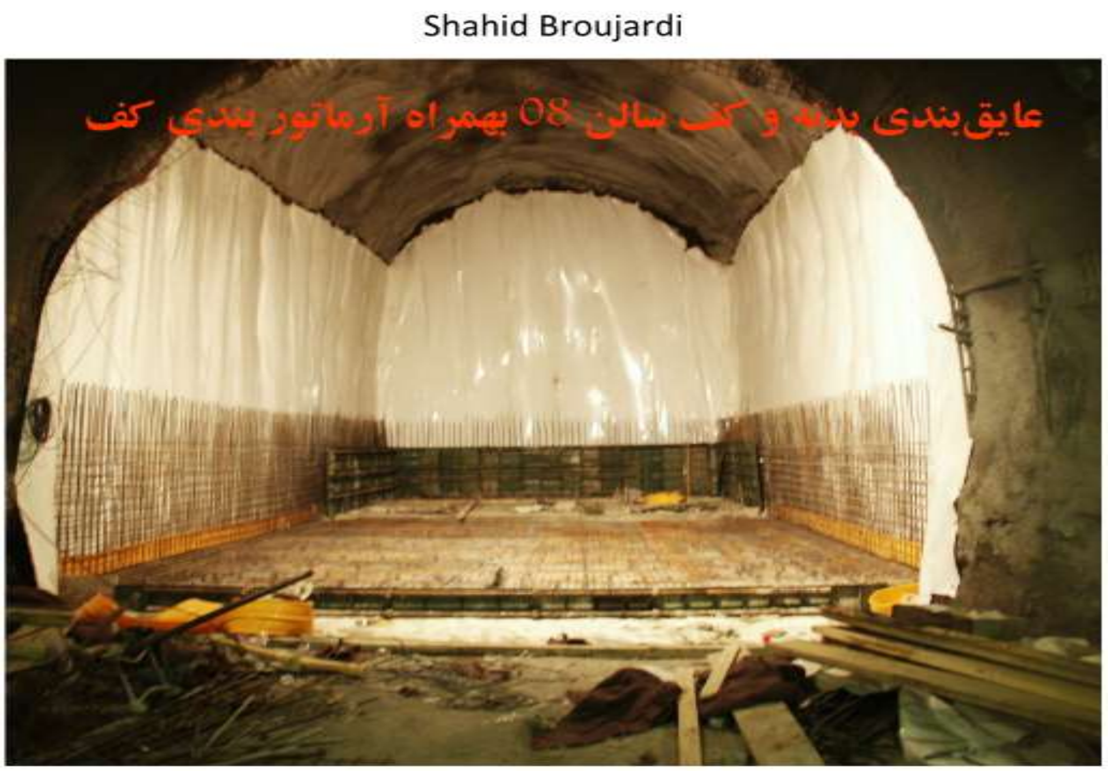
The paper — written by David Albright, a former weapons inspector and president of the institute; Olli Heinonen, former deputy director general of the International Atomic Energy Agency (IAEA); Frank Pabian, a former inspector for the IAEA; and Andrea Stricker, a senior policy analyst at the institute — reports the Iranian documents show that under the Amad Plan there was a project for designing the warhead for a nuclear weapon.

The Amad Plan is Iran's nuclear weapons research program. After 2003, it was restructured and parts of it were made covert. One project associated with Amad was called Project 110. Under Project 110 was the Shahid Boroujerdi project.



Iranian Tunnel Plot and Topographic Map Dated November 12, 2002
Overlain on Google Earth with Satellite Imagery from March 3, 2004
(Location: Parchin, Iran)

Blast Trap
Blast Trap
Tunnel Entrance
Tunnel Entrance
Planned Half-Buried Facilities Alcove
Image Landsat / Copernicus
Image © 2018 DigitalGlobe
Google Earth
3 MAR 2004



Shahid Broujardi

The documents in the archive show that Iran built an underground tunnel at the Parchin military site to accommodate the secret research of the Shahid Boroujerdi project.

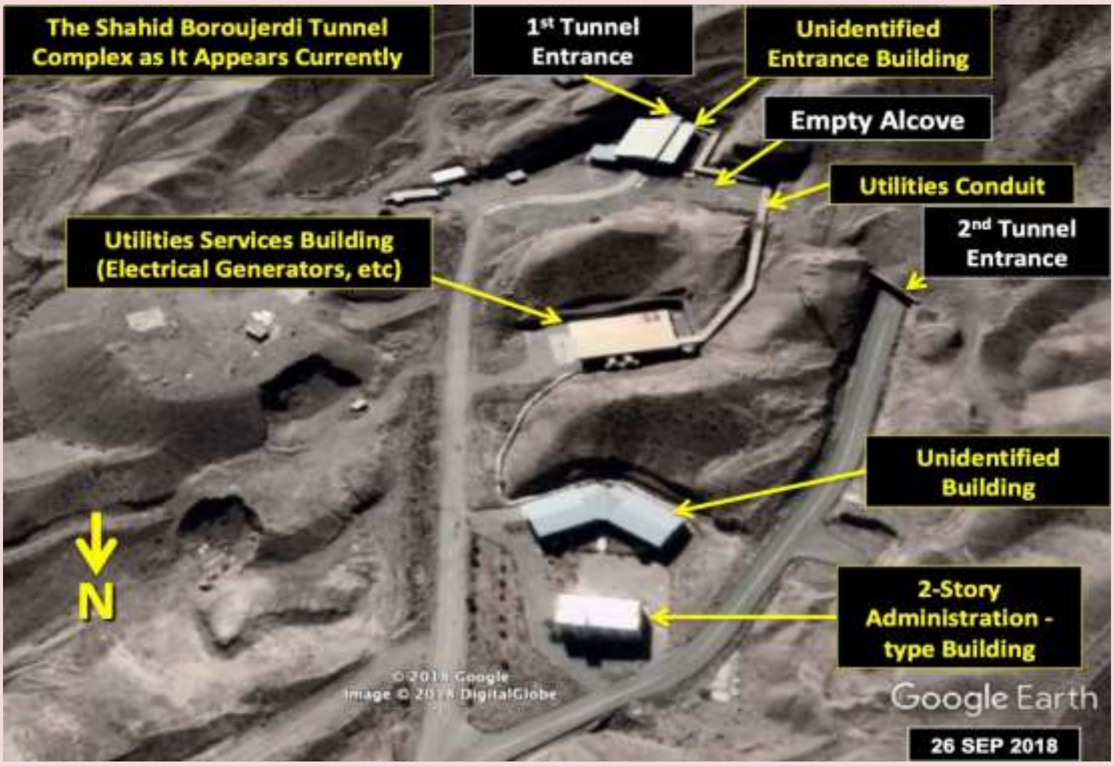
"The purpose of Project Shahid Boroujerdi was most likely the production and fabrication of uranium metal components for nuclear warheads," the paper asserted. "Although uranium is not directly mentioned in any of the documents available to the Institute, the most logical choice of materials to be handled in this facility is uranium."

That the metal used in the secret facility was likely uranium could be supported from a declaration of Iran to the IAEA, that an "Iranian project 3.14 was involved in shaping uranium metal." This matched the project number for the Shahid Boroujerdi project in the nuclear archive captured by Israel.

One document in the archive described the rooms in the underground facility and their roles. The paper noted that the most sensitive rooms were fully underground (described as "buried" in the documents). These include rooms for" metal reduction, melting and casting, and metal forming," according to the paper.

"Overall," the paper assessed, "this site's location and layout would connotate a production-scale facility rather than a research and development facility." The files Israel recovered from Iran didn't document all of the equipment in the facility or the expected annual production of weapons-grade uranium the facility could produce. However, the paper estimated — "with a high degree of uncertainty" — that the facility could produce enough enriched uranium for 2.5 to 3.3 nuclear weapons annually.

According to the paper, the site has never been inspected, nor has Iran been known to have discussed it with the IAEA.


The Shahid Boroujerdi Tunnel Complex as It Appears Currently
1st Tunnel Entrance
Unidentified Entrance Building
Empty Alcove
Utilities Conduit
2nd Tunnel Entrance
Utilities Services Building (Electrical Generators, etc)
Unidentified Building
2-Story Administration - type Building
N
© 2018 Google
Image © 2018 DigitalGlobe
Google Earth
26 SEP 2018

Iran, in fact, has denied ever undertaken "uranium metallurgy relevant to making nuclear weapons." The IAEA, in its final assessment of Iran's nuclear program in December 2015, stated, "Iran informed the [IAEA] that it had not conducted metallurgical work specifically designed for nuclear devices, and was not willing to discuss any similar activities that did not have such an application."

The paper asserts:

The information about a heretofore unknown Project 110 facility highlights the immense value of the Nuclear Archive seized by Israel in filling in missing pieces of the jigsaw puzzle that is Iran's nuclear weapons program. It also highlights the urgent need for the IAEA to inspect previously associated military sites in Iran, and once again, provides substantial evidence that Iran's declarations to the IAEA are incomplete and deliberately false.

In reviewing the files recovered from Iran's nuclear archive, the team has learned not only that Iran's nuclear weapons program had progressed further than previously thought, but that Iran possessed “advanced capabilities” to develop nuclear weapons. What the experts concluded, was that “that Washington and the IAEA were constantly underestimating how close Tehran was to a bomb” prior to negotiating the deal that was finalized in 2015.

In a previous paper published by the institute, Albright, Heinonen, and Pabian argued that the new information contained in the archive “necessitates calling for more action by the IAEA and the Joint Commission, which administers the Joint Comprehensive Plan of Action (JCPOA).”

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

C²BRNE DIARY

EXPLOSIVE NEWS

Advanced Explosives Detector for Airport Security

Source: https://i-hls.com/archives/87624

Dec 23 – A new explosives trace detector will provide solutions for the challenge of rapidly screening passengers and cargo in airports.

The **TRACER 1000 detector** is based on mass-spectrometry, a technique for measuring the mass-to-charge ratio of matter particles.

TRACER 1000 can detect a number of substances that include peroxides, explosive materials, fentanyls, heroine, and cocaine. This according to 1stdetect.com.

With a similar CONOPS (concept of operations) and standard swab sampling mechanism to collect trace samples from surfaces, the device was designed to replace the current generation of IMS-based explosives trace detectors currently deployed at airports, cargo inspection depots, and other high-security facilities globally.

US-based Astrotech has announced that the TRACER 1000 has passed the European Civil Aviation Conference's (ECAC) common evaluation process (CEP) for airport checkpoint screening of passengers, according to airport-technology.com.

It is said to be the first mass spectrometry-based explosives trace detector (ETD) to have passed ECAC's laboratory testing protocol.

ECAC is the European regulator on aviation security and is the equivalent of the US Transportation Security Administration (TSA).

After receiving formal certification at the CEP Management Group's next meeting, Astrotech plans to start offering TRACER 1000 to airports worldwide.

In January, the TRACER 1000 was accepted by ECAC into European evaluation process for security screening in airports.

Thomas Pickens III, CEO of 1st Detect, the wholly owned subsidiary of Astrotech, said: "ECAC's support throughout this process demonstrates their commitment to setting the global standard of security by adopting the most advanced explosives detection technology.

"The TRACER 1000 was designed to improve safety and enhance the airport experience for travellers and personnel by reducing wait times at security checkpoints."

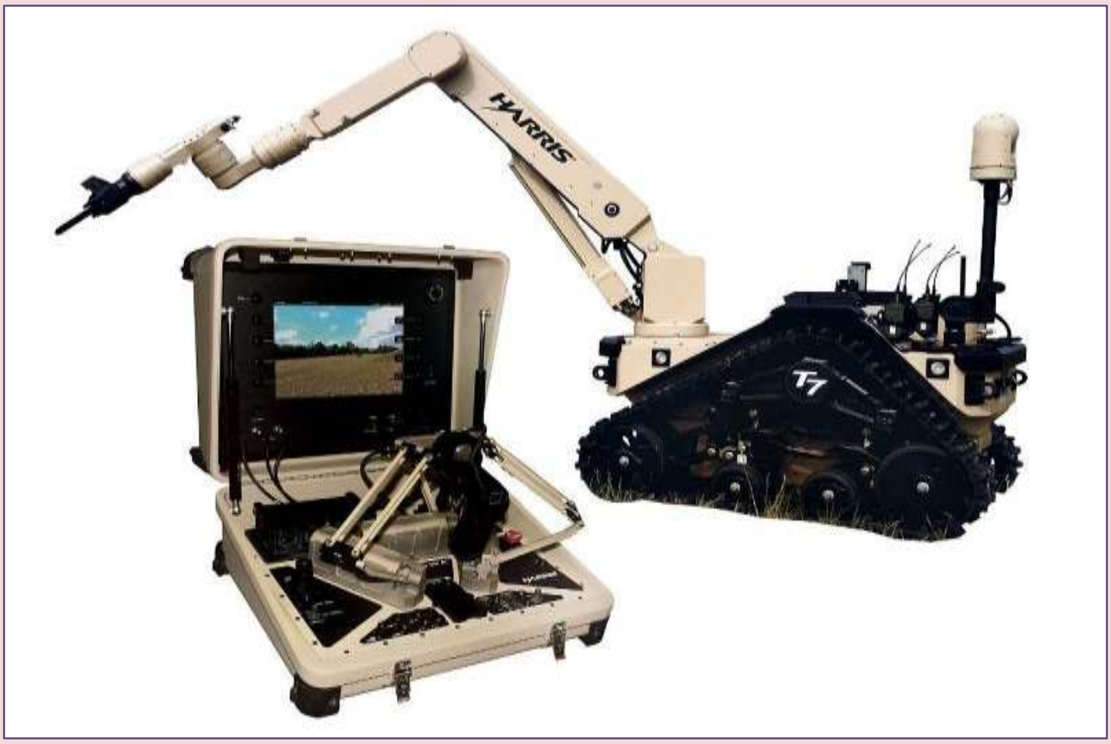
"We look forward to improving the safety of the world's air transportation systems with our high-quality instruments for many years to come."

Another official from Astrotech stated: "Passing ECAC's CEP test for airport checkpoint screening of passengers is an important validation of our technology."

Unexpected Advantage of New Robotic Bomb Disposal Tech

Source: https://i-hls.com/archives/87761

Dec 28 – Bomb disposal robots with technology that allows human operators to "feel" their way through disarming explosive devices have been delivered to the British Army. The system was designed to provide operators with human-like dexterity while they operate the robot's arm using the remote-control handgrip giving them physical feedback, allowing intuitive detailed control, according to the MoD.



The robots use state-of-the art "advanced haptic feedback", in which vibration is used to guide an operator's hand movements as they work to defuse a device from a safe distance.

Haptic technology, also known as haptics, is what creates the vibration sensitivity found in some modern computer game controllers.

Four **Harris T7 unmanned ground vehicles** (UGV) costing almost £1 million each have been delivered to explosive ordnance units, the first of 56 dues to begin service by 2020.

Defence Secretary Gavin Williamson said: "These robots will go on to be an essential piece of kit, preventing harm to innocent civilians and the brave operators who make explosives safe. "The robots will provide the Army with the latest bomb-disposal technology and will prove to be trusted companions both on UK streets and in deadly conflict zones."

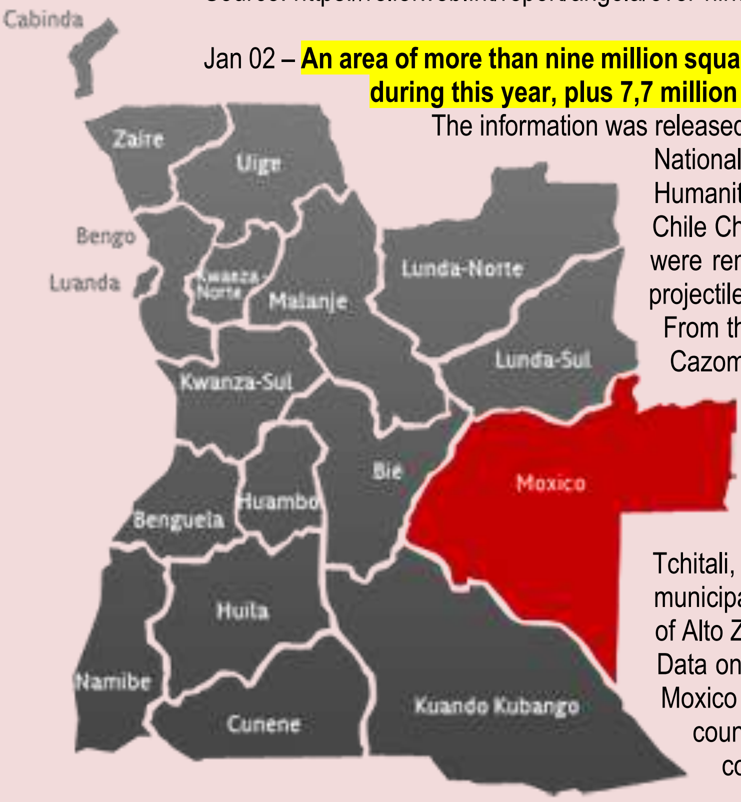
The T7 also comes with equipment including HD cameras and all-terrain tank-style tracks.

It underwent eight weeks of trials in the UK and United States, as reported by shropshirestar.com.

The robots will replace the British Army's Wheelbarrow Mk8B remote controlled robots, which have been in operation since 1972 and will be phased out from 2020.

Over nine million square meters cleared of landmines

Source: https://reliefweb.int/report/angola/over-nine-million-square-meters-cleared-landmines



Jan 02 – **An area of more than nine million square meters of land was demined in Moxico province during this year, plus 7,7 million square meters compared to 2017.**

The information was released Sunday in Angolan city of Luena by the official of the National Inter-sectoral Committee for Demining and Humanitarian Assistance (CNIDAH) of the province of Moxico, Chile Chicanha, noting that this year 576 antipersonnel mines were removed and destroyed, as well as 67 anti-tank, 1,473 projectiles and 4,063 ammunition.

From the clean areas, he highlighted the surroundings of the Cazombo aerodrome (Alto - Zambeze), the perimeter of the bridge over the Luena river, the road that gives access to the community of Tchafinda, Sinai Novo and polygons of the 72nd brigade.

He said that in spite of the mine clearance work, there were accidents with mines in the localities of Tchitali, Moxico municipality, Francisco neighborhood, municipality of Léua, and in the outskirts of the municipalities of Alto Zambezi and Bundas.

Data on the impact of the mines on the communities point to Moxico as one of the 18 provinces of the most mined in the country, with a size of 299 square meters, of which 250 are confirmed and 49 are suspect.

Land mines will be hidden killer in Yemen decades after war

Source: https://abcnews.go.com/International/wireStory/land-mines-hidden-killer-yemen-decades-war-59994106

Jan 02 – They lurk under shifting desert sands, amid the debris of urban roadsides and inside abandoned schools, some set to go off at the lightest touch.

Land mines scattered by Yemen's Houthi rebels are largely unmapped and will remain a threat even if the latest push for peace succeeds in halting the conflict, those involved in their eradication say.

While the Houthis' use of Scud and other retrofitted ballistic missiles has drawn attention for striking deep inside Saudi Arabia, their widespread use of mines represents a risk for generations to come in the Arab world's poorest country.

"Mines today exist in every single area of Yemen," Ousama al-Gosaibi, the program manager for the Saudi-funded Masam demining project, told The Associated Press during a trip to the southern city of Aden organized by the Saudi military. "It's not being used as a defensive (or) offensive mechanism. It's being used to terrorize the local population across Yemen."

A Houthi official acknowledged the rebels widely use mines, but said Saudi-led airstrikes have left behind ordinance that is just as deadly.

Yemen's war pits the Iran-aligned Houthis against the internationally recognized government, which is backed by a coalition led by Saudi Arabia and supported on the ground by the United Arab Emirates.

More than 60,000 people have been killed in the war since 2016, according to the U.S.-based Armed Conflict Location & Event Data Project, or ACLED, which tracks the conflict. The fighting has displaced 2 million, spawned a cholera epidemic and pushed the country to the brink of famine. Millions wake up hungry each day, not knowing from where their next meal will come. Many civilian deaths in the war have been blamed on Saudi-led airstrikes, which have hit markets, health facilities and weddings.

Among the dangers facing combatants and civilians alike are land mines. The Houthis looted government armories when they captured much of northern Yemen, including vast stockpiles of anti-tank mines. Anti-personnel mines also litter the country, despite the government joining a 1997 international convention banning their use.

A U.N. panel of experts said in 2016 that the Houthis had used land mines in their retreat from the southern city of Aden. Since 2016, land mines and other explosives planted by the Houthis have killed at least 222 civilians and wounded others in 114 incidents, according to ACLED.

"Due to the difficulty of obtaining accurate estimates, these figures are likely to make up a fraction of all mine detonations involving civilians in Yemen," ACLED said.

Making things worse is the fact that a third of all health facilities in Yemen are closed, said Nasser Baoum, the government's health minister.

"Mines have caused a huge problem," Baoum told the AP. "It's OK for an army person to be injured during battle or to be hit by a mine, but for a child to be hit while she's in the field or on the way to fetch water, that's a tragedy."

Al-Gosaibi accused the Houthis of reconfiguring anti-tank mines that previously needed over 100 kilograms (220 pounds) of pressure to detonate so that they require less than 10 kilograms (22 pounds) — meaning a child could trigger the explosive.

Yahia al-Houthi, the former director of the Yemen Executive Mine Action Center, a Houthi-controlled de-mining center, acknowledged the rebels use anti-tank mines but denied tampering with them to target individuals. He also claimed the Houthis never used anti-personnel mines, despite widespread evidence to the contrary.

Brig. Gen. Yahia al-Sarie, a Houthi officer, said the rebels only use land mines on the battlefield and not in civilian areas. "This is a war, so what do you expect us to do? Receive the other side with flowers?"

He said the rebels had mapped the mines and would be able to remove them "in no time" once the fighting ends.

Al-Gosaibi accuses the Houthis of using Iran-supplied technology like infrared sensors and of adopting Iranian tactics like hiding bombs inside fake rocks. A report in March by the group Conflict Armament Research said roadside bombs disguised as rocks in Yemen bore similarities to others used by the Iran-backed Hezbollah in southern Lebanon and by Iran-linked insurgents in Iraq and Bahrain.

Mines planted by the Houthis, some resembling a model previously displayed in Iran, also have been found in the Red Sea, according to a 2018 U.N. experts report. Those mines "represent a hazard for commercial shipping and sea lines of communication that could remain for as long as six to 10 years," the report warned.

The Saudi-led coalition, Western countries and U.N. experts accuse Iran of supplying weaponry from assault rifles to ballistic missiles to the Houthis. Iran supports the Houthis but denies arming then, and Iran's mission to the U.N. dismissed the latest allegations of "Iranian ghost weapons."

"Yemen has long been awash with a wide range of weapons — including ballistic missiles — and Yemenis do not need Iranian weapons to conduct war," said Alireza Miryousefi, a spokesman for Iran's mission.

Unexploded cluster munitions and bombs dropped by coalition aircraft — including some manufactured in the United States — also litter Yemen, according to the U.N. The coalition has faced widespread international criticism over indiscriminate airstrikes that have killed large numbers of civilians.

Al-Houthi said their forces had removed 500,000 missiles and cluster munitions from Saud-led strikes.

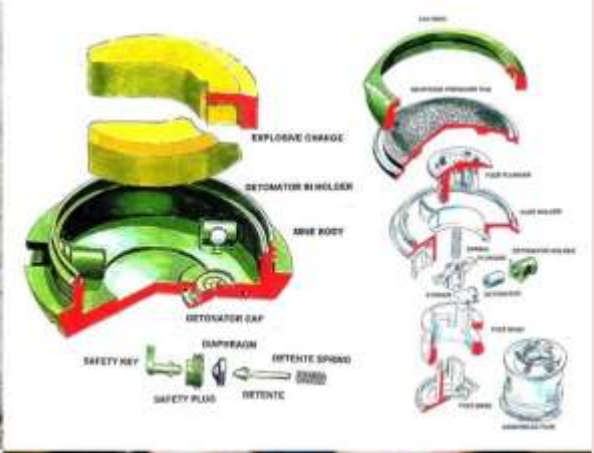
Saudi Arabia has alleged as many as 1 million mines may have been laid by the Houthis. Al-Gosaibi described Yemen as being the most-mined nation since World War II, based on his group's estimate of the mines laid by the rebels. Saudi officials have released pictures showing fields of deactivated land mines.

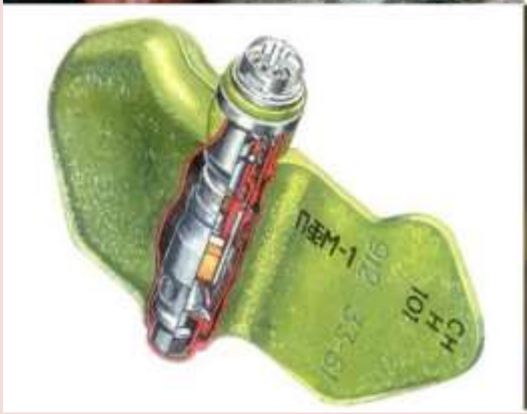
International groups dealing with land mines have been hesitant to estimate the scale of the crisis, given the limited information they have. Yemen is also littered with mines from previous conflicts.

"It's going to take years," al-Gosaibi said. "You cannot rebuild Yemen without addressing the mine issue. It's us on the ground first before rebuilding starts."

Drones Used to Find Toy-Like “Butterfly” Land Mines

Source: https://www.scientificamerican.com/article/drones-used-to-find-toy-like-butterfly-land-mines/





Jan 02 – A type of land mine called the “butterfly” has a particularly insidious reputation for two reasons: It is known for killing or crippling children who may pick up what looks a lot like a green plastic toy, and its mostly nonmetallic construction means it often evades traditional mine detectors. Butterfly mines’ light-touch detonators go off easily if stepped on by a fighter—or farmer—and their relatively small charge often maims people without immediately killing them.

More than a million Russian-made PFM-1 land mines—the most common butterfly type, possibly inspired by similar U.S. weapons deployed during the Vietnam War—still litter Afghanistan after decades of conflict. During the Soviet-Afghan War in the 1980s, military helicopters dropped swarms of these mines, whose “wings” let them flutter to the ground. This created instant minefields blocking high mountain passes, contributing to the problem of land mines and unexploded ordnance responsible for killing or injuring more than 30,000 Afghan civilians since 1978. In recent years children have made up the majority of victims killed or wounded by such weapons in Afghanistan.

Land mine clearance usually involves a careful, meticulous, time-consuming process of interviewing local residents and then sweeping suspected areas twice on foot, using handheld mine detectors. The estimated costs of removing a single mine can range from $300 to $1,000—and even confirming a patch of ground is safe without finding any mines costs money. But now, early tests by a group of U.S. researchers have shown they may be able to make the process a lot faster and more efficient by using a thermal imaging camera mounted on a quadcopter drone.

"The only way to clear mines is to poke every inch of the ground," says Alex Nikulin, assistant professor of energy geophysics at Binghamton University in New York. "But we can tell you where to poke."

Nikulin and his team are basing their strategy on the fact that plastic heats up and cools down differently than the surrounding soil and other parts of the environment. By conducting flight tests around sunrise and sunset, when temperatures can rapidly change, the researchers showed that inert PFM-1 land mines lying on the ground become clearly visible in thermal imagery captured by the drone camera and displayed on a laptop. They presented their work at the annual meeting of the American Geophysical Union, held in Washington, D.C., in December.

In field trials conducted in September 2017 at a New York state park, the team was able to pick up almost 78 percent of the mines during four trials. That is not yet good enough to fully replace survey work by ground teams. But it could help narrow down the locations and general layout of PFM-1 minefields, says Alex van Roy, deputy head of operations at the Geneva-based Swiss Foundation for Mine Action (FSD)—and a mine action specialist who formerly served in the Australian Army.

"This drone with this tech may allow you to determine in a much more rapid fashion where the minefield footprint is," says van Roy, who was not involved in the Binghamton team's research. "You find the perimeters of the footprint so that you can focus your manual, expensive clearance team in as small an area as possible."

The idea of using thermal imagery to detect land mines has been explored before but has only recently become more practical, as both drones and thermal imaging cameras get smaller and less expensive. A next step could use computer software to automatically detect land mine signatures in the thermal imagery, Nikulin says. His team hopes to recruit coders to develop a machine-learning algorithm capable of handling image recognition patterns. The goal is to eventually offer a $10,000 boxed set—which would include the off-the-shelf drone, infrared camera and a laptop loaded with custom software—to humanitarian demining organizations.

Cost matters a lot. Some of FSD's demining work in Afghanistan and Iraq gets U.S. State Department funding, but the Swiss foundation still relies heavily on donors—and on spending its funding wisely. "If [the technology] costs $50,000, we can't use it," van Roy says. "That's enough to purchase 10 traditional land mine detectors, or maybe fund a team of humans in Afghanistan for a month."

There are other complicating factors. Some plastic land mines originally dropped decades ago may have been buried in landslides or earthquakes, van Roy says. Sunlight exposure may have degraded others to the point where their shapes defy easy visual identification. Governments also often restrict drone use in conflict zones within countries such as Afghanistan or Iraq.

Still, the Binghamton team's focus on Afghanistan is a good strategy, van Roy says. Thermal imaging from the air may not work for buried land mines or cluttered environments with a lot of vegetation or human-made artifacts—but it does seem better suited for spotting the PFM-1 land mines dropped in Afghanistan's dry, high-elevation mountain passes with their generally sparse population and relatively light underbrush.

How to spec out an EOD response truck

Source: https://www.policeone.com/police-products/vehicles/specialty/articles/482401006-How-to-spec-out-an-EOD-response-truck/

Jan 07 – With domestic terrorist attacks being a growing concern for U.S. police departments, many are choosing to acquire one or more EOD response trucks to deal with suspected bombs in their jurisdictions. These rugged, blast-hardened vehicles are designed to efficiently carry bomb disposal technicians, their protective suits and tools, and mobile bomb disposal robots to bomb incident scenes to defuse and/or remove possible explosive devices before they go off.

If your department plans to acquire its first EOD response truck, or add new vehicles to an existing fleet, here are some points to consider when you spec out the truck.

Budget comes first

When it comes to acquiring an EOD response truck, "the biggest barrier is the cost," said bomb disposal expert Brian Knudsen. He is Director of Business Development and Public Relations with the United States Bomb Technician Association, and a17-year veteran with the Colorado County Sheriff's Office. "So, before you start pulling together plans and contacting vendors, figure out how much money you've got to work with," he said.

Get what you need

The key to getting maximum value for an EOD response truck purchase is by paying only for what you need. There is no point buying a truck strong enough to resist roadside IEDs (improvised explosive devices) like those used in Afghanistan, if your department is serving a relatively peaceful suburban area.

"Similarly, EOD response trucks in America don't need the kind of protection from hostile forces that is required overseas," said Knudsen. "Don't spend money on this protection unless you actually need it."

Climate counts

Select an EOD response truck that is suited for the temperature range, weather variations and driving conditions in a police department's specific jurisdiction.

For instance, if the jurisdiction gets hot in the summer, air conditioning is a must. If the winters are bitterly cold, then insulation and good heaters are mandatory.

If you drive in rough roads, don't forget four-wheel drive.

What do you need to carry?

An EOD response truck is primarily a transportation platform. This means it has to carry all the people and equipment necessary to handle bomb situations from the station house to the incident scene.

The vehicle must have enough room for bomb suits, x-ray equipment, bomb disposal tools and protective equipment – plus robotic bomb disposal units and the onboard equipment to control them, receive live video from the units' cameras and communicate this information to the outside world.

That's not all: The EOD response truck will need to carry antennas, and have enough power to run all the systems onboard with room to spare for future additions. As well, the vehicle may need to tow a trailer-mounted Total Containment Vessel (TCV) for safe bomb disposal, or have enough space on its truck bed to have one mounted.

"There is a whole range of items that an EOD response truck can be expected to carry, and it varies from department to department," Knudsen said. "The smart thing to do is to compile a list of what your department wants to have on the truck and then review the options for doing so with vendors; both to see what is available and what these options cost."

Get advice from other departments

It makes no sense to reinvent the wheel: When your department specs out an EOD response truck, talk to other departments that already have these trucks for their buying advice.

This will let you know which vendors make the most reliable EOD response trucks, deliver on their product promises and provide consistent after-sales service 24/7.

OK, WE FIGURED IT OUT. YOU JUST HAVE TO UNPLUG THE GREEN CABLE!
0:05
THAT AWKWARD MOMENT WHEN YOU'RE COLORBLIND.
0:02
PABLO STANLEY
memecenter.com MemeCenter

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Al-Qaeda Cybersecurity Tutorial to Jihadists: Fix Your Lame Passwords

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/al-qaeda-cybersecurity-tutorial-to-jihadists-fix-your-lame-passwords/

October 2018 – Jihadists received a cybersecurity lesson in a new magazine issue released this month by al-Qaeda in Syria, with encouragement to "no longer think of a password as a necessary evil or an annoying action" but "as your personal Ribat [fortification] position, as your shield to repel countless invisible attacks."

Please Login

Username: Username

Password: ●●●●●●

□ Remember Password

That means, the article chided, not selecting "123456" or the word "password" to protect myriad online accounts on which so much jihadist activity is conducted nowadays.

The guidance was included in Hay'at Tahrir al-Sham's English-language online magazine *al-Haqiqa,* which published its first issue in February 2017. The third issue of the magazine, published this past February, delved into cyber issues with articles on "media jihad" basics and the use of Bitcoin to fundraise.

"You know that feeling? Opening a social media app on your phone, swiping down and looking in vain for your favorite channel? Only realizing seconds later, that it must have been suspended…. again…? Irritating, right?" began the media jihad piece. "If this is annoying for you as a reader, imagine how tiresome it must be for the brothers operating these channels, who are working hard every day to bring you the latest developments."

Whereas that issue briefly ruminated on the sharia compliance of cybercurrencies, the newest *al-Haqiqa* released this month included a Bitcoin graphic urging reader to "share your wealth to finance jihad."

The password protection article declares that, by using an acronym derived from the first letters of a user's favorite hadith or quote, "Even the best spy agency would have to dedicate all of its computing power and resources for many years still finding this a very tough nut to crack."

"Your password length should be at least twelve characters long. Your password should be a combination of lower-case letters, upper case letters, numbers and hyphens. Make no mistake: any password is crackable, but obviously longer ones are harder to figure out," the anonymous author instructs.

Acknowledging that "most of us are creatures of habit and stick to their trusted password for years if they get the chance," with jihadists being no exception, readers are told to change their passwords every six months, pick different passwords for each "highly sensitive" account, and resist the temptation "to write your passwords down somewhere."

"A memorable combination of letters is all that protects you from the Kafir [disbeliever] enemy such as their police and intelligence services. Remember there are spies everywhere: they will try to crack your password via phishing expeditions and via hacking," states the article, calling a strong password "your first line of defense."

Aspects of this defense discussed in the article include the use of password managers and two-step verification. "Avoid the ones who are web-based online or offer you 'convenient' cloud functions. Instead use a freely available offline program like KeePass. A password manager will randomly generate unguessable passwords, remember them for you, and automatically use those saved passwords to log in to your secure sites," continues the guide. "The best offline password managers work on all your devices, be they desktops, laptops, smartphones, or tablets."

Al-Haqiqa recommends a Time-based One-Time Password algorithm (TOTP), but tells followers to be choosy: "Google has a TOTP app, but it is better if you pick an alternative open source application, so you would not even have to be connected to the internet."

"Never use any information about yourself that can be found in the public record. This includes birthdays, anniversaries, license plate numbers, or home addresses. Never make your password the same as your username. Never use recognizable keystroke patterns like ‘1qaz2wsx’ on a qwerty keyboard,” continues the tutorial. “…Never replace letters with numbers in a common dictionary word. Most botnets are keen to so-called ‘l33tspeak’ and will crack ‘Pr0ph3t’ just as fast as the word ‘Prophet’. Never use the ‘remember password’ option in your browser.”

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Previously she was an editorial board member at the Rocky Mountain News and syndicated nation/world news columnist at the Los Angeles Daily News. Bridget is a weekly columnist for the New York Observer and a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is a Senior Risk Analyst for Gate 15 and Washington Bureau Chief for PJ Media. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.*

AI advancement opens health data privacy to attack

Source: http://www.homelandsecuritynewswire.com/dr20181231-ai-advancement-opens-health-data-privacy-to-attack

Dec 31 – **Advances in artificial intelligence have created new threats to the privacy of health data**, a new UC Berkeley study shows.

The study, led by professor Anil Aswani of the Industrial Engineering & Operations Research Department (IEOR) in the College of Engineering and his team, suggests current laws and regulations are nowhere near sufficient to keep an individual’s health status private in the face of AI development. The research was released today on JAMA Network Open.

UC Berkeley says that in the work, which was funded in part by UC Berkeley’s Center for Long-Term Cybersecurity, Aswani shows that by using artificial intelligence, it is possible to identify individuals by learning daily patterns in step data (like that collected by activity trackers, smartwatches and smartphones) and correlating it to demographic data. **The mining of two years’ worth of data covering more than 15,000 Americans led to the conclusion that the privacy standards associated with 1996’s HIPAA (Health Insurance Portability and Accountability Act) legislation need to be revisited and reworked.**

“We wanted to use NHANES (the National Health and Nutrition Examination Survey) to look at privacy questions because this data is representative of the diverse population in the U.S.,” Aswani says. “The results point out a major problem. If you strip all the identifying information, it doesn’t protect you as much as you’d think. Someone else can come back and put it all back together if they have the right kind of information.”

“In principle, you could imagine Facebook gathering step data from the app on your smartphone, then buying health care data from another company and matching the two,” he explains. “Now they would have health care data that’s matched to names, and they could either start selling advertising based on that or they could sell the data to others.”

Aswani makes it clear that the problem isn’t with the devices, but with how the information the devices capture can be misused and potentially sold on the open market.

“I’m not saying we should abandon these devices,” he says. “But we need to be very careful about how we are using this data. We need to protect the information. If we can do that, it’s a net positive.”

Though the study specifically looked at step data, Aswani says the results suggest a broader threat to the privacy of health data. “HIPAA regulations make your health care private, but they don’t cover as much as you think,” he says. “Many groups, like tech companies, are not covered by HIPAA, and only very specific pieces of information are not allowed to be shared by current

HIPAA rules. There are companies buying health data. It's supposed to be anonymous data, but their whole business model is to find a way to attach names to this data and sell it."

Aswani says he is worried that as advances in AI make it easier for companies to gain access to health data, the temptation for companies to use it in illegal or unethical ways will increase. Employers, mortgage lenders, credit card companies and others could potentially use AI to discriminate based on pregnancy or disability status, for instance.

"Ideally, what I'd like to see from this are new regulations or rules that protect health data," he says. "But there is actually a big push to even weaken the regulations right now. For instance, the rule-making group for HIPAA has requested comments on increasing data sharing. The risk is that if people are not aware of what's happening, the rules we have will be weakened. And the fact is the risks of us losing control of our privacy when it comes to health care are actually increasing and not decreasing."

— Read more in Liangyuan Na et al., "Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning," JAMA Network Open (21 December 2018).

Wi-Fi "Vision" Poses Security Threat

Source: https://i-hls.com/archives/87886

Dec 31 – New research shows that ordinary Wi-Fi signals from smartphones can be used to "see" behind closed doors and track individuals in their own homes.

A group of scientists led by Yanzi Zhu at the University of California, Santa Barbara, have found a way to see through walls using ambient Wi-Fi signals and an ordinary smartphone.

They say the new technique allows an unprecedented invasion of privacy: "Bad actors using smartphones can localize and track individuals in their home or office from outside walls, by leveraging reflections of ambient Wi-Fi transmissions", according to technologyreview.com.

This Wi-Fi based tracking technology looks for changes in an ordinary Wi-Fi signal that reveal the presence of humans. A Wi-Fi "vision" would make walls and doors almost transparent. Wi-Fi "light" is the signal coming out of transmitters, and people as well as other bodies can be tracked according to how they reflect this "light".

But this is not done by producing an image. The data that Zhu and colleagues use is just a measurement of the signal strength at a specific location. That doesn't tell you anything about the location of the transmitter. And without knowing that, it's impossible to say where any human that distorts the field would be.

So, the first step in the researchers' approach is to locate the Wi-Fi transmitter. They do this by measuring the change in the signal strength as they walk around outside the target building or room.

It is even possible to work out exactly where the transmitter sits inside a house, because floor plans of most homes and offices in the US are downloadable from places such as real estate websites. All this can be done via smartphone apps.

It's not hard to imagine how a malicious actor might use this to work out if a building was occupied or empty.

The team say there are various defenses against this type of attack, such as geofencing Wi-Fi signals, but these are difficult to implement and have limited effectiveness. The most promising form of defense seems to be adding noise to the signals; the researchers are hoping to develop this in more detail in future.

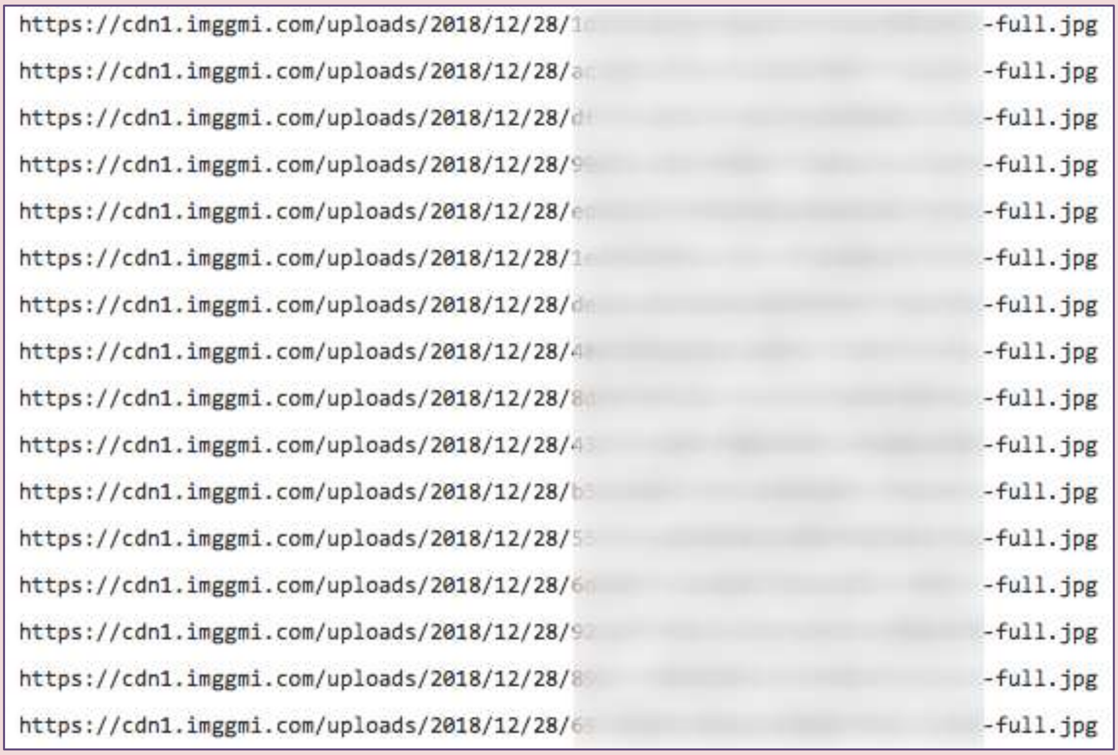
In the meantime, this work suggests that the mere presence of Wi-Fi signals is a significant risk to privacy. "While greatly improving our everyday life, [wireless transmissions] also unknowingly reveal information about ourselves and our actions," say Zhu and co. For the moment, this risk has been largely overlooked. That will need to change quickly.

Dark Overlord hackers vow to leak 9/11 related data stolen from law firm

Source: https://www.hackread.com/the-dark-overlord-hackers-leak-9-11-related-data/

Jan 01 – On Monday when the whole world was gearing up to celebrate New Year's Eve hackers from The Dark Overlord group made astonishing claims that they stole a trove of data from Hiscox Syndicates Ltd, a law firm responsible for handling insurance files related to 9/11 terrorist attacks.

This was reported by MotherBoard after a Pastebin announcement surfaced online in which hackers stated that they have also hacked Lloyds of London and Silverstein Properties. It is noteworthy that Hiscox supports international businesses via Lloyd's insurance market around the world.



```
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
https://cdn1.imggmi.com/uploads/2018/12/28/[redacted]-full.jpg
```

On the other hand, hackers maintain that Hiscox and Lloyds of London "are one of the biggest insurers on the planet." Moreover, while stating the reason for targeting the law firm hackers demanded ransom in Bitcoin and threatened to leak crucial 9/11 insurance related files if their demand is not met.

The stolen data according to the group includes emails, non-disclosure agreements, liability analysis, retainer agreements, defense formations, litigation strategies, settlements, collection of expert witness testimonies, testimonies, communications with government officials in countries all over the world, voice mails, dealings with the FBI, USDOJ, DOD and other confidential communication.

According to the group's Pastebin post, Hiscox is well aware of the attack and paid the initial ransom but breached its agreement by involving law enforcement authorities.

"This involvement with law enforcement became clear to us months later through a source of ours disclosing details of the client to us that we never informed the source about. We were absolutely appalled by this transgression against our agreement. We decided to offer this company a second chance to repent, accept responsibility, and satisfy our penalty request. They declined to accept our offer, so we're here today," the post said.

To prove their hack, The Dark Overlord hackers also published 16 screenshots of the firm's internal communication. It also published a download link apparently containing 10GB of encrypted data whose decryption keys will be published later on their official Twitter account or on a Dark Web form called "KickAss."

"If a full public release happens in the near future, we'll guarantee that we're going to withhold only the most highly confidential and sensitive documents for private sale. For the rest of you: don't worry, there's thousands of documents still to go around," the group said.

"If you're one of the dozens of solicitor firms who was involved in the litigation, a politician who was involved in the case, a law enforcement agency who was involved in the investigations, a property management firm, an investment bank, a client of a client, a reference of a reference, a global insurer, or whoever else, you're welcome to contact our e-mail below and make a request to formally have your documents and materials withdrawn from any eventual public release of the materials. However, you'll be paying us," the Pastebin post said.

The Dark Overlord is a notorious group of hackers known for targeting banks, healthcare insurance firms, plastic surgery clinic, media giants like Netflix, Steve Harvey's Funderdome TV show. The group went on to leak student data and sent death threats to an Iowa based Johnston Community School District forcing it to close some of its schools. The messages were sent to parents via text included physically harming their kids and even killing them.

In May 2018, Serbian authorities arrested a 38-year-old man from Belgrade suspected of being one of the members of The Dark Overlord hacking group. However, based on its recent attack it is not rocket science to realize the group is alive and still haunting its victims'

Online Jihad: 5 Things Terrorists Told Us in 2018 About Future Plans

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/terrorism-study/online-jihad-5-things-terrorists-told-us-in-2018-about-future-plans/

Dec 31 – Regardless of the physical territory occupied by ISIS at the end of 2018 or the amount of land al-Qaeda controls in Yemen, the online space functions as terrorists' kitchen table: no matter where in the world, no matter their background or day job or language, this is where jihadists gather for support, recruitment and inspiration. The past year's content reflected terror groups and lone operatives eagerly embracing this borderless realm, and sent some distinct messages about how online jihad has evolved and where it's headed.

Disinformation Ops Aren't Limited to Politics

Terror groups aren't blind to the disinformation campaigns that have permeated electoral processes, sharply tailored to specific audiences with half the story or full-on fake news. They know that, similarly, spinning the right bit of disinformation can help with recruitment and attack encouragement. ISIS crafted its own Kremlin-worthy dezinformatsiya campaign soon after the Oct. 1, 2017, massacre at the Route 91 Harvest country music festival in Las Vegas, claiming through their Amaq news agency that the "Las Vegas attacker is a soldier of the Islamic State who carried out the attack in response to calls for targeting coalition countries."

Yet even as it became readily apparent that Stephen Paddock had no apparent ideological motive, ISIS persisted – through both official and unofficial channels – in claiming the shooter as their own, even granting him the kunya "Abu Abdul Barr al-Amriki." The claims lasted into 2018; a January propaganda image released by the ISIS-supporting Wafa' Media Foundation warned "Las Vegas' massacre is not far from you," and showed crosshairs and flames positioned over the Planet Hollywood Resort & Casino on the Las Vegas Strip. Vegas images were included in a January video from ISIS' official Al-Hayat Media Center using a nasheed to call on Westerners to "go answer the call, don't spare none, kill them all, it is now time to rise, slit their throats, watch them die."

As the year rolled on, the deza op transformed from outright claims to holding Paddock and his crime aloft as inspiration for jihadists, from his high sniper vantage point to the choice of target. Their campaign had many months to gain traction and plant seeds in the minds of would-be jihadists before the August Las Vegas Metropolitan Police Department report noting Paddock "was not a religious person, did not believe in any higher power, and found religious people to be ridiculous."

The 'You, Too, Can Jihad' Campaign

Another big theme in 2018 recruitment propaganda was accessibility. Terror groups will always have a soft spot for training camp videos showing recruits jumping through flaming hoops – they're self-styled "lions," after all – but they also want the guy who can't manage a pull-up to cook up an IED or poison a salad bar. They're not exactly required to ace a Quranic knowledge exam, either: As al-Qaeda in the Arabian Peninsula emir Qasim al-Raymi said in a 2017 inclusivity spiel, jihad is for the "pious and immoral" alike. Simple messaging underscores the "come as you are, just attack" messaging, from the ISIS lone-jihadist slogan "Just Terror" to al-Raymi telling would-be attackers to "take it easy" and not stress out while prepping for an assault.

In a January ISIS video, a visually impaired Kazakh jihadist called for attacks, following another release from al-Hayat Media Center featuring an American-accented ISIS fighter with one leg who called on Western supporters, including the disabled, to conduct knife or gun attacks.

Emphasizing that they want jihadists from all walks of life and levels of ability, ISIS released a February video showing a wheelchair-bound jihadist being loaded into an IED-outfitted pickup before driving off to his target and detonating the device. "It's true that I'm disabled, but I've been given a lot of suggestions in terms of areas I could work in… I'm not doing this out of weakness, or because of any anguish or suffering," Abu Abdillah Ash-Shami tells the camera before becoming a suicide bomber. In other parts of the video, jihadists were shown in dusty battle scenes using crutches or being pushed in a wheelchair by a comrade.

Terror groups are not only encouraging outside-the-box recruits, but attack methods. An online propaganda poster distributed this month by al-Ansar, one of the many ISIS-supporting media groups, directed the "lone lion" to "kill the infidels in ways which no one else ever used," with suggestions including snakes, electrocution, poisoned arrows and unleashing wild animals.

Tech Strategy Rolls with the Changes

Terror groups are acutely aware of how technology has aided their borderless growth, and equally aware of how important tech training is to their followers to keep them under the radar. Al-Qaeda accounts still seem to fly under that radar with greater ease – the group's As-Sahab media arm launched a WordPress site in November featuring speeches, latest news and video archives and it remained live for weeks, while AQAP propaganda was available for free download on BarnesAndNoble.com until early this year and Anwar al-Awlaki lectures were available in a Google Play app – while ISIS staked out new cyber territory in an effort to evade the censors.

ISIS still loves Telegram, but faced with suspensions they've been trying out Viber along with forging down other avenues including WhatsApp. An Indian youth told police in July that he had received WhatsApp messages from numbers in Memphis, Tenn., and Starkville, Miss., trying to threaten him into gathering information for ISIS. Terror suspects have been found to be participating in private ISIS WhatsApp chats. What's key to terror groups is that they can utilize diversified social media to recruit new members, keep open lines of communication among adherents, spread propaganda and remind others of their obligation to do the same in a "media jihad" campaign.

Jihadist leaders take cybersecurity seriously, not just trying to infiltrate disbelievers' domains and fundraise with Bitcoin but ensuring that followers follow basic password hygiene (stop using "123456," says al-Qaeda) and encryption protocols. In a January video, al-Raymi railed against cell phones as "a form of a spy agent – an agent that is always with us."

"When you see what is going on in the web forums you will be surprised," al-Raymi said. "The transgression against the work of the mujahidin that goes on is unbelievable. They expose mujahidin's vision and plans, and then go on to open an open debate in a chat room."

Indie Is the New ISIS

This year, the online haunts of ISIS were flooded with posters, videos, and reading materials originating not from the official ISIS media shop but crafted by independent media groups wholeheartedly behind the mission. While ISIS still operates official media, including the weekly *al-Naba* newsletter, this army of volunteers has effectively blurred that line between official direction and unofficial inspiration. The unofficial messaging is stark and simple, follows an editorial calendar that includes campaigns calling for holiday attacks, and seizes quickly on attacks to try to push copycats into waging their own jihad.

In October, the Justice Department charged Ashraf al Safoo of Chicago, whose day job was in website development and whose side gig was allegedly cranking out indie propaganda as a member of the Khattab Media Foundation. "Brothers, roll up your sleeves! Cut video publications into small clips, take still shots, and post the hard work of your brothers in the apostate's pages and sites. Participate in the war, and spread fear," he allegedly posted online in May.

Just in the past couple of months, ISIS-backing media groups have called for grenade and cleaver attacks on concerts, urged use of off-the-shelf drones to augment jihadist activities, suggested opportunistic crowded targets such as the France "yellow-vest" fuel protests, threatened specific locations from the U.S. Capitol to the UN Security Council or downtown Toronto, depicted a gunned-down Santa Claus, and more. It may sound like just noise from fanboys with too much time and Photoshop, but not to the impressionable: Everitt Aaron Jameson, who pleaded guilty this year to plotting a Christmas 2017 attack in San Francisco, loved with a heart on Facebook one of those indie calls for attacks depicting Santa overlooking Times Square with a box of dynamite at his side.

Bioattacks on Their Mind

Terror groups, particularly the independent ISIS-supporting groups, showed distinct curiosity in their communications this year about branching out into bio, agricultural or chemical attacks. It's certainly not a new passion of theirs, but ISIS supporters – while not claiming responsibility for sticking needles in fruit – used Australia's strawberry contamination crisis this year to gin up more threats and suggestions. "O Crusaders! We will never allow you to enjoy the taste of what you desire," said one poster that depicted a small bottle of poison and a bowl containing grapes, apples and oranges. "O Crusaders, We will make you check everything and anything you eat out of fear, horror and terror," said another image of strawberries, a poison bottle and a photo of the Sydney Opera House. Yet another poster from ISIS supporters simply showed the word "Australia" as a man clutched his stomach.

Al-Faqir, one of the ISIS-backing media outlets, released a video in July discussing how to wage a bioattack on the West "that cannot be detected or tracked" by authorities. "Sprinkle the liquid substances or the basics of bacteria with drinking water to take effect automatically," the video advised would-be jihadists. "Sprinkle the crushed material on exposed fruit and public foods or scatter them in the air in crowded places — with caution." An Al-Taqwa Media Foundation poster distributed in December conspicuously was plastered with biohazard warning symbols – "You have realized the danger of the Islamic State. But you did not know the treatment, and you will not know the treatment, because there is no treatment!" read the text – while an image from another group showed radiological warning symbols on a home with the ISIS "Just Terror" slogan.

Their flourishing interest comes amid floundering interest in biodefense in many quarters. Former Sen. Joe Lieberman (I-Conn.) said at an October meeting of the Blue-Ribbon Study Panel on Biodefense that, while a bioattack is coming with "reasonable certainty," the "bottom line is we don't think we're ready." He added that "fear is a great motivator" in homeland security, but "certainly with regard to a bioterror attack the fear level is down."

***Bridget Johnson** is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Previously she was an editorial board member at the Rocky Mountain News and syndicated nation/world news columnist at the Los Angeles*

Daily News. Bridget is a weekly columnist for the New York Observer and a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is a Senior Risk Analyst for Gate 15 and Washington Bureau Chief for PJ Media. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.

10 Largest Data Breaches in 2018

Source: https://i-hls.com/archives/87932

Jan 02 – Data breaches compromised the personal information of millions of people around the globe in 2018. Data breaches are security incidents in which information is accessed without authorization. They can happen for a variety of reasons, e.g. hacking, data can be mishandled or sold to third parties, holes in a website's security system, etc.

The data breach that caused the largest number of users affected was against India government ID database.

Here are the 10 biggest data breaches that were revealed this year, ranked by the number of users affected, according to businessinsider.com:

10. Facebook — 29 million

This breach affected highly sensitive data, including locations, contact details, relationship status, recent searches, and devices used to log in between July 2017 — September 2018.

"The hackers were able to exploit vulnerabilities in Facebook's code to get their hands on 'access tokens' — essentially digital keys that give them full access to compromised users' accounts.

9. Chegg — 40 million

Personal data including names, email addresses, shipping addresses, and account usernames and passwords were affected. An unauthorized party gained access to an American education company database that hosts user data, according to ZDNet.

8. Google+ — 52.5 million

Private information on Google+ profiles was affected, including name, employer and job title, email address, birth date, age, and relationship status. A software glitch caused Google to expose the personal profile data of 500,000 Google+ users. Google has decided to shut down Google+ for good in April 2019.

7. Cambridge Analytica — 87 million

Facebook profiles and data identifying users' preferences and interests were were compromised. In 2015, a personality prediction app called "this is your digital life," improperly passed on user information to third parties that included Cambridge Analytica, a data analytics firm that assisted President Trump's presidential campaign by creating targeted ads using millions of people's voter data.

Only 270,000 Facebook users actually installed the app, but due to Facebook's data sharing policies at the time, the app was able to gather data on millions of their friends.

6. MyHeritage — 92 million

This breach affected email addresses and encrypted passwords of users who have signed up for the service, as they were sitting on a private server somewhere outside of the company.

5. Quora — 100 million

The breach affected account info including names, email addresses, encrypted passwords, data from user accounts linked to Quora, and users' public questions and answers. A "malicious third party" accessed one of Quora's systems, according to Reuters.

4. MyFitnessPal — 150 million

Usernames, email addresses, and encrypted passwords were affected when an "unauthorized party" gained access to data from user accounts on MyFitnessPal, an Under Armour-owned fitness app.

3. Exactis — 340 million

Detailed information compiled on millions of people and businesses including contact details, personal interests and characteristics, and more was affected. A security expert spotted a database "with pretty much every US citizen in it" left exposed "on a publicly accessible server," although it's unclear whether any hackers accessed the information, according to WIRED.

2. Marriott Starwood hotels — 500 million

Guest information including phone numbers, email addresses, passport numbers, reservation dates, and some payment card numbers and expiration dates was compromised by hackers who accessed the reservation database for the hotel chain and copied and stole guest information.

1. Aadhar — 1.1 billion

This breach affected private information on **India** residents, including names, their 12-digit ID numbers, and information on connected services like bank accounts. India's government ID database, which stores citizens' identity and biometric info, experienced "a data leak on a system run by a state-owned utility company Indane." Indane hadn't secured their API, which is used to access the database, which gave anyone access to Aadhar information, according to ZDNet.

Next Cyber Threats – 2019 Forecast

Source: https://i-hls.com/archives/87996

Jan 03 – As 2018 ends, it's crucial to step back and reflect on some cybersecurity realities. Although US government cybersecurity teams do their best to confront hacking attempts, the lack of time and tight budgets make it difficult to respond to the evolving threat vector. Meanwhile, the attack surface has broadened due to the number of connected devices and data flowing through organizations – devices and data that many employees need access to in order to get on with their jobs.

Things are probably only to get more complicated in 2019, when the issue of trust will be thrust to the forefront of agencies' cybersecurity challenges. In 2019, more government agencies will be placing trust in cloud providers to protect their data. They'll also be placing trust in the individuals that access and manage their data, even as the security of personal biometric data comes into question. Federal government agencies in the US should have on their radar two major threats, according to fifthdomain.com:

Industrial IoT threat

In 2019, the Internet of Things is going to be among the most challenging area of security. The risk is growing as more devices get connected and as network connectivity moves further to the edge. When such devices are exploited through cloud infrastructure, the result is significant disruptions for governments deploying smart cities and using networks for everything from public transit to disaster management.

In particular, connected devices within manufacturing environments, i.e., the Industrial Internet of Things (IIoT), are extremely desirable targets for attackers, as they offer access to the underlying systems of multi-tenanted, multi-customer environments. As control systems evolve, they are patched, maintained, and managed through cloud service providers. Since processor speed is critical to performance for IIoT, it's chosen more often over security.

Moreover, many cloud providers simply don't offer strong enough isolation for a multi-tenant architecture or multi-customer applications, leaving IIoT devices vulnerable. Agencies will need to move from visibility to control where their IT and operational technology networks converge.

Authentication challenge

As biometric and facial recognition software become prime targets for hackers, protecting identity information will continue to be an ongoing challenge in 2019. Email addresses, passwords, and personalized questions are no longer sufficient to protect identities online, but even two-factor authentication and biometric authentication may not be enough. This is especially surprising, because it uses unique data such as fingerprints, movements, and iris recognition. Facial recognition especially has gone mainstream thanks to the Apple iPhone X, but even this seemingly secure technology has serious vulnerabilities.

To combat this, federal agencies should use behavioral biometrics, which provide a continuous authentication layer. Behavioral biometrics recognize identifiers such as mouse movement and scroll speed, which are far harder to mimic, and can be paired with facial recognition or other security measures for layered protection.

In sum, having visibility into the cyber behavior of end-users is crucial to reacting quickly to threats — and to correctly identifying what's a threat and what's an employee legitimately trying to get their job done.

The quiet threat inside 'internet of things' devices

By Charles T. Harry

Source: http://www.homelandsecuritynewswire.com/dr20190115-the-quiet-threat-inside-internet-of-things-devices

Jan 15 – Governments, too, are getting into the act – cities, especially, want to use new technologies to improve energy efficiency, reduce traffic congestion and improve water quality. The number of these "internet of things" devices is climbing into the tens of billions. They're creating an interconnected world with the potential to make people's lives more enjoyable, productive, secure and efficient. But those very same devices, many of which have no real security protections, are also becoming part of what are called "botnets," vast networks of tiny computers vulnerable to hijacking by hackers.

As Americans increasingly buy and install smart devices in their homes, all those cheap interconnected devices create new security problems for individuals and society as a whole. The problem is compounded by businesses radically expanding the number of sensors and remote monitors it uses to manage overhead lights in corporate offices and detailed manufacturing processes in factories. Governments, too, are getting into the act – cities, especially, want to use new technologies to improve energy efficiency, reduce traffic congestion and improve water quality.

The number of these "internet of things" devices is climbing into the tens of billions. They're creating an interconnected world with the potential to make people's lives more enjoyable, productive, secure and efficient. But those very same devices, many of which have no real security protections, are also becoming part of what are called "botnets," vast networks of tiny computers vulnerable to hijacking by hackers.

Botnets have caused problems on the internet, from sending vast amounts of spam mail to disrupting websites around the world. While traditionally most botnets are comprised of laptop and desktop computers, the growth of unsecured devices such as industrial sensors, webcams, televisions and other smart home devices is leading to a growing disruptive capability.

Tiny computers everywhere

The "internet of things" includes countless types of devices – webcams, pressure sensors, thermometers, microphones, speakers, stuffed animals and many more – made by a vast array of companies. Many of these manufacturers are small and unknown, and don't have popular brands or public reputations to protect. Their goals are to produce lots of devices to sell as cheaply as possible. Customers' cybersecurity isn't a real concern for them.

These devices' variety means they're useful for lots of things, but also means they have a wide range of vulnerabilities. They include weak passwords, unencrypted communications and insecure web interfaces. With thousands, or hundreds of thousands, of identically insecure devices scattered all over the world, they're a wealth of targets ripe for the hacking.

If, for instance, a manufacturer has set an unchangeable administrative password on a particular type of device – it happens more often than you might think – a hacker can run a program searching the internet for those devices, and then logging in, taking control and installing their own malicious software, recruiting the device into a botnet army. The devices run normally until the hackers' issue instructions, after which they can do more or less anything a computer might do – such as sending meaningless internet traffic to clog up data connections.

Blocking internet access

That type of attack when emanating from thousands of devices at once, called a "distributed denial of service," can shut down companies' servers or even block wide swaths of the internet from being publicly accessible. A major DDoS attack in 2016 interrupted connections to Amazon, Netflix and Paypal from customers on the east coast of the U.S.

That attack was linked to a botnet-control software program created by three teenagers seeking to use more than 100,000 hijacked webcams and other internet-connected devices from around the world to gain an advantage over other players of the "Minecraft" online video game.

The size and scale of these attacks – and the broad range of devices that can contribute to them – make this both a private problem and a public one. People want to secure the devices in their homes and pockets, of course. Yet the same networks that stream television shows and music also link burglar alarms to police, manage traffic lights in congested areas and let self-driving cars talk to each other.

All that activity can be drowned out if hackers flood the internet, or sections of it, with meaningless messages. Traffic would stall across towns, even counties, and police officers would have a hard time communicating with each other to try to straighten everything out.

Even small devices, in their hundreds of thousands, all around the world, can work together to have huge repercussions both online and in the physical world.

__Charles T. Harry__ is Associate Research Professor of Public Policy; Director of Operations, Maryland Global Initiative in Cybersecurity; Senior Research Associate, Center for International and Security Studies, University of Maryland.

Cyber Trends and Threats – A Review of 2018 and Expectations for 2019

By Tomer Nuri (CTO *and* VP of Technologies in Malam Team)
Source: https://i-hls.com/archives/88322

Summary of 2018

2018 has begun with a recovery from the events of 2017 such as WannaCry, Petya, and the information leak from Equifax – an event that preoccupied the industry throughout 2018 and will serve the negative model for cyber crisis management.

2018 has brought with it new events and consequent threats. One of the worst events of the year in cyber security was the hacking of the Marriott chain after purchasing Starwood and the exposure of personal information of over 500 million customers, an event that was spread onto four years. Alongside information leaks that were the result of hackers' malintent, 2018 had also other reasons for cyber security breaches. It had processes where sensitive information was exposed as a result of error or negligence, usually events of data mobility like the transference of infrastructure and data to cloud servers, decentralization, operating advanced interfaces (API), etc. In this category we could recall the exposure of Exactis' database, and the event of personal information exposure on Twitter, resulting from improper data security procedures.

In 2018, which was expected to be the year where privacy regulations would advance both locally and globally, including GDRP, we were acquainted with much unauthorized and improper sharing of information through social media to third party companies (such as Facebook and its cooperation with Cambridge Analytics). Information breaches have increased in cloud servers because of the data's availability, but the same migration of information had drawn hostile agents anywhere it was to be found, while hackers have focused in places where accessibility to info was highest. This was especially prevalent in digital and mobile applications.

in 2018, out of 600 information-leak events, a significant portion was done on application infrastructure like fitness, recreation and lifestyle apps such as Under Armor, Ticket Fly, Pumpup and My Heritage. Noted cyber events included the spreading of false information in legitimate science channels (in a disinformation model, or "fake news"), which took shape in different political campaigns. On the national level 2018 was bound with significant cyber campaigns and attacks by Russia and Iran. A lot of focus was put on information leaks in big corporations and on tapping into research and different academic networks in the world alongside critical infrastructure.

In the field of critical infrastructure there was seen a sharp increase in the amount of threats from IoT and OT networks while the main targets being the user (either locally or as a product of working procedures), the points of interface between OT and IT, and high vulnerability and lack of professional personal for arresting events throughout time.

2018 has raised awareness to critical national infrastructure such as weapons platforms, atomic energy infrastructure, and emergency systems (such as the Triton event which was identified in the TRICONEX system of Snyder Electronics) alongside IoT networks that have come to be intricate and more common. 2018 has seen an increase in the complexity of IoT systems, and the transition from focusing on DDOS events to complicated network events that work on the same plane with applicative interfaces (API), which exploit this plane for multi-system campaign cyber attacks whose purpose is the diversion of traffic, surveillance, etc. (such as the VPNFILTER event).

Cyber criminal groups have signalled their presence throughtout the web in 2018, where small criminal groups merged into criminal syndicates with resources and the ability to cope with enforcement, both physically and cybernetically. Alongside this, there was also seen a change in the model of ransomware, with a transition to localized threats combined with other kinds of threat.

Trends in 2019

Significant Challenges in Information Security and Privacy

The challenge in the cyber defense model for protection against cyber threats stems from a short exposure time and from a lack of adequation to a long-time frame required for identification and recovery. This challenge will worsen due to threats a new model that will allow for reduced time lapses from the moment of exposing the weakness to the moment of "arming" the Exploit.

The risk for information leaks will increase due to the hackers' shift of focus to the places where information is vulnerable including mobile and cloud-based apps, alongside information exposure risks that will grow due to insecure info migration.

2019 will be the year where Data Custodians, which is to say information managers entrusted with data security, will have to take initiative action in order to guard our information. They will be required to heavier enforcement of privacy and data protection. This will be done in accordance with the enforcement of local and international regulations such as the GDRP, according to the demand of the interests of the relevant organizations.

Artificial Intelligence as Both Protection and Threat

Artificial Intelligence Technologies (AI) found in the forefront of analytical cyber defense systems will continue to root themselves in defense systems, but in 2019 AI technologies are also expected to form the basis for complex security threats. AI technologies could serve hackers in quickly identifying weaknesses, in the automation of attack procedures, and in creating elaborate campaigns of Social Engineering alongside the improvement of mechanisms for bypassing defense systems, hacking of WEB services defenses, and further mechanisms whose aim is to identify a human user, or a machined BOT, etc.

Threats on Critical Infrastructure

2019 is expected to see an escalation in threats posed on critical infrastructure, both in focusing on strategic-national ones such as energy, water, industry and the like, and also by a focused threat on ICS and IoT infrastructure, both public and private. Focusing on these two sectors will force the move from network-based events to more "secret" threats, allowing the operation of a multi-system and multi-phased threat.

Complex Threats

2019 is expecting a rise in Cryptocurrency BOT threats, whose source is in the access to different WEB services. Activating such a threat will give rise to to both decentralized and inclusive events.

A more extensive use of Best of Breed threats is expected this year, in the form of threats that combine a number of attack mechanisms used in a troubling synergy. This model will create a challenge difficult to ignore for cyber security personal since it requires an accordance with procedures for arresting and classifying events.

New Defense Methodologies and Technologies

The dangers in information leaks alongside the increase of network threats coming from the use of Lateral Movement technologies by attackers will lead to a wider implementation of the Zero Trust conception in both business and critical networks, together with the application of advanced analytical defense technologies.

The need for advanced Network Visibility infrastructure will increase throughout 2019 due to the need of dealing with a growing complexity of media networks, the wide migration to cloud servers, and the adoption of micro-nano segmentation conceptions alongside the increase in the amount of encrypted traffic.

The growing lack in professional personnel in the cyber field will require, in 2019 more than ever, an investment in the enrichment of teleprocessing personal using the different technologies, and the application of automation and rapid response time to threats.

Smart Cities. Is it Wise to Get Smarter?

Source: https://i-hls.com/archives/88394

Jan 20 – We are in an era of intelligent and urgent urban innovation. Our homes are connected, our streets are thriving labyrinths of interconnectivity, and our businesses are a hive of data streaming and surveillance. Communities are now emerging as sophisticated centres of technical excellence, prompting micro and macro revolutions in virtually every aspect of our lives. Across the world, digital “smartness” is either being activated, enhanced, evangelised or considered a transformative option. Is this trend a good one?

As the popularity and inevitability of smart cities expand (i.e. technology to improve energy use, transport systems or other infrastructure), so too does a cybercriminal’s opportunistic attack surface. Are we now putting the public’s data and infrastructure at an unprecedented risk? Are we the authors of a 21st century tale of two cities where one is hyperconnected and vulnerable and the other overly cautious and developmentally moribund? More importantly, what the Dickens can we do to get the balance right?

The race to evolve

Urban business-as-usual will not work. Population growth and dwindling resources are driving mass migrations to the worlds’ cities, and present infrastructures are incapable of pre-empting and adapting to the consequences – much less achieving optimal, equitable living environments in the long term.

One of the smart cities’ most compelling promises is the capacity to address traditional problems with data-driven incision, mining insights from countless sensors, interactions, and behaviours. There are numerous associated economic benefits to this technological shift. According to a recent whitepaper by ABI Research, worldwide smart city technologies could unlock more than $20 trillion in additional economic benefits in the next decade.

Europe has big ambitions to take advantage. 2017 European Parliament research claims that the region already has 240 cities at over 100K in a population with some smart city features in place. By the end of 2019, the Smart Cities and Communities European Innovation Partnership predicts there will be 300 smart cities in play.

A future of symbiotically connected communities, services, and processes is undeniably an admirable vision. However, with all the pressures to move at pace, there are growing concerns that cybersecurity risks are inadequately anticipated or managed.

Unfortunately, many devices, systems, and technologies powering today’s smart city dream are still being developed without appropriate security architectures or threat mitigation solutions. This short-sightedness can cause a raft of vulnerabilities leading to serious issues threatening livelihoods and, in some cases, life itself. A hacker commandeering a smart parking meter may be a nuisance but a cybercriminal infiltrating a nuclear plant could cause cataclysmic repercussions.

Lessons learned

At this year’s Black Hat conference, IBM’s X-Force Red Team examined existing municipality technologies to determine the possibility of “supervillain” style attacks.

Researches focused on four common devices and found 17 vulnerabilities, of which nine were deemed critical. One European country was using a vulnerable device to detect radiation. In the US, it was a system monitoring traffic control. The vulnerabilities in question on both occasions were not complex — the vendors simply failed to implement basic security measures.

To spook us even more, IBM’s researchers went on to simulate an attack on devices that monitor water levels in dams. In less than a minute, they were able to flood surrounding areas. The simulated hack was on a commonly used piece of smart city tech and was easy to hijack causing widespread mayhem.

Architecting the future

The U.N. predicts that two-thirds of the world's population will reside in densely packed megacities by 2030. This means a mass of technology coming online fast, especially with the advent of 5G, and this could potentially fuel boundless IoT fantasies and realities.

Business leaders, tech disruptors, developers, service providers, and planners need to ramp up collaboration with industry regulators and ecosystem partners urgently to ensure appropriate rollouts of secure, seamless networks and devices. The tech industry at large should also do more to ensure the principle of 'security-by-design' is embraced throughout the entire infrastructure development ecosystem. Furthermore, end-to-end security has to improve, including tighter authentication of users as well as enforced policies for all communication paths. At the same time, service providers have to enhance their privacy-focused data encryption capabilities with the latest advanced software.

In summary, we need governments, city planners, and business leaders to start heeding the warnings signs of growing cybercrime and include cybersecurity experts at all stages, from design and construction to infrastructural management and beyond. We all want smarter cities, but we need to get wiser at navigating the threat landscape to stay streets ahead of cybercriminals.

*By **Keiron Shepherd,** Senior Security Specialist, F5 Networks*

C²BRNE DIARY

DRONE NEWS

Building Trust in Passenger Drones

Source (video): https://i-hls.com/archives/87628

Dec 22 – A new passenger drone could be a steppingstone to a new form of convenient urban transportation. The electric-powered vertical-takeoff-and-landing aircraft, the Hexa is currently targeting recreational crowd.

Matt Chasen, CEO of startup LIFT Aircraft is a former Boeing engineer with a background in mechanical and aerospace engineering. He explains that "today's regulatory environment does not allow for a transportation use of these aircraft — yet" but his company will "build public trust in the technology. Once that happens, it's inevitable that people will want to use it for certain types of commuting flights," even if it will take years.

To operate the Hexa, Chasen said, customers will undergo an orientation that includes watching safety videos and training in a virtual-reality simulator for up to an hour. A basic proficiency test will follow, then preflight checks with ground support.

According to washingtonpost.com, the drone-like aircraft — which is controlled using a joystick in the cockpit and stabilized by a flight computer — **weighs 432 pounds, seats one person, and has 18 sets of propellers, motors and batteries. Prospective pilots have to weigh less than 250 pounds.**

During flight, pilots can see safety information on an augmented-reality display inside the aircraft. In the event of an emergency, he said, flight controllers can take over the aircraft and fly it remotely like a drone. The aircraft can travel just over 60 mph at top speed and includes air-cushioned floats, allowing it to land on water if necessary.

The company hopes to begin offering 15-minute flights over a popular lake outside Austin next year. It is also considering 25 cities across the US for other "aircraft hubs," which would be located near tourist destinations and entertainment areas. Though the cities have yet to be named, the company is already accepting reservations.

Chasen said he doesn't think the FAA will certify vertical-takeoff-and-landing aircraft for commercial transportation until they're proved safe. Once that happens, he said, a new wave of alternative transportation is likely to quickly emerge.

EDITOR'S COMMENT: Although I am a great fan of technology and innovations, I would strongly advice to forbit further development of passenger drones. Can you imagine what a terrorist could achieve in urban environment? Conventional or asymmetric, the effect and the consequences could be enormous. In addition, the perpetrator could escape over the roofs before the activation of any flying response. We failed to prohibit the transfer of military UAV technology into civilian commercial production lines and now the situation is uncontrollable despite regulations and penalties. At least we have the time to stop passenger drones.

Israeli Technology Defeated Gatwick Airport Drones

Source: https://i-hls.com/archives/8765

Dec 23 – The British Army used a cutting-edge Israeli anti-drone system to defeat the unmanned aerial vehicle (UAV) that brought misery to hundreds of thousands of people at Gatwick airport.

At first, the Police had been seen with an off-the-shelf DJI system that tracks drones made by that manufacturer and shows officers where the operator is. However, the drone used at Gatwick is thought to have been either hacked or an advanced non-DJI drone, which rendered the commercial technology used by the police useless, reports dailymail.co.uk.

At that point, the Army's 'Drone Dome' system made by the Israeli Rafael was called in.

Six 'Drone Dome' systems were bought by the British Army in 2018 for £15.8 million. A similar system was used by British and US special forces to protect them from drones while liberating Mosul in Iraq and neutralise ISIS drones in Syria, but passengers trapped at Gatwick are furious the weapons were not brought in earlier.

Army officers use a high-tech radar and a laser rangefinder to locate drones within a 2.1- and 6.2-miles radius. Once the system has a lock on the drone, a radio frequency jammer is then used to overload the drone with signals – knocking out the commands from the unknown owner.

This can be used to make a 'soft-kill' and cease control of the unmanned aerial vehicle (UAV) and land it safely.

The British Army did not buy a version equipped with a high-powered laser which can make a 'hard-kill' on drones by effectively melting them.

The system is an 'end-to-end system designed to provide effective airspace defence against hostile drones used by terrorists to perform aerial attacks, collect intelligence, and other intimidating activities', according to Rafael. It uses four radars to give full 360° coverage to scan the entire skyline. **This detection process can spot transport aircraft from about 31 miles away but for a smaller UAV, like the one used to terrorise Gatwick, the 'Drone Dome' can only offer a detection range of between 2.1 and 6.2 miles.**

The system allows the authorities to perform a ‘soft-kill’ when the detection programme is integrated with the radio frequency jammer. An antenna made of gallium nitrate is used and this allows the tech to be portable and easy to set up.

Police were forced to turn to the military devices after failing with commercially available technology. They first tried to identify the location of the drone and its operator by using a briefcase-sized piece of commercially available equipment called AeroScope. It is believed to be **on loan** at Gatwick airport from COPTRZ, however, it is only able to identify DJI drones from the extensive database provided by the Chinese manufacturer. This ground-based device is used throughout industry and at many events to ensure protection from drones.

EDITOR’S COMMENT: The conclusion is that the second busiest airport of the capital of the United Kingdom could not afffort to pay ~263,000 UKP to have such a system ready at anytime! Most probably because all the illegal UAV flight were supposed to happen at Heathrow or Luton airports! History repeats itself – boring! Sorry COPTRZ! This time your free offer did not pay back! In the meantime, check the device again to see if it works effectively in protecting industrial settings and target

Terror Challenges Include Potential Drone ‘Swarm Attacks,’ ‘More Subtle’ Extremist Activity

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/terror-challenges-include-potential-drone-swarm-attacks-and-more-subtle-extremist-needles-in-haystacks/

October 2018 – The current terror threat landscape includes a growing threat from drone use — including in potential “swarm” attacks — and diverse extremist groups metastasizing in an online space impervious to military action, national security leaders told Congress.

FBI Director Christopher Wray reminded the Senate Homeland Security and Governmental Affairs Committee at a Wednesday hearing on threats to the homeland that the landscape has changed “significantly” since 9/11, with not just the threat of al-Qaeda attacking a large city in “spectacular” traditional fashion but the ISIS method of using social media “to lure people in and inspire them remotely to attack whenever and wherever they can.”

“And we now face homegrown violent extremists, or HVEs, who self-radicalize at home and are prone to attack with very little warning. This HVE threat has created a whole new set of challenges with a much greater number, much greater volume of potential threats, and each one of them with far fewer dots to connect and much less time to prevent or disrupt an attack. These folks are largely radicalized online and they’re inspired by the global jihadist movement,” Wray said.

The director confirmed to lawmakers that “right now, as I sit here, we’re currently investigating about 5,000 terrorism cases across America and around the world,” with about 1,000 of those cases homegrown violent extremists spanning all 50 states.

Among the FBI’s recent successful disruptions of attack plots, Wray noted, have been the plan of Everitt Aaron Jameson, 27, of Modesto, Calif., to attack Christmas tourists on San Francisco’s Pier 39 and the June arrest of Cudahy, Wis., resident Waheba Issa Dais, 45, for maintaining a virtual library for jihadists of instructions on how to make bombs, biological weapons, poisons and suicide vests.

“In the cyber arena, the threat continues to grow, and the more we shift to the internet as the conduit and the repository for everything we use and share and manage, the more danger we’re in,” Wray added.

Russell Travers, acting director of the National Counterterrorism Center, said that despite “a lot of good news” when it comes to strengthening America’s defenses, including aviation security measures and border control initiatives, “we need to be cautious, because challenges remain.”

“Military operations have bought us time and space as we address a global terrorist threat, but the diverse, diffuse and expanding nature of that threat remains a significant concern,” he told the committee. “…The world has a lot of work to do in the non-kinetic realm to deal with radicalization and underlying causes.”

Terrorists have also proven “innovative” when it comes to their “ability to exploit technology and the attributes of globalization” for planning and disseminating propaganda.

“We’re in the early stages of seeing terrorist use of drones and UASs for swarm attacks, explosive delivery means and even assassination attempts. High-quality fraudulent travel documents will increasingly undermine the namespace, screening and vetting system, and threaten border security. We will see greater use of crypto currencies to fund operations. And the potential terrorist use of chemical and biological weapons has moved from a low-probability eventuality to something that is considered far more likely,” Travers said. “In many cases, terrorist exploitation of technologies outpaced the associated legal and policy framework needed to deal with that threat.”

The U.S. also faces a challenge in analyzing mass amounts of data to uncover threats, he added.

“Since 2009, when Umar Farouk Abdulmutallab tried to blow up Northwest Flight 253 over Detroit, we have seen an explosion of information: encrypted social media, publicly available information and captured electronic media from investigations in the battlefield,” Travers continued. “As the haystack has gotten bigger and the needles subtler, prioritization becomes extremely difficult. Determining which information is relevant and addressing the competing legal, privacy, policy, operational and technical equities remains a work in progress.”

He stressed that while “in a crowded national security environment, it is completely understandable that terrorism may no longer be viewed as the number one threat to the country,” the U.S. “will need to guard against complacency.”

Homeland Security Secretary Kirstjen Nielsen similarly warned about unmanned aerial systems as an example that “emerging threats are outpacing our defenses.”

“Terrorists and criminals are already using drones to surveil, smuggle, kill and destroy, and our country is in the crosshairs,” Nielsen testified.

“At DHS, we are also concerned about weapons of mass destruction. Terrorists and nation-states continue to pursue the development of chemical and biological weapons to conduct attacks,” she said.

Sen. Doug Jones (D-Ga.) asked Wray what the FBI is doing about domestic terrorism threats from neo-Nazis and other far-right extremists. “I don’t want that kind of threats to get overlooked because there are threats on mosques, there’s threats on Jewish community centers, bomb threats,” he said.

Wray said there are about a thousand active domestic terrorism investigations that “cover the waterfront of the full range of extremist ideologies from right to left, and everything in between.”

“We have assessed that that’s a steady, very serious threat. And I think we’ve had a hundred-some-odd arrests just of domestic terrorism subjects, you know, over the last year or so,” Wray said. “So it’s something we take very seriously. And every JTTF, every Joint Terrorism Task Force structure that you would be well familiar with from your past, is very active in the domestic terrorism space as well and something we take very seriously.”

Of the current array of terror threats, Travers said, “I do worry about taking our eye off the ball a little bit. There are much more really hard national security challenges we have to address, and they have supplanted terrorism to a degree, but we need to be careful.”

The NCTC director noted that “the private sector, the social media companies are much more willing to work with us than they were” even as there’s no agreed-upon definition of “terrorist content.”

“It’s going to be a large challenge for us going forward because as the terrorists get younger, they’re getting at this, and it poses massive issues for the intelligence community and law enforcement,” Travers said.

Nielsen said it’s important to realize “we don’t want to get to the point where a threshold has been crossed — we need to have a holistic approach to counter those narratives so that no one is radicalized.”

***Bridget Johnson** is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Previously she was an editorial board member at the Rocky Mountain News and syndicated nation/world news columnist at the Los Angeles Daily News. Bridget is a weekly columnist for the New York Observer and a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is a Senior Risk Analyst for Gate 15 and*

Washington Bureau Chief for PJ Media. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.

Bioweapons Threat at Large Venues Could Come from the Sky, Fear Security Experts

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/wmd/bioweapons-threat-at-large-venues-could-come-from-the-sky-fear-security-experts/

August 2018 – Drones that can disperse bioweapons are a top worry for operators of venues hosting large gatherings — especially as regulations hamstring drone mitigation efforts and even knocking a suspicious unmanned craft out of the sky could inadvertently unleash a toxic payload such as anthrax spores.

“Unfortunately, in today’s environment, mass gathering events attended by large numbers of people may be considered a terrorist target due to a large concentration of people, symbolic nature of the event, high-profile attendees and increased media attention,” Lou Marciani, director of the National Center for Spectator Sports Safety and Security at the University of Southern Mississippi, told the Blue-Ribbon Study Panel on Biodefense in Washington on Tuesday. “So, terrorists and other violent criminals are placing significant emphasis on attacking soft targets.”

Former Sen. Joe Lieberman (I-Conn.) and former Pennsylvania Gov. Tom Ridge, the first Homeland Security secretary, co-chair the panel, which includes former Secretary of Health and Human Services Donna Shalala, former Senator Majority Leader Tom Daschle (D-S.D.), former Rep. Jim Greenwood (R-Pa.), and former Homeland Security Advisor to President George W. Bush Kenneth Wainstein.

At a daylong panel on the impact of large-scale biological events on business and the economy, Marciani noted that vulnerable mass gatherings range from the Super Bowl to college playoffs, NBA and NHL to concerts, political conventions and more.

With the vulnerability of such events underscored by attacks like last year’s mass shooting at a Las Vegas music festival, Marciani outlined the challenge as ensuring public health, safety and security while public and private sectors interact in a complex way.

A security plan must “ensure intelligence regarding intent to use biological agents is combined with public health data,” he said, “improve domestic medical intelligence efforts,” "continue to advance national bio-surveillance," address lacking public health infrastructure, and "develop a national medical intelligence program."

"But a big concern to our profession is an aerial attack… presently, we lack the authorities needed to counter threats from unmanned aircraft systems. We need Congress' assistance in providing additional counter-UAS authorities to DHS and other federal departments and agencies to legally engage and mitigate UAS threats in the national airspace system," Marciani told the panel, emphasizing that mass gathering venues must "utilize collaborative planning processes to develop emergency operation plans for each venue, and the process should include high-level decision makers and ensure that planning, training, exercises, standards and lessons learned are connected."

On the government side, he said officials should add training courses on biological measures for first responders to build capacity and enhance training for biodefense.

Adequate biodefense at large venues, he said, "still has far to go." Marciani recommended establishing a sports and entertainment biodefense task force to report back to the Blue-Ribbon Study Panel.

Joe Coomer, vice president of security for AMB Sports and Entertainment, told the panel that "short of large-scale natural disasters, a biological event is one of the great unknowns for a lot of venues and our stadiums that we don't necessarily face on a daily basis — we don't test, we don't train."

"We have plans that review what to do, when to do it, but it's so broad in scale of what a biological event could be," he said.

The former director of security for Mercedes Benz Stadium in Atlanta,University of Phoenix Stadium in Glendale, Ariz., and the Indiana Convention Center and RCA Dome in Indianapolis added that he's confident from his experience planning with emergency managers that if an event occurs forensic investigation on the back end "will be pretty swift" in pinpointing the who, what, when, where, how and why.

"But when it comes to the immediate mitigation of a guest in the hot zone, we're now talking about a wild card that a lot of us can prep and plan for on paper, but until it's actually exercised, we don't know the implications of it," Coomer continued. "The mass event environment is highly dynamic and if we have a release through an explosion, is it through an aerosol, is it through a food contamination, what is the correct response? Again, plans on paper do work for us, except when these acts actually do happen it's how do we response strategically and surgically — are we talking about a handful of people, are we talking about tens of thousands of folks?"

Another challenge is how much staff would be around to help given the transient workforce on game days. "A lot of them do receive basic emergency evacuation training," but in a biocontamination situation he said there could be up to a 70 percent workforce reduction as "they will self-evacuate with everyone else because their commitment is at that level, that volunteer level or that hourly level."

After a biological event, Coomer noted, venues would face big challenges in winning back public confidence to convince fans to return and finding employees who would want to work in that venue again.

Daschle noted that a “nightmare I keep thinking about… is a drone with an aerosolable biological weapon.”

“UAVs and drones, that is our boogeyman right now,” Coomer acknowledged. “…Our country probably sells some of the best products out there to mitigate drones and UAVs, and we cannot deploy them.”

Even with technology to identify the owner of the drone and track him down, “at best it’s a written warning, so there’s no teeth to anything that we can do to these folks.”

“And it’s getting to the point a lot of sports industries are ready to take on what is, well, if knocking one of those things out of the sky is what we’ve got to do to find out what the courts are going to do to us, can we live with that if we know it’s going to save lives?” Coomer added.

Daschle stressed that checking drone licensing is “meaningless if it’s a terrorist.”

“Is there the equivalent of an anti-missile device or something that would be able to actually target a drone to knock it out?” the former senator asked.

Coomer cited technologies such as geofencing around property that would trigger a response if penetrated by an unfamiliar drone, and drone hunter-killers that are drones designed to capture the bad drone. “I know if seems very Hollywood, but we’ve seen these things demo’d at certain test sites,” he added. Other drones can fire netting to capture a drone and drag it off.

“In Europe, we’re seeing advancements using falcons and eagles knocking drones out of the sky,” he said, to which it was noted that a bad takedown of a bioweapon-laden drone could have disastrous fallout.

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Previously she was an editorial board member at the Rocky Mountain News and syndicated nation/world news columnist at the Los Angeles Daily News. Bridget is a weekly columnist for the New York Observer and a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is a Senior Risk Analyst for Gate 15 and Washington Bureau Chief for PJ Media. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.*

Authorities must do more to meet airport drone threat – Met police chief

Source: https://uk.reuters.com/article/uk-britain-drones-gatwick/authorities-must-do-more-to-meet-airport-drone-threat-met-police-chief-idUKKCN1OQ0OP

Dec 27 – Government and security officials must “up their game” to tackle the illegal use of drones at airports which brought chaos to London’s Gatwick airport in the run-up to Christmas, Britain’s most senior police officer said on Thursday.

Three days of drone sightings at Britain’s second busiest airport lead to about 1,000 flight cancellations and disrupted the travel of 140,000 passengers in what is thought to be the most disruptive incident of its kind.

ALWAYS THE SAME SAD EXCUSE!

London’s Metropolitan Police Commissioner Cressida Dick said no police force around the world could be sure of preventing the problem posed by drones at airports.

“I think the whole country and certainly the government will have watched what’s gone on and said we need to up our game here,” Dick told BBC radio.

“You won’t find a police service in the world I think who would be sitting complacently thinking: ‘well we could always deal with a drone’.”

The drones were first spotted at Gatwick on Dec. 19. Every time the airport sought to reopen the runway, the drones returned and authorities only regained control over the airfield after the army deployed military technology to guard the area.

Security Minister Ben Wallace said on Monday that Britain's security forces now had detection systems that could be deployed across the country to combat the drone threat.

"The drone technology is always changing. We have to keep up with that. There are a whole variety of tactics and technologies that we are now using, can use and in the future, they will have to change again I'm sure," said Dick.

"I've been talking to colleagues around the world. I can tell you this is not an easy problem. We are doing our very best here and going into the future I'm sure working closely with others we will get better and better."

The police investigation into the Gatwick incident is ongoing. Detectives on Sunday released without charge two people they had suspected of flying the drones.

Flying drones within 1 km (0.6 mile) of a British airport boundary is punishable by up to five years in prison.

"We need to work even more closely with the private companies, we need to work even more closely with the military, we need to try to be able to prevent the criminal use of drones for whatever motivation near our airports," Dick said.

EDITOR'S COMMENT: I always have this recepie in my mind when dealing with security planning: Think as a terrorist when designing your defenses; think as a victim when designing your responses! How come we always play by the book (flying drones within 1 km of British airports is punishable by up to five years in prison) the moment the intruder/terrorist/criminal/insurgent/enemy follows a different book? Make the penalty 50 years, arrest one or two of drone users, put them in jail and put strict rules in UAVs production and specifications. Yes, all these oppose the principles of democracy and free enterprise but do you think it would be a good excuse to be said to the relatives of the 300 people killed because a UAV was sucked by an airplane's tourbines during take off or landing? If yes, please go ahead and do nothing! The whole story resembles the penalties punishing human smugglers/trafficers in part responsible for the human tsunami currently flooding the EU. A few years in prison against thousands not to say millions of euros or dollars in the pocket of criminals and their associates and the odds to be arrested. Life is for those who dare – remember? In agony to hear the "more" written in the title of this article.

Is the US Prepared for Drone Attack?

Source: https://i-hls.com/archives/87749

Dec 26 – The temporary shutdown of UK Gatwick Airport due to drones flying over the airfield has raised worldwide concern. In the US, forbes.com claims that the country is not prepared for such attacks not only from the security technology perspective but also from the legal aspect.

The U.S. has not yet developed the legal strategy and training to enable law enforcement and prosecutors to respond to these types of events and appropriately prosecute the perpetrators.

Current counter-drone techniques have major drawbacks. There are two types: **detectors and defenders.** Detectors do just that, detect drones using different methods (radar, radio waves, etc.). Defenders disrupt or destroy the unmanned aircraft using all sorts of creative technology: shotgun shells; jammers that disrupt the radio frequency signals between the drone and the pilot; GPS signal spoofers, which allow taking over control of the drone; lasers; and even trained eagles.

The consequences are that In using a jammer to take down a drone, it would also disrupt the use of that radio frequency spectrum in a wide area for a host of important functions, interfering with Wi-Fi and cellular communication signals and airport navigation aids, and potentially resetting equipment for power companies.

In addition, not all drones are radio-controlled and jammable — there are systems that can be programmed to fly a defined route.

Use of projectiles or lasers to take a drone down raises risks of harming bystanders and damaging nearby property.

While some of the counter-drone techniques have been used effectively by the military in war zones and by intelligence agencies, such as jamming and GPS spoofing, they have been made illegal for unauthorized use by law enforcement in the U.S. due to the collateral damage that they could cause.

In the United States, there are anti-jamming laws and anti-GPS-spoofing laws. It is illegal to damage or destroy an aircraft or hack into a drone. Civilians or authorities who used these counter-drone techniques would open themselves to extra lawsuit liability from plaintiff attorneys whose clients might have been hurt because of the illegal operation.

So, can anyone do anything to stop these drones? Multiple federal laws have been passed within the last two years to give the authority to use counter-drone measures to the Department of Homeland Security, Department of Justice, U.S. Coast Guard, Department of Energy and Department of Defense. But even with these new laws, there will still be a need to determine safe and effective rules of engagement against misused drones. DHS and DOJ will be working on this quickly in light of the events at Gatwick.

EDITOR'S COMMENT: We have to redefine certain things related to technological progress. Drones proved useful tools for the military (reconnaissance; armed attacks against enemy positions, surveillance) and there are certain equally useful uses in the civilian sector (provide a real time operational picture [accidents; disasters]; surveillance; detection [CBR included]; S&R operations; rapid delivery of defibrillation equipment to name a few. But what is the point for a company to deliver parcels with an UAV; or pizzas; or carry people from A to B? What is the point to allow citizens to fly cameras over our heads for their fun or for making their own videos or for their own reasoning? Since legislation proved inefficient to control the problem it might be better to control the product. Our world would keep on turning even without UAVs!

The Drone to Beat All Drones

Source (video): https://i-hls.com/archives/87842

Dec 31 – Russia's Mikran has recently announced its production of a new counter-drone drone robot. The device is built to hunt small immediate airborne pray. The Russian firm has stated that its mission, among others, is to devour the competition.

"This drone has a very colorful name: 'Carnivora.' It was obviously selected due to its mission — attack and incapacitate other drones and UAVs, to 'cannibalize' them," Samuel Bendett, a research analyst at the Center for Naval Analyses, told c4isrnet.com. "According to the developers, the drone can use nets to intercept targets; can carry several types of high-explosive ammunition, as well as reconnaissance equipment. Currently, according to Mikran, the prototype is undergoing factory flight tests."

To carry those payloads, Carnivora has a rather large body in comparison to other medium drones. It weighs in at a maximum weight of around 40 kilos, with 35 liters of space for payload inside.

The fixed-wing drone has an almost 5-meter wingspan, and a top speed of 150 kmh and is designed to stay airborne for between 10-15 hours. The Carnivora is billed as made for the future threat environment, where electronic warfare renders remote control difficult.

However, Carnivora is hardly the only drone designed for combat in denied environments. Kalashnikov also recently announced an Arctic drone designed to operate without satellite navigation.

"More importantly, the UAV is able to work "in the conditions of radio-electronic suppression with the complete loss of satellite navigation signals." This is key — Russians are actively training their forces and designing military tech to operate in an environment where the loss of GPS and other traditional navigation systems would be imminent," says Bendett. "This is one of the ways Russian forces are preparing to counter what they perceive is a technologically superior adversary that will take aim at the Russian navigation, satellite and other technology."

The electromagnetically denied environment is the future threat guiding the mission of the Carnivora. But its design is likely also shaped by the experience of Russian forces in Syria, where they encountered small commercial off-the-shelf drones used in simple and sophisticated attacks on Russian military bases and installations.

"C-UAV efforts are receiving lots of attention across the Russian armed forces — taking down small adversary drones is now getting built into the Russian military's most important targets," says Bendett. "This drone that can hunt and destroy other small drones fits into that."

The Future of Swarm Robotics

Source: https://i-hls.com/archives/88001

Jan 03 – Swarm robotics have an expanding variety of uses, ranging from industrial to military and defense purposes. Back in 2015, the University of Lincoln unveiled a pheromone system called Communication System via Pheromone. Inspired by insects, the system emits an artificial trail like a light. Once a robot picks up the trail, it would follow it, creating a swarm with others.

The U.K. is the leader in European swarm robotics, for the main reason that its military has identified swarm robotics as a priority, according to roboticsbusinessreview.com. Shortly after the U.K. introduced a fund valued at almost $1 billion to develop and acquire "next-generation defence technologies," including "dragonfly drones," its Ministry of Defense unveiled a competition to develop technology around unmanned air system (UAS) swarms.

A team of researchers in **Rome** and the Netherlands is working on the Swarm Robotics for Agricultural Applications (SAGA) project which is intended to develop vision processing, radio communication systems, and protocols for multiple unmanned aerial vehicles.

This past summer, researchers in **Belgium** published a paper on "Autonomous Task Sequencing in a Robot Swarm." It showed how wheeled robots could work together in a "chain gang."

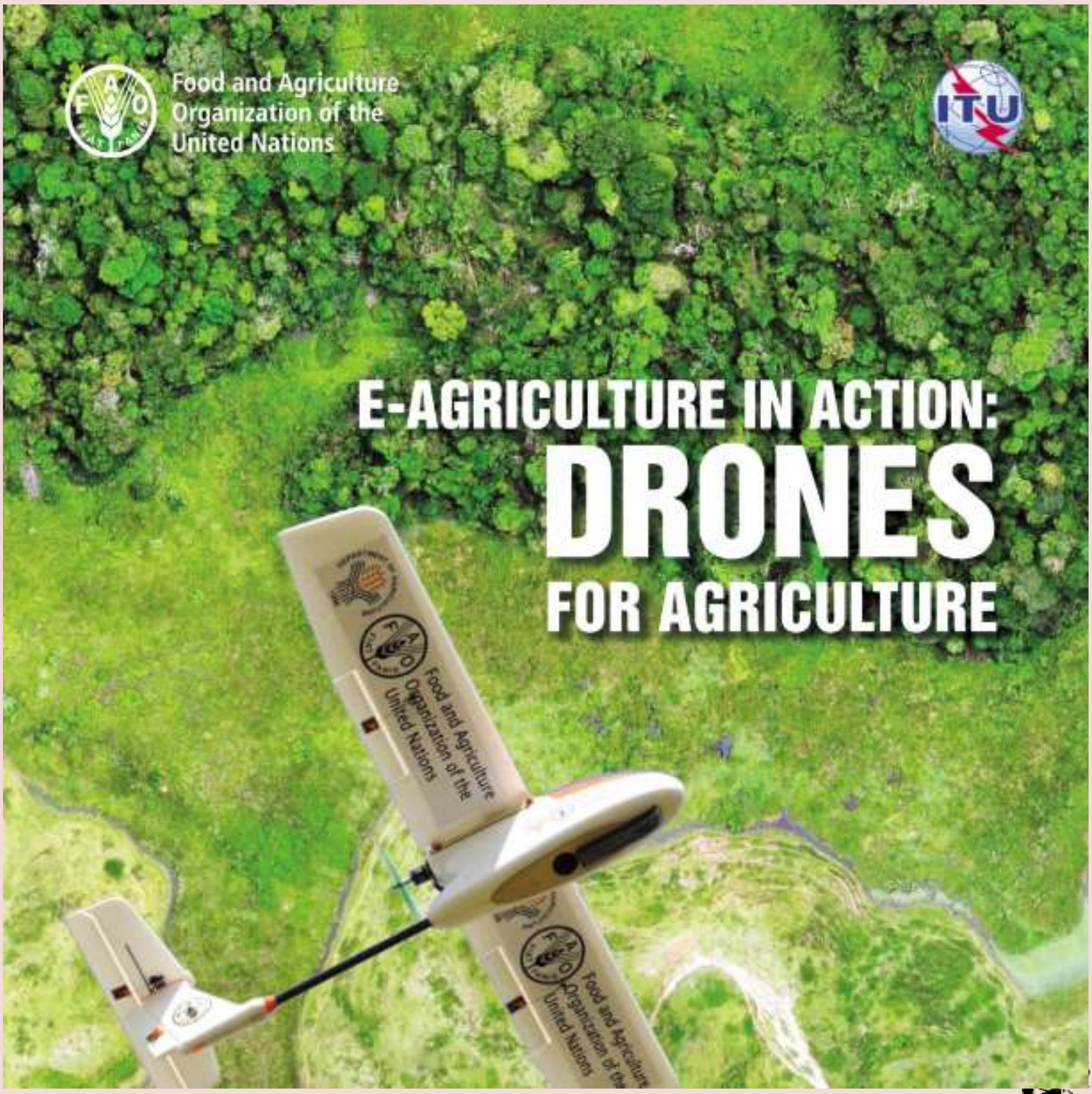
In the **Netherlands**, the DelFly drone from the Delft University of Technology could help with disaster recovery, monitoring inventory in warehouses, and even replace endangered bees for pollination. A team in Austria is also working on drones to help honeybees, while the possibility of tiny surveillance drones has raised privacy concerns.

Two universities in Lisbon, **Portugal**, jointly developed 3D-printed "aquatic surface robots" that work in a swarm. These robots, which are envisioned to be deployed in the hundreds or thousands can be used for search and rescue, maritime surveillance and more. They operate autonomously by being connected to an "artificial brain".

In addition, the **CPSwarm** (Cyber Physical Swarm) European project includes drones, vehicles, and other cyber-physical systems as part of smart cities research.

Of course, the U.S. and China have their own drone swarm projects in the air and in the water, many of which are for entertainment or military purposes. Russia has claimed that a January attack on a base in Syria was conducted by a U.S.-commanded aerial drone swarm. This is leading to work on swarm countermeasures, as well as debates about the ethics around swarm use.

The global "swarm intelligence" market was worth $10.5 million last year and will experience a compound annual growth rate of 37.49% between then and 2028, mostly driven by defense, according to Research and Markets. European swarm robotics has received significant support because EU policymakers have prioritized it as an important robotics field to invest in.



Source: http://www.fao.org/3/I8494EN/i8494en.pdf

Media Reports of Terrorist Attempts to Employ UAVs

Source: https://www.armscontrol.ru/UAV/clips.htm

- In 1995, Aum Shinrikyo, the Japanese terrorist group that attacked the Tokyo subway with sarin gas, planned to use remote-control helicopters to spray dangerous chemicals from the air.[1] The helicopters crashed during testing.
- In 2001 Osama bin Laden considered using remote-control airplanes packed with explosives to kill President George W. Bush and other heads of state at the G-8 summit in Genoa, Italy.[2]
- In June 2002, quoting a German intelligence official, the *Reuters* news agency reported that al Qaeda might be planning to attack passenger aircraft using model airplanes.[3]
- One terrorist group, the Revolutionary Armed Forces of Colombia, or FARC, were discovered in possession of nine remote-controlled unmanned aircraft when a Colombian army unit overran one their remote camps in August 2002.[4] However, such radio-controlled craft can only be effectively flown for a few miles.[5]

- According to *Debka.com*, in December 2002, Palestinian toy importers in Jerusalem and Ramallah were told to order hundreds of model airplanes for distribution to Palestinian children in hospitals. Subsidies from European Union member-governments could legitimately be allocated to this humanitarian purpose. The model airplanes were purchased in Europe and shipped openly to Palestinian shopkeepers. The model planes were sent to Palestinian workshops for conversion into miniature air bombers with explosive payloads. Tanzim militiamen from Arafat's Fatah, sent out to open areas near Jericho to test the new weapons, discovered they could fly to a distance of 1 kilometer and an altitude of 300 meters. The only problem was how to guide the plane to a target inside a built-up Israeli area where it would no longer be visible to the remote control holder. A small adjustment was made in the engine enabling the operator to cut it out from a distance, so that it dropped to the ground and blew up. Contrary to reports that Arafat had withdrawn from the day-to-day management of Palestinian terrorist operations, *DEBKAfile's* counter-terror sources emphasize that the results of the model plane conversion tests were brought before him. Delighted with its performance, he ordered the new weapon to be used in the coming days in Jerusalem. He chose Jerusalem, calculating that it would be some time before Israeli security and intelligence authorities caught on to and learned how to intercept the new miniweapon whizzing around the city before it blew up. The deadly toy is easily launched from Arab Jerusalem. Its flying time is estimated at no more than 2-3 minutes.[6]
- *The Vremya Novostei* newspaper reported in November 2003 the theft of a copy of the newest developmental reconnaissance UAV model from a building plant in Israel. The UAV weighs 14 kg and has a wingspan of 1.5 m.[7] The thief was not caught, and there were fears about the possible use of the model by terrorists.
- According to the London *Independent* newspaper, a British national held at Camp Delta, Guantanamo Bay, Cuba, has confessed to being part of an al Qaeda plot to acquire a drone to attack the House of Commons with anthrax.[8]
- According to *Reuters*, in early March 2004, Israeli intelligence prevented a terrorist act with use of a UAV loaded with explosives. Representatives of the administration of Prime Minister Ariel Sharon claimed that a Palestinian extremist group planned to attack a Jewish settlement in Gaza sector.[9]
- According to Hamas, six of their senior activists were killed in March 2004 when a UAV they had planned to launch against Israel blew up prematurely in central Gaza as they were preparing it for flight. Possibly, the March 2004 incident involved axplosive-packed drone.[10]
- On November 7, 2004 at 10:30 Lebanese guerrilla group Hezbollah flew an unmanned spy plane "Mirsad 1" over northern Israel. The plane, launched from southern Lebanon, flew along Israel's northern Mediterranean coast until it reached the coastal resort of Nahariyah, turned back and landed at sea off the coast of Lebanon. "Mirsad 1" can carry explosives of about 40 and 50 kilograms," Hezbollah chief Shaikh Hassan Nasr Allah told few days after the incident. "It does not have the capacity of only reaching Nahariya (in northern Israel), but

deeper and deeper, against electricity and water installations and military bases," he added.[11]

[1] Michael Gips, "A Remote Threat," *Security Management Online*, October 2002.
[2] Michael Gips, 2000.
[3] Michael Gips, 2000.
[4] "Colombia - FARC Drones Discovered," *EFE News Service*, August 28, 2002.
[5] Dennis M. Gormley, "UAVs and Cruise Missiles as Possible Terrorist Weapons," In "New Challenges in Missile Proliferation, Missile Defences, and Space Security," Ed. by James Clay Moltz, Occasional Paper N 12, Center for Nonproliferation Studies, Mauntbatten Centre for International Studies, July 2003.
[6] "Arafat's New Terror Weapon: Exploding Toy Planes," DEBKAfile Special Counter-Terror Report, January 14, 2003, 4:33 PM (GMT+02:00).
[7] "Israeli Reconnaissance Plane Has Been Stolen," *Vremya Novostey*, November 11, 2003.
[8] Testimony of Dennis M. Gormley, Senior Fellow, Monterey Institute's Center for Nonproliferation Studies, before the Subcommittee on National Security, Emerging Threats, and International Affairs of the U.S. House of Representatives Committee on Government Reform, March 9, 2004.
[9] "Terrorist Act with UAV Employment Has Been Prevented in Israel," - *in Russian*, *Polit.Ru*, March 10, 2004.
[10] Ed Blanche, IDF uses armed UAVs against Gaza militants, *Jane's Missiles and Rockets*, December 1, 2004.
[11] Eugene Miasnikov, Terrorists Develop UAVs (A Comment on 'Mirsad 1' Flight Over Israel, December 6, 2004.

Why airports can't stop drones from causing chaos

Source: https://www.cnbc.com/2019/01/08/why-airports-cant-stop-drone-disruptions.html

Jan 09 – London's Heathrow airport had to suspend flights on Tuesday after drone sightings there, following similar disruptive incidents at Gatwick in December that affected 1,000 flights.

© picture-alliance/AP Photo/J. Stillwell

The move to suspend flights is understandable. Airports and the airlines that pay them don't want to see a drone sucked into a jetliner's engine, or a drone that's rigged as an explosive device wreaking havoc.

But it seems absurd that a couple of $500 drones and some rogue pilots can disrupt millions of dollars of business by causing flight delays and negative experiences for travelers.

With so much at stake — in terms of safety and profits — why aren't airports better prepared to deal with drones?

It's not for lack of technology, said Lance Sherry, director of the Center for Air Transportation Systems Research at George Mason University.

"Counter drone" systems are already on the market, though they are not perfect and are constantly evolving, he said. They employ high-resolution radar and other sensors to detect drones. Some use lasers, ballistics, nets and signal jammers to intercept and take drones down as needed.

Examples of counter-drone companies range from newer start-ups like Dedrone in San Francisco, to larger defense firms like the $2 billion Israeli company Rafael and Rome-based Leonardo.

The CEO of Dedrone, Joerg Lamprecht, said all players in the air travel industry are still grappling with the question of authority.

"Airports have a lot of red tape," he said. "This is a new issue. Who is in charge, who controls the airspace, who is the one that should be providing drone detection? Who has the authority to manage this and to intervene – is it federal police, local police, someone who owns the airspace?"

Interdictions are allowed at military bases in the United States and some fixed sites that are owned by federal agencies. But authority hasn't been determined at every commercial airport.

Brian Wynne, president and CEO of the Association for Unmanned Vehicle Systems International, wants to see the drone industry and aviation authorities around the world agree to "remote identification," something like digital license plates, for drones. With remote identification, he believes, airports could easily identify a drone's owner and contact them to land the drone if it's flying where it shouldn't.

No matter how the laws shape up and counter-drone technology evolves, Sherry said the disruptions at Heathrow and Gatwick should serve as a wake-up call.

"If you look at the industry as a whole, the way it works the airports, airlines, air traffic controllers, aircraft makers, and fuel companies all have to cooperate to provide air service. Everyone's objectives are different. And it is sort of a 'tombstone' industry, where it takes an accident to get funding to flow and people working on a problem. Until just now? There has been nothing dramatic enough to make them work on this. We should all be thankful that these incidents were not more severe, there were no injuries or fatalities."

The drone sightings at Heathrow and Gatwick prompted quick regulatory changes. Law enforcement in the U.K. is now permitted to land, seize and search drones, and to fine operators who fail to comply with orders to land their small drones, or fine those who fly without properly registering their drones as well. Wynne said he's hoping for similar advances on the regulatory front in the U.S. soon.

New Safety Standard for Flying Drones Over Crowds

Source: https://i-hls.com/archives/88211

Jan 11 – Flying drones over crowds of people can be dangerous, and from now on the Federal Aviation Administration (FAA) will require a permission to do so. The permission entails the installation of a parachute system for drones that fly over crowds.

The first case where the system was required was for CNN's Snap Drone produced by Vantage Robotics. Back in 2017 Indemnis and DJI worked together to develop a parachute system that would be approved by the FAA.

Indemnis and DJI announced that the **Indemnis Nexus parachute system for the DJI Inspire 2 drone** has been validated as compliant with the new international standard for drone parachutes.

This breakthrough in reliable parachute technology for small drones opens a wide range of new possibilities for professional drone operators intending to demonstrate that they can safely and reliably fly over people as well as sensitive locations.

Indemnis, based in Anchorage, Alaska, joined DJI in a safety partnership in 2017 to develop industry parachute standards as well as a parachute system that can deploy instantly if a drone encounters flight

anomalies, reducing the potential energy of any impact on the ground.

The U.S. Federal Aviation Administration (FAA) prohibits most drone operations directly over people as a safety precaution. Professional drone operators can apply for a waiver from that restriction if they can demonstrate they have robust safety mitigations in place. The Indemnis system is intended to be the core of a parachute-based safety mitigation plan for a waiver, and can also help provide one path forward for advanced operations as the FAA considers how to allow routine flights directly over people.

“Indemnis has tested our parachute systems in thousands of real-world unplanned failure scenarios, and NUAIR’s validation of our work is an exciting step toward making professional drone operations over people safe, routine and productive,” said Amber McDonald, Indemnis President/ CEO.

Nexus is a ballistic parachute launcher, triggered automatically if the drone suddenly begins tilting abnormally or falling. It deploys the parachute within 30 milliseconds at 90 mph, through a tube that rapidly inflates to keep the parachute lines away from the drone body and propellers. Indemnis offers the Nexus package today for the Inspire 2, and intends to offer it for Matrice 200 series and Matrice 600 series drones by late 2019.

NUAIR Alliance, which manages one of the FAA-designated test sites for drone technologies at Griffiss International Airport in Rome, New York, put the Indemnis Nexus through 45 functionality tests across five different failure scenarios last month during four days of testing. Those tests validated that the Nexus on the Inspire 2 complies with the ASTM International F3322-18 Standard Specification for Small Unmanned Aircraft System (sUAS) Parachutes. DJI, Indemnis, the FAA and other industry stakeholders collaborated on developing the ASTM consensus standard, which was finalized late last year after more than a year of work.

Drone jamming system to protect European airports, public spaces

Source: http://www.homelandsecuritynewswire.com/dr20190115-drone-jamming-system-to-protect-european-airports-public-spaces

Jan 15 – The company has developed a drone alarm and protection system that is being installed at a number of prominent sites around Europe, including an airport. It has the potential to prevent the kind of costly disruption that hit London’s Gatwick and Heathrow airports recently.

Horizon**’s Richard Gray interviewed Hermansen.**

Richard Gray: Why are drones posing a growing problem in our skies?

Dan Hermansen: If you go back maybe five years, that is when the first incidents started to appear. At the time, there wasn’t really anybody taking care of the airspace below normal flying level. So, if you were flying below 200 or 300 metres, no one really cared as no other aircraft were at that level unless you were close to an airport.

Over the last five years we have seen regulations come into force in different countries to make sure that drones are not flying close to areas like airports, prisons, military facilities or other critical infrastructure. But more and more people are using the technology. They are given drones as toys for Christmas, so naturally they will go out and fly them.

Gray: Is it deliberate or because people don’t know any better?

Hermansen: In some cases, it is just ignorance. People who are not aware of the rules and regulations. I think if you look at some of the recent cases at Gatwick and Heathrow (airports), this could be what has happened there. (People) want to go out and try their new toy and don't realise they need to be at least one kilometre from an airport. Then someone reports a drone flying close to the airfield and it causes the kind of shutdowns we have seen recently.

But then there are also those people who don't care about the regulations. This is a more worrying issue from our perspective.

Gray: How are drones being used in these cases?

Hermansen: There are some who are using them for criminal acts. For example, drones are being used to smuggle drugs, telephones or other stuff into prisons. That is a very specific use case where the pilot is deliberately breaking the rules.

There is another category where we categorise it as terrorism or harassment, which is what we have been looking at over the past few years. The military, for example, is concerned about direct attacks. There are soldiers who are being attacked by commercial drones that have been retrofitted with grenades or other explosives.

At the height of the conflicts in Iraq and Afghanistan, there were a lot of roadside bombs that used improvised explosive devices or IED. Now that IED is actually flying. It's not dug into the dirt at the side of the road but is strapped onto a simple drone and flown into a vehicle or crowd of people.

With an airport, however, you don't even need to strap a bomb onto the drone. You just need to fly it into the area. The pilot can be hidden away inside a tall building so no-one can see them.

Gray: What can the impact be on airports?

Hermansen: There have been multiple airports now that have been closed down due to drone sightings. There were reports in Dubai, Copenhagen and Heathrow in London in the past. On these occasions the airports were closed for half an hour to an hour to ensure the drone had gone, but during the recent incident at Gatwick, it was more than a day where no planes could take off. There were around 900 flights cancelled and 120,000 passengers affected. Imagine how costly that is.

Gray: Why are airports not better protected?

Hermansen: Very few airports have any countermeasures or even processes in place to detect and defeat drones. They have been left miserably behind as the technology has enabled people to get hold of these things.

Gray: Do there need to be more regulations?

Hermansen: I'm not sure it will really help to regulate any more. Most countries now have regulations in place and to fly a drone in an urban area, for example, you need a licence. The problem is that there are people who do not adhere to the regulations.

Gray: Is this where anti-drone technology can help?

Hermansen: Yes. We have been developing a drone alarm and protection system called KNOX. It uses radio frequency sensors to monitor the wireless spectrum looking for the control signals or video transmissions used by drones. (Algorithms) can give an indication of what direction the signal is coming from and how strong it is, giving an indication about how far away it is.

We also get information about what type of signal it is, so we know what sort of threat we might be facing – how big the drone is and what sort of payload it can carry.

What's smart about the radio frequency sensors is that they don't have to be in line of sight of the drone. As soon as the drone controller is turned on, the sensors will pick it up. So, we can get a pre-warning about a drone before it is even airborne.

Gray: What sort of range does it work over?

Hermansen: It has a range of a few kilometres, so it is only picking up things in the immediate vicinity, which is what you want if you are trying to protect a building or a facility. We also use a scanning radar that is specifically tuned to look for drones. It can see anything that is the right size and moves like a drone in its line of sight. We have developed a tracking algorithm that can distinguish drones from other similar sized things like a bird. It looks for unique features of a drone, like propellers.

Gray: Once you identify a drone, what then happens?

Hermansen: We localise the radio frequency signals to and from the drone in time and direction, and produce a jamming signal. This is noise that causes the drone to lose connection with the pilot. When this happens, most commercial drones will fly back to the pilot's location automatically.

We can also jam the drone's positioning system (GPS) and when this happens the drone will perform a controlled landing using its on board sensors and gyros. Some of the cheaper drones might not have these, in which case they will crash land.

Gray: Can you also catch the pilot?

Hermansen: If you have multiple sensors placed some distance apart you can triangulate where the signal is coming from and locate the pilot, which is something the authorities might want to do.

Gray: Is your system already being used?

Hermansen: We are working on trials at five different locations around Europe and in Israel. Getting the permission to test the jamming part of the technology in Europe has been difficult but we have a police force that is trialling our system at their headquarters now. We are also testing it at two prisons, one sports stadium and an airport in Denmark. We are hoping to finalise all the demonstrations and testing in the next six months.

Gray: How do you see anti-drone technology being used in the future?

Hermansen: I think it's inevitable that drones will become part of our daily lives and will be used a lot more. There are companies looking to use them for deliveries or other commercial activities. Anti-drone technologies will make (this transition) safer.

We are working on other projects with partners in the US to online traffic management system for drones. It is really paving the way for what many see as the second wave of drone technology that will carry people in autonomous flying taxis.

Drone regulation in the EU

In 2016, the European Commission proposed the establishment of an automated traffic management system for drones operating at low-level, referred to as "U-space."

Up until 2018, EU Member States were solely responsible for smaller drones (weighing less than 150 kilograms). However, legislation was adopted on 26 June 2018 to introduce EU-wide regulations for drones.

The European Aviation Safety Authority has proposed a number of EU-wide rules for the use of civil drones, such as keeping your drone in sight at all times, not flying more than 150 metres from the ground and keeping away from airports and helipads.

The European Commission has committed EUR €44 million to integrate drones safely into the airspace and to the SESAR R&D programme under its U-space initiative.

This interview is published courtesy of Horizon, the EU research and innovation magazine

Drones 'endangered aircraft' 18 times in three months

Source: https://www.bbc.com/news/uk-46919876

Jan 18 – **There were 18 near misses between aircraft and drones across Britain between July and October 2018,** according to an air safety body.

Out of the reported incidents, 12 took place in Greater London.

The UK Airprox Board (UKAB) said the "highest risk of collision" occurred when a large "commercial drone" was seen to pass within 20 metres of an Airbus A380 as it approached Heathrow.

Drone sightings disrupted about 1,000 flights at Gatwick Airport in December.

Departures at Heathrow Airport were also halted temporarily after drone activity was reported earlier this month.

Heathrow has since deployed an anti-UAV defence system, which can detect, track and ground problem drones.

Aviation minister Baroness Sugg said: "The actions of these drone users were not only irresponsible, but illegal.

"The law could not be clearer that this is a criminal offence and anyone endangering others in this way faces imprisonment."

Image copyright PA Image caption Counter-drone equipment was used at Gatwick during December

Outside of London, other incidents reported by the UKAB - which monitors near misses involving aircraft - occurred in Manchester, Cambridgeshire, Birmingham, Cardiff, Glasgow and the East Midlands.

The UKAB reported that **one of the category A incidents took place as an Embraer 190 aircraft was landing at Glasgow Airport. It concluded a "definite risk of collision" had existed, after a "shiny white drone" was flown directly above an airliner, just 15-30 metres away.**

A total of 120 near misses between drones and aircraft were reported in the year between 4 December 2017 and 4 December 2018.

Q&A: A look at what happens when drones get near airports

Source: https://www.apnews.com/ce41205647824258b226442dd5c7e97f

The ability of drones to interfere with airliners — and inconvenience their passengers — has now been demonstrated on two continents, and the problem is likely to get worse as the number of small, unmanned devices multiply.

Law enforcement authorities are trying to figure out who flew a drone so high and so close to Newark Liberty International Airport that incoming flights were held up briefly during a peak hour at one of the nation's busiest airports.

Flights resumed within about 30 minutes — much more quickly than after a similar incident last month at London's Gatwick Airport.

Here are some common questions readers have about these incidents and brief answers.

WHAT HAPPENED IN NEW JERSEY?

The pilots of both a Southwest Airlines flight and a United Airlines flight reported seeing a drone around 3,500 feet (1,000 meters) above Teterboro, New Jersey, about 9 miles (15 kilometers) from the Newark airport, on Tuesday.

As a precaution, the Federal Aviation Administration held up 43 flights already in the air and bound for Newark; nine landed instead at other airports. Another 170 Newark-bound planes were briefly delayed on the ground before taking off from other airports around the country.

No video of the reported drone has surfaced.

WHO WAS OPERATING THE DRONE?

Authorities have not determined that. The FAA alerted New Jersey State Police and the FBI.

CAN WE BE SURE THERE WAS A DRONE?

Some drone operators are skeptical about a drone reported at 3,500 feet and whether pilots in a fast-moving jet could accurately identify such a tiny object.

Vic Moss, a founder of Drone U, a drone-operator school based in Albuquerque, New Mexico, said many consumer drones are restricted from going that high, although home-built devices or older drones are not. There are, however, videos online showing drones at such altitudes.

"It's possible, but it's just incredibly unlikely that it was an actual drone," Moss said. "Drones are the new UFO."

WHAT HAPPENED IN LONDON?

In mid-December, hundreds of flights were canceled and more than 100,000 people were stranded or delayed over two days after reports of drones spotted near the runway at Gatwick Airport, a major international hub.

A few days later, police arrested two men living near the airport but later cleared them, and no other suspects have been identified. Police also said that two drones found near the airport were not involved in the disruption.

A few weeks later, a reported drone sighting briefly halted flights departing from London's Heathrow Airport, one of the world's busiest.

WHY IS THIS HAPPENING?

If the intrusions in New Jersey and London were deliberate, the motives are not clear. Officials in London said there was no indication that the Gatwick incident was terror-related. A criminal investigation has been opened into the Heathrow incident.

WHAT ARE THE LAWS ABOUT FLYING DRONES NEAR AIRPORTS?

Federal rules forbid operating a drone within 5 miles (8 kilometers) of most airports or above 400 feet (120 meters) without a waiver from the FAA.

ARE DRONE MANUFACTURERS RESPONSIBLE?

Devices from the biggest maker of consumer drones, DJI, include so-called geofencing — technology designed to prevent the aircraft from taking off near an airport. A drone that is launched properly but enters a no-fly zone will hover at the edge of the zone, according to a DJI spokesman.

Owners say DJI can take days to unlock no-fly restrictions around even small airports. But DJI says those requests now are automated and handled quickly.

However, many drones offered for sale don't include such restrictions: They have no GPS or geofencing.

CAN OPERATORS DISABLE SAFETY SYSTEMS?

Yes. There are online discussions in which drone operators talk about hacks, but they involve some level of technological sophistication.

"The geofences (from manufacturers like DJI) are in place, but in some cases they can be defeated — it's not easy," said Tom Kilpatrick, a drone pilot who founded a drone company in Oklahoma. "They are designed to prevent the average drone operator from flying near an airport."

Home-built drones would likely not have those same safety features.

WHAT'S BEING DONE TO PREVENT DRONES FROM INTERFERING?

DJI says it has developed technology to track nearby drones — their flight path and the operator's location — using mobile, ground-based units.

The technology is currently only used to identify other DJI drones.

WHAT ARE AIRPORTS DOING?

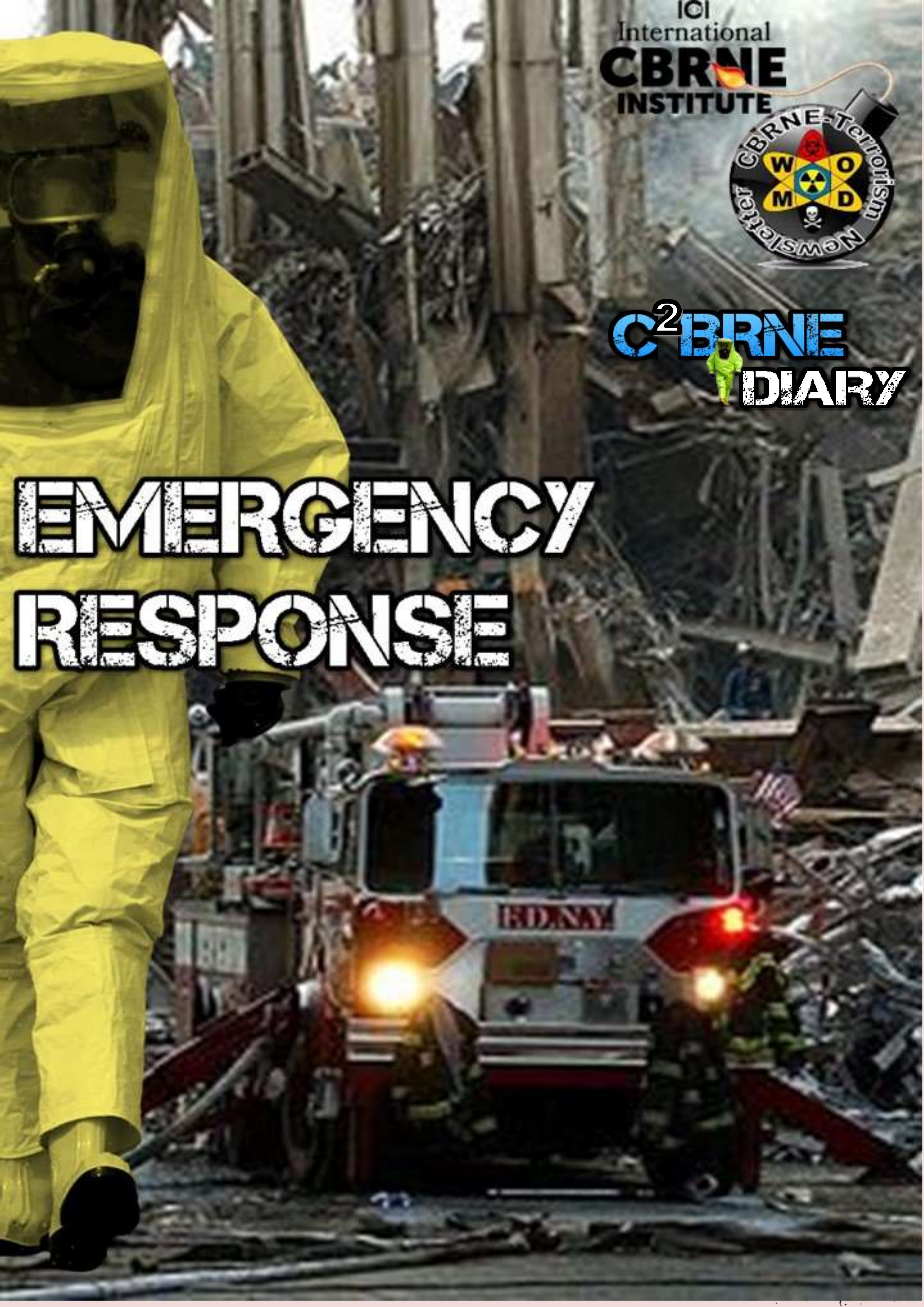
The Port Authority of New York and New Jersey, which operates the Newark airport, said in a statement that agency officials met last week with counterparts from the FAA, FBI and Homeland Security Department "to review and enhance protocols for the rapid detection and interdiction of drones.” A spokesman would not provide specifics and declined to say whether the airport has any anti-drone technology.

After the Gatwick incident, British officials said they have deployed drone-defense equipment at other U.K. airports, although they gave few details.

ARE TOUGHER RULES IN THE WORKS?

Late last year, Congress gave the Homeland Security and Justice departments authority to develop and deploy a system to identify drones and disable — even destroy — drones that authorities consider a threat.

FAA spokesman Greg Martin said any such system has to be designed carefully so that it doesn’t interfere with navigation equipment used by planes.

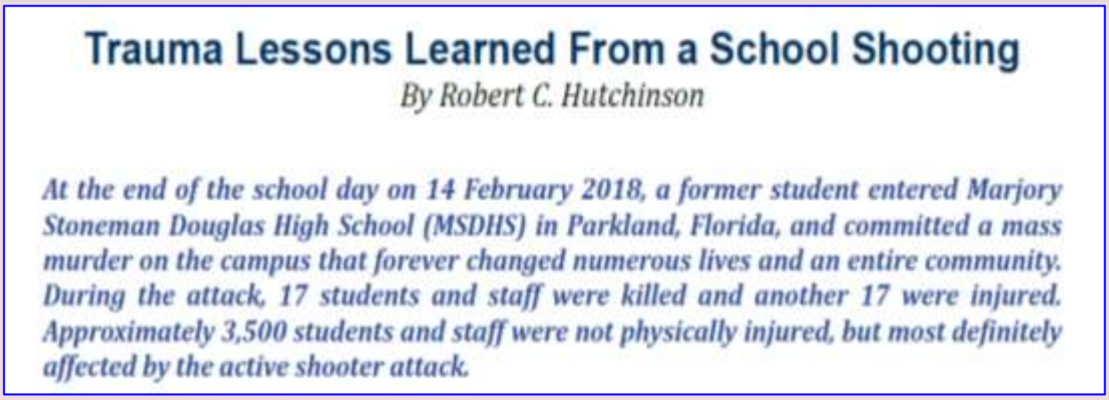


International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

EMERGENCY RESPONSE



Trauma Lessons Learned From a School Shooting

By Robert C. Hutchinson

At the end of the school day on 14 February 2018, a former student entered Marjory Stoneman Douglas High School (MSDHS) in Parkland, Florida, and committed a mass murder on the campus that forever changed numerous lives and an entire community. During the attack, 17 students and staff were killed and another 17 were injured. Approximately 3,500 students and staff were not physically injured, but most definitely affected by the active shooter attack.

DomPrep Journal. Volume 14, Issue 12, December 2018
Source: https://www.domesticpreparedness.com/journals/december-2018/

Robert C. Hutchinson *has been the chief of police for the Broward County Public Schools, Special Investigative Unit since 2016. He was the former deputy special agent in charge and acting special agent in charge with U.S. Department of Homeland Security (DHS), Homeland Security Investigations in Miami, Florida. He retired in 2016 after more than 28 years as a special agent with DHS and the legacy U.S. Customs Service. He was previously the deputy director and acting director for the agency's national emergency preparedness division and assistant director for its national firearms and tactical training division. His writings, interviews and presentations often address the important need for cooperation, coordination and collaboration between the fields of public health, emergency management and law enforcement. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.*

Parkland Shooter Used Emergency Drill to His Advantage

By Aden Magee

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/lesson-parkland-shooter-using-emergency-drill-his-advantage/

February 2018 – Initial reports regarding this month's mass shooting at Marjory Stoneman Douglas High School in Parkland, Fla., cited an ominous potential dynamic that gave counterterrorism experts cause to contemplate whether we were seeing yet another evolution in sophistication of the lone active-shooter. **The fact that the school conducted a fire drill earlier in the day and the shooter later activated the fire alarm at the initiation of his attack reminded us of an important anti-terrorism lesson** – one that is no less relevant because it may not have been the exact methodology employed by the Parkland shooter. Although it appears that the assailant was not as calculating as the initial reports may have suggested, there are practical lessons and implications that must be proactively addressed to effectively prepare for future attacks.

The Parkland shooter initiated his attack by triggering the school fire alarm system, which initially compelled hundreds of unsuspecting students to expose themselves as more vulnerable by running toward the exits, and the shooter. Whether the shooter understood the specific vulnerabilities presented by the Parkland emergency evacuation procedures or, more likely, based this plan on a general knowledge of how the students would respond,[i] the event demonstrated the often-overlooked challenge that emergency safety and security procedures present. In fact, the irony that security professionals must appreciate is that the very procedures enacted to protect facilities and its occupants during an emergency situation can actually be exploited by a determined and calculating threat actor to render the facility and its occupants even more vulnerable.

A basic understanding of the terrorist attack planning process and how other like-minded threat actors can be expected to approach their objectives provides ample perspective regarding this complicated security challenge.

Sophisticated terrorist organizations execute a relatively consistent attack preparation process that is based largely on the collection of information to maximize

the probability of mission success. Terrorist operatives observe potential targets during the planning phase of an operation to determine strengths, weaknesses, and vulnerabilities. During the final stages of preparation, terrorist operatives observe and collect information to finalize attack planning with a detailed focus on specific vulnerabilities that can be effectively exploited to enable the attack. Key to these final preparation efforts are detailed evaluations of security procedures, which may include "tests" and "probes" of security.

As a target surveillance technique, terrorists conduct tests of security at potential target locations to gather data on specific security procedures. Such activities include approaching security control points or moving into sensitive areas to observe security or law enforcement responses. **Specific areas of interest to terrorists include how long it takes security or law enforcement to respond to an incident, the number of responding personnel, and the routes taken to a specific location.** Probing efforts to test security usually involve a plausible reason for observing the practices and effectiveness of security at a specific point, but they could also include more blatant efforts to penetrate physical security barriers or test the response procedures to assess strengths and weaknesses.

A **common method** employed by threat actors to test security measures is to prompt a potential target location/facility to initiate security response procedures — commonly by delivering anonymous threats (e.g. telephonic, email threats) — to observe the reaction procedures of security forces and occupying personnel. **A basic example of a test of security is the "suspicious package" threat.** This scenario involves a readily observable item (i.e. box, briefcase, suitcase) that is left unattended in a suspicious location. In many cases in responding to these situations, security professionals (to include explosive ordinance disposal) conduct the meticulous and deliberate process of neutralizing the potential threat only to find that it was inert/innocuous all along. Too often, the relief and satisfaction of performing a safe and successful neutralization may lead to a tendency to disregard the fact that no one returned during the hours of drama to claim the item, nor was there a feasible explanation for why the item was left unattended in the first place.

Emergency safety and security procedures are planned and executed to minimize the loss of life and resources during a specific emergency situation. As with the example of the response to the "suspicious package," this dynamic can lead to a single-minded focus that results in "blind spots," which the calculating adversary can readily exploit. Augmenting these "blind spots" is a tendency to attribute the triggering actions as "prank" calls, emails, or other guises. This perspective represents a minimalist approach into which security professionals cannot allow themselves to fall.

Although the "suspicious package" example is not most relevant to an active-shooter situation, it does demonstrate how taking the seemingly appropriate actions in regard to emergency response can actually be leveraged against the practitioners in the future. The "suspicious package" example reflects the common tendency to narrowly assess emergency reaction exercises purely from the standpoint of how well they followed the plan and how successful they were in accomplishing the immediate objective. In this example, however, the event enables a threat actor to determine how long it takes for the item to be reported to police or security forces, how long it takes these forces to respond, and the specific procedures employed in responding to and addressing the situation. Given this pervasive threat potential, these events should be evaluated from a "worst-case scenario" perspective, with the assumption that the emergency situation was orchestrated as an opportunity for a threat actor to observe and identify vulnerabilities. Only then can the plan benefit from the standpoint of what a calculating adversary observed, how that adversary will take advantage of this intelligence, and how the plan must be adjusted to prevent the adversary from gaining advantage from this knowledge in the future.

Schools and other similar potential active shooter/terrorist targets employ emergency response procedures that are very effective in practice, but simply do not stand up when executed in the face of a knowledgeable, determined, and calculating threat actor. From the mind of an active shooter or terrorist intent on maximizing casualties, areas of interest in observing security/safety response procedures will include chokepoints where large volumes of occupants exit the facility, and other "target rich" locations such as where individuals congregate after evacuating a threatened facility. Post-exercise facility re-entry procedures are another vulnerability of potential threat interest due to a tendency to rush occupants back to work.

There will be many lessons learned from the Parkland school shooting, but one that should not be lost in the clutter of the more obvious debates is a lesson that cannot be relearned too many times. **As a standard practice, security managers should ensure that emergency reaction drills/exercises are evaluated from the standpoint of the vulnerabilities that an adversary conducting pre-attack surveillance and planning would observe if present.** Even if it is a pre-planned (and even unannounced) emergency exercise such as a fire or bomb threat drill, security managers should assume that potential attackers are observing the measures to identify vulnerabilities for exploitation during a future attack. Particularly when an event is not preplanned and is stimulated from an external source, security managers must be increasingly vigilant in observing the event from the eyes of a calculating and determined adversary. The tendency to write such events off as pranks or system errors is a classic example of underestimating the threat. To the other appropriate extreme, sophisticated security planners will incorporate surveillance detection methodologies during the execution of emergency response procedures as an active threat countermeasure based on an exacting understanding of the terrorist/threat target attack planning process and hostile surveillance techniques.

By evaluating emergency response procedures and exercises from the standpoint of the adversary, security professionals will identify the same vulnerabilities the enemy would. This perspective enables the proactive implementation of threat mitigation procedures to anticipate and prevent the enemy's actions at specific points of vulnerability. This **"red team" approach** enables security professionals to evaluate their emergency response procedures through the eyes of the enemy. As a result, for example, informed emergency response plans will proactively deploy armed security personnel to locations such as chokepoints and assembly areas where known vulnerabilities in the previous plan existed.

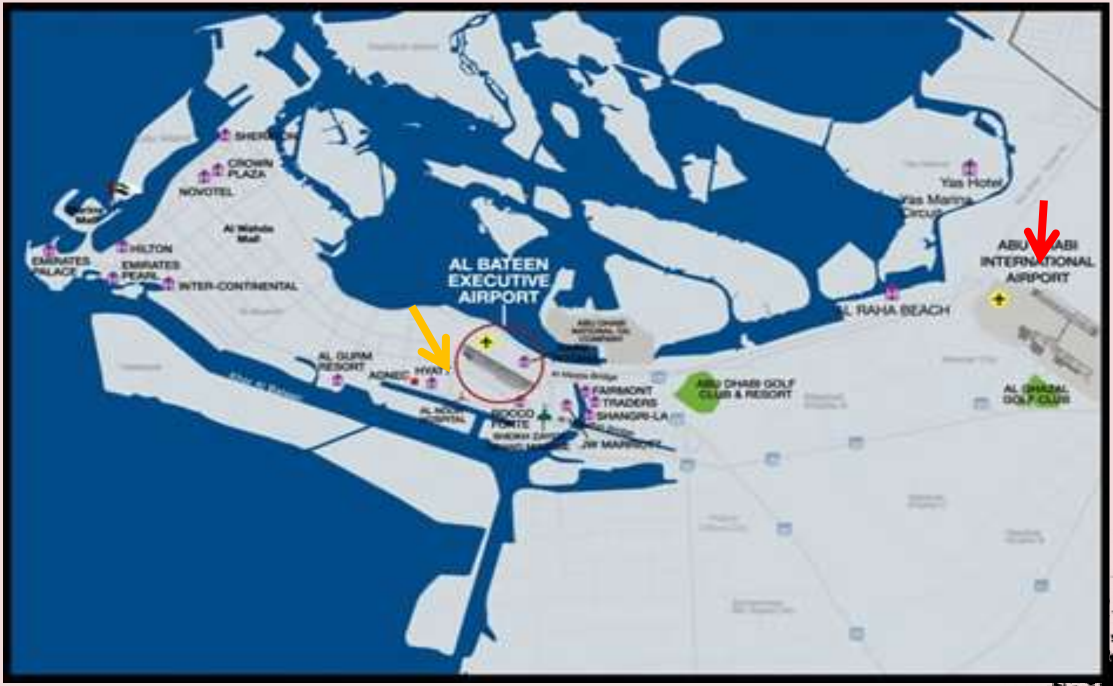
[i] Parkland was the fifth school shooting in the U.S in which a fire alarm was triggered.

***Aden Magee** is a retired U.S. Army Military Intelligence officer specializing in terrorist and unconventional warfare threats as a senior consultant/advisor to the Department of Defense, Department of Homeland Security, and the Federal Bureau of Investigation.*

Emergency drill to be held at Abu Dhabi airport

Source: https://www.thenational.ae/uae/emergency-drill-to-be-held-at-abu-dhabi-airport-1.806338

Dec 26 – A full scale emergency exercise will be held at Al Bateen Executive Airport in Abu Dhabi on Wednesday.



The exercise will begin at 4pm and end at 6pm though it is not expected to disrupt any flights, Abu Dhabi Airports said in a statement.

"The emergency drill will measure the preparedness of all relevant emergency response agencies and evaluate the emergency response capabilities and implementation strategies of Al Bateen Airport," the statement read.

Abu Dhabi Airports said the exercise will carried out in accordance with regulations issued by the General Civil Aviation Authority, as well as standards and recommendations stipulated by the International Civil Aviation Organisation.

Al Bateen airport opened in the late 1960's and was Abu Dhabi's first main airport until the current airport opened in 1982. Al Bateen now exclusively handles private flights.

EDITOR'S COMMENT: Two hours for a preparedness drill? What is this? A joke? This is the ideal airport for any type of drills (conventional and asymmetric). I am sure that the short duration mentioned is a printing mistake…

AMERICA'S EMERGENCY RESPONSE SYSTEM:
FIRST RESPONDERS:
EMS
FIRE DEPT.
POLICE
SECOND RESPONDERS:
WHY CAN'T THE RESCUE SQUAD HELP THOSE PEOPLE?
SOME-ONE SAID THEY CAN'T GET THRU THE CROWD.
THAT'S AWFUL!
THIRD RESPONDERS:
TED, HOW DID IT FEEL WHEN TV 7 BEAT YOU TO THE DISASTER SCENE?
OF COURSE WE WERE DEVASTATED, SUE.
FOURTH RESPONDERS:
HONK! HONK! HONK!
HONK!
HONK!
I'M AN ATTORNEY! TAKE MY CARD!
NO--TAKE MINE!
www.BRADVELEY.COM
VELEY

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

ASYMMETRIC THREATS

New policy design required to tackle global environmental threat: Report

Source: http://www.homelandsecuritynewswire.com/dr20190111-new-policy-design-required-to-tackle-global-environmental-threat-report

Jan 11 – A pioneering new report has devised a seven-point plan to help policymakers devise new, coherent and collaborative strategies to tackle the greatest global environmental threats.
A team of international researchers, including experts from the Land, Environment, Economics and Policy (LEEP) Institute at the University of Exeter, has examined how politicians and legislators can develop a new way to tackle the growing threat of climate change.
The perspective piece, which is published as the cover article in *Nature Sustainability*, comes in response to advice from leading scientists, suggesting that the human impact on the environment are already tipping the world into a new geologically significant era.
Called the Anthropocene, this new era is defined by the effect human-kind has already caused on Earth, from mass extinctions of plant and animal species, polluted oceans and altered atmosphere.
Exeter says that in the new report, the scientists argue that while policies are available, there also needs to be a new way to tackle the geographical, boundary, spatial, ecological and socio-political complexities of the issue; and that will require working together across disciplines.
Professor Ian Bateman of LEEP and co-author of the paper said: "The paper shows that the integrated nature of the planetary boundary problems requires an integrated policy response.
"Traditional policies tend to be highly piecemeal, highly inefficient, prone to failure and can even be counterproductive. Such policies take vital resources from key areas while providing short term sticking-plaster efforts for high visibility, often politically motivated causes."
Recent research into the Anthropocene has suggested that there are multiple threats to the resilience of the Earth systems.
While the report acknowledges that there are no 'simple solutions', it does outline seven guiding principles to help tackle the growing environmental threat brought by man-made climate change.
These include selecting existing, robust policies to help formulate policy decisions, the need for decisions to be made consistently across regional, national and global boundaries, and a more conclusive look at the true extent that the environment is being impacted.
The report is authored by Professor Bateman, Dr. Donna Carless and Amanda Robinson from Exeter, alongside some of the world's leading researchers in the field.
Together the team undertook the first unified assessment of the policy options for tackling the challenges of the Anthropocene. These include the integrated global problems of climate change; the pollution of air, land, freshwater and sea; and the rapid loss of genetic diversity around the world.

— Read more in "Driving spaceship Earth," Nature Sustainability 2, no. 1 (2019).

Defense Department Warns About Climate Change Impacts to Armed Forces and Bases

Source: http://time.com/5507465/climate-change-impact-armed-forces-bases/

Jan 18 – **The U.S. Defense Department has issued a dire report on how climate change could affect the nation's armed forces and security, warning that rising seas could inundate coastal bases and drought-fueled wildfires could endanger those that are inland.**
The 22-page assessment delivered to Congress on Thursday says about two-thirds of 79 mission-essential military installations in the U.S. that were reviewed are vulnerable now or in the future to flooding and more than half are at risk from drought. About half also are at risk from wildfires, including the threat of mudslides and erosion from rains after the blazes.

“The effects of a changing climate are a national security issue with potential impacts to DOD missions, operational plans and installations,” Defense Department spokeswoman Heather Babb said Friday in an email.

The report contradicts the view of President Donald Trump, who has rejected the scientific consensus that climate change is real and man-made. The report’s premise echoes the findings of the National Climate Assessment, written by 13 federal agencies and released in November. It concluded that the effects of global warming are accelerating and will cause widespread disruption.

Trump rejected those findings. “I don’t believe it,” he said at the time.

The new Defense Department report, which was mandated by Congress, describes widespread impacts, dispersed across the U.S., with more coastal flooding along the East coast and Hawaii.

U.S. military facilities are already encountering some of the effects, the Pentagon says, noting that Joint Base Langley-Eustis in Virginia has experienced 14 inches of sea-level rise since 1930. And Navy Base Coronado in California already is subject to flooding during tropical storms.

In the Washington area, several Defense Department sites — including Joint Base Andrews, home of Air Force One — are experiencing drought conditions that have been severe in the past 16 years, the report says. Those conditions can lead to ruptured utility lines and cracked roads, the Pentagon warns, as moisture disappears from soil.

The Defense Department stresses in its report that it is working with nations around the world “to understand and plan for future potential mission impacts” from climate change, describing it as “a global issue.”

But Democratic lawmakers said the Defense Department pulled its punches by listing what Senator Jack Reed, the top Democrat on the Senate Armed Services Committee, called a “phone book” of threats without offering a plan of action.

“It fails to even minimally discuss a mitigation plan to address the vulnerabilities,” House Armed Services Committee Chairman Adam Smith said in a statement. Committee member Jim Langevin said the Defense Department “for no apparent reason” omitted the threat to U.S. bases abroad.

Pentagon History

The Pentagon has long expressed concern over climate change and its military implications worldwide.

Defense Secretary Jim Mattis, who resigned last month, had been at odds with Trump over climate change, telling Senate Armed Services during his confirmation process that “the Department of Defense must pay attention to potential adverse impacts generated by this phenomenon.”

“Climate change is impacting stability in areas of the world where our troops are operating today,” Mattis wrote in written responses to questions from the committee. “It is appropriate for the Combatant Commands to incorporate drivers of instability that impact the security environment in their areas into their planning.”

In 2013, Republican Senator Jim Inhofe of Oklahoma, who now is chairman of the Senate panel, pressed Admiral Samuel Locklear, who was head of U.S. Pacific Command, to say that his concerns about climate change were being misrepresented by “environmental extremists.”

Obama Administration

Instead, Locklear said about 280,000 people died in natural disasters in the Pacific region from 2008 to 2012. “Now, they weren’t all climate-change or weather-related, but a lot of them were,” the admiral said.

Under the Obama administration, responding to the effects of climate on the nation’s military was a top initiative, but the Trump administration has taken a different tack. Climate change was omitted in 2017 as a threat from the National Security Strategy, a list of the top dangers facing the nation.

“Given future global energy demand, much of the developing world will require fossil fuels, as well as other forms of energy, to power their economies and lift their people out of poverty,” the 2017 strategy said. “U.S. leadership is indispensable to countering an anti-growth energy agenda.”

Shortly after taking office, Trump revoked a memorandum that Obama signed in 2016, directing the Defense Department to account for climate change in its decisions about where to build new facilities and how it prepares for future threats.

Senator Dick Durbin, the ranking Democrat on the Defense Appropriations Subcommittee, responded by calling Trump's decision to rescind the memorandum "a security disaster."