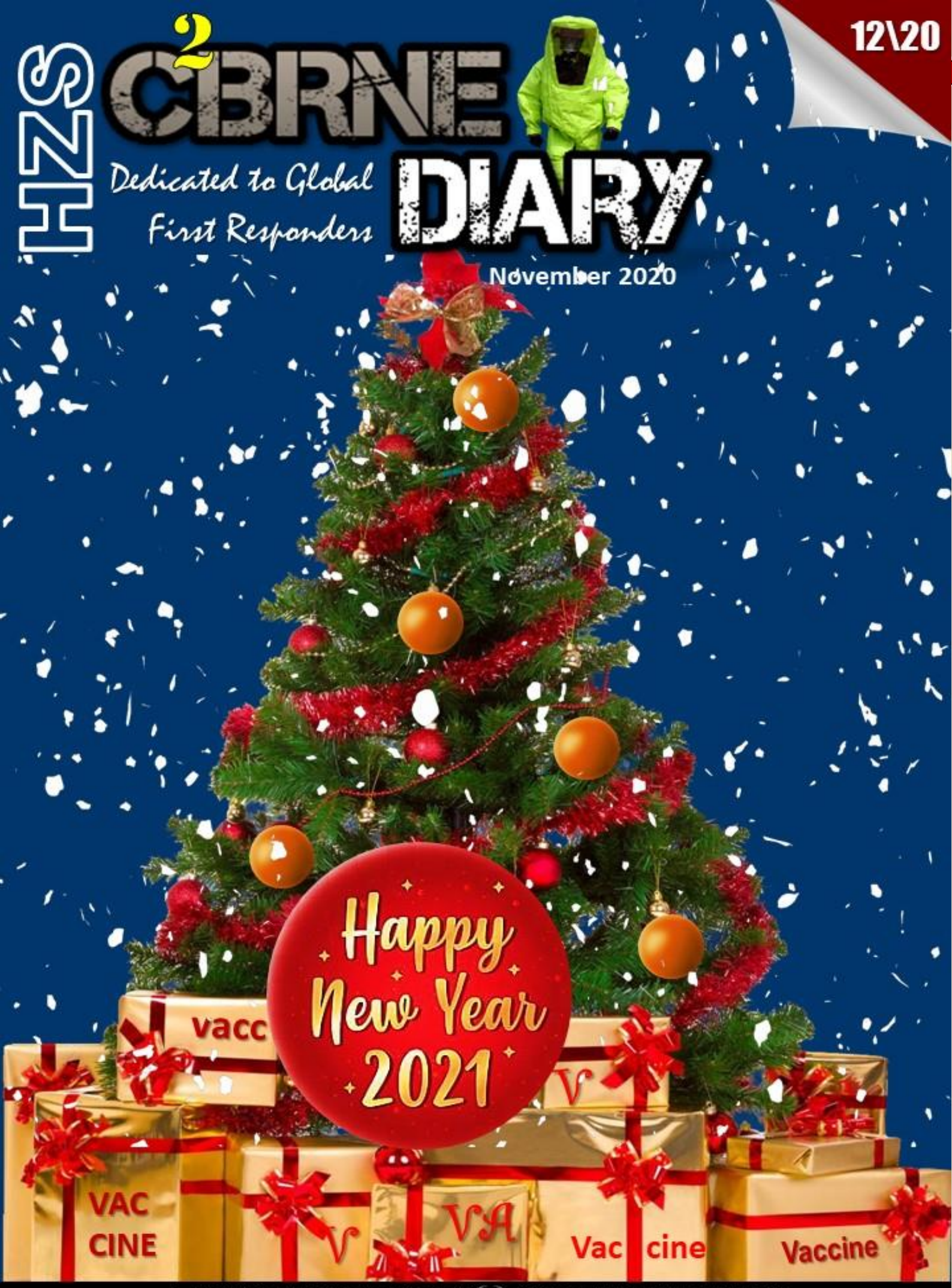
12\20

HZS

CBRNE DIARY

Dedicated to Global First Responders

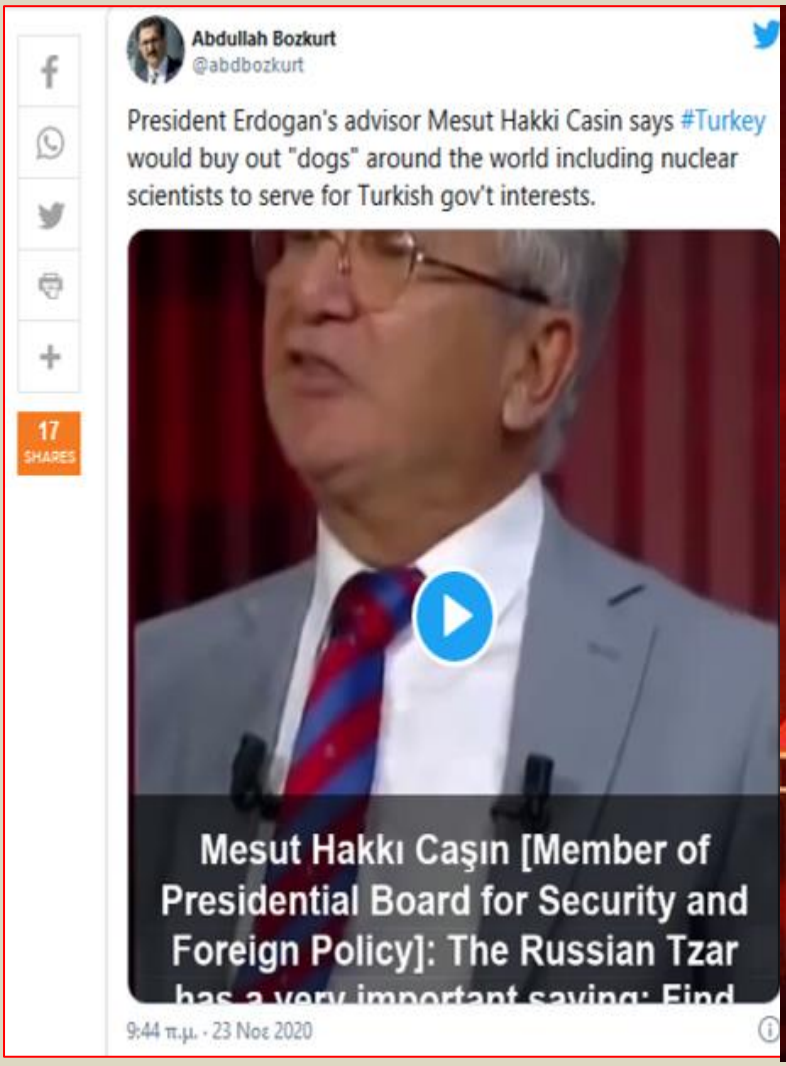
November 2020



A HOTZONE SOLUTIONS GROUP PUBLICATION


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
HOTZONE
SOLUTIONS
GROUP
C2BRNE
DIARY
DIRTY R-NEWS

Turks always do what they announce …



Medical Management of Radiation Emergencies: REAC/TS Launches New RadMed App

Source: https://cbrnecentral.com/medical-management-of-radiation-emergencies-reac-ts-launches-new-radmed-app/25465/

Oct 14 – The Oak Ridge Institute for Science and Education (ORISE) Radiation Emergency Assistance Center/Training Site (REAC/TS) has launched a new RadMed app, providing a wide range of resources on the medical management of radiation incidents that can be downloaded free on mobile devices and utilized while on the go.

The REAC/TS RadMed App includes:

- Updated eGuide for The Medical Aspects of Radiation Incidents, 5th edition
- Basic health physics and dose estimation (US and SI Units)
- Treatment of whole body and acute local radiological illnesses and injuries
- Assessment and treatment of internal contamination with radioactive materials
- Patient decontamination
- Delayed effects of exposure to ionizing radiation
- Risk and psychological issues
- Dicentric chromosome assay (DCA)
- State, federal and international resource database

- Assessment tools for radiation incident preparedness
- REAC/TS courses
- REAC/TS videos
- Real-Time REAC/TS news
- Links to partner resources

"The REAC/TS RadMed app offers healthcare professionals, emergency responders and planners, public health professionals and health physicists' easy access to essential medical information and resources when dealing with a radiation incident," said REAC/TS Director Carol Iddins. "We created the RadMed app with our target audiences in mind to provide easy access to the resources they need."

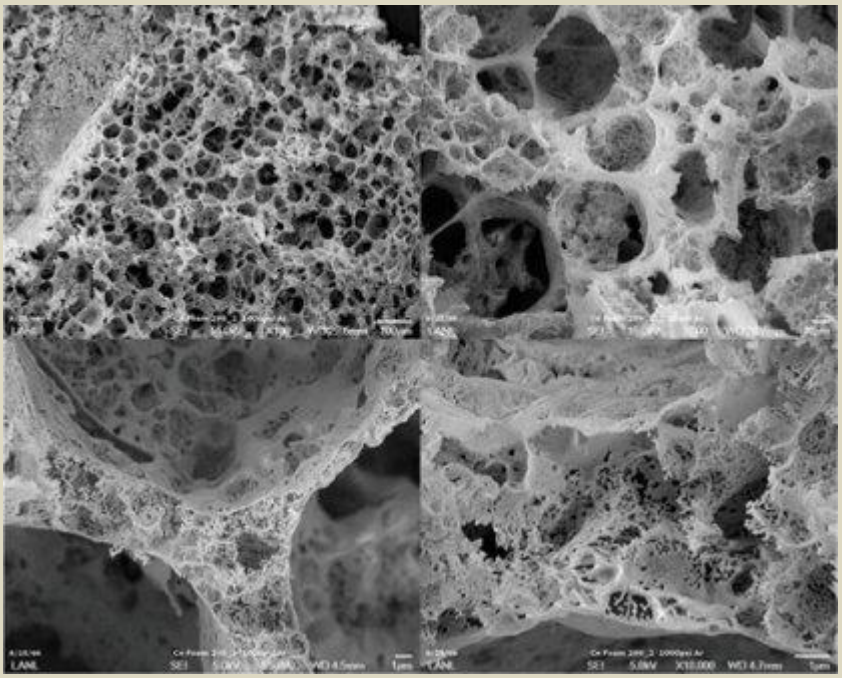
Visit the RadMed page to learn more about the RadMed app, and download it for free by searching for REAC/TS RadMed in the Apple and Android app stores.

Novel Chemical Process a First Step to Making Nuclear Fuel with Fire

Source: http://www.homelandsecuritynewswire.com/dr20201127-novel-chemical-process-a-first-step-to-making-nuclear-fuel-with-fire

Nov 27 – Developing safe and sustainable fuels for nuclear energy is an integral part of Los Alamos National Laboratory's energy security mission. Uranium dioxide, a radioactive actinide oxide, is the most widely used nuclear fuel in today's nuclear power plants. A new "combustion synthesis" process recently established for lanthanide metals—non-radioactive and positioned one row above actinides on the periodic table—could be a guide for the production of safe, sustainable nuclear fuels.

"Actinide nitride fuels are potentially a safer and more economical option in current power-generating systems," said Bi Nguyen, Los Alamos National Laboratory Agnew postdoc and lead author of research recently published in the journal *Inorganic Chemistry*, which was selected as an American Chemical Society Editors' Choice Featured Article.



"Nitride fuels are also well suited to future Generation IV nuclear power systems, which focus on safety, and feature a sustainable closed reactor fuel cycle. Actinide nitrides have superior thermal conductivity compared to the oxides and are significantly more energy dense," said Nguyen. Nitrides are a class of chemical compounds that contain nitrogen, versus oxides, which contain oxygen.

Scanning electron microscope images of cerium nitride foam

Actinide nitride fuels would provide more safety and sustainability because of their energy density, offering up more energy from less material, as well as better thermal conductivity—allowing for lower temperature operations, giving them a larger margin to meltdown under abnormal conditions.

Actinide nitrides, however, are very challenging to make and the production of large amounts of high purity actinide nitrides continues to be a major impediment to their application. Both actinides and lanthanides are at the bottom of the periodic table and potential methods to make actinide materials are typically first tested with the lanthanides because they behave similarly, but are not radioactive.

Los Alamos National Laboratory and Naval Research Laboratory scientists discovered that LnBTA [lanthanide bis(tetrazolato)amine] compounds can be burned to produce high-purity lanthanide nitride foams in a unique technique called combustion synthesis. This method uses a laser pulse to initiate dehydrated LnBTA complexes, which then undergo a self-sustained combustion reaction in an inert atmosphere to yield nanostructured lanthanide nitride foams. This work was funded by the Laboratory Directed Research and Development (LDRD) program.

LnBTA compounds are easily prepared in bulk and their combustion is readily scalable. There is an ongoing collaboration between the Laboratory's Weapons Modernization and Chemistry divisions to examine actinide analogues for combustion synthesis of actinide nitride fuels.
The research team includes Nguyen, David Chavez, Bryce Tappan, and Alexander Mueller of the Explosives Science and Shock Physics group, Jacqueline Veauthier and Jaqueline Kiplinger of the Inorganic Isotope and Actinide group, Brian Scott of Materials Synthesis and Integrated Devices group, and Damon Parrish of the Naval Research Laboratory.

Prominent Iranian physicist assassinated near Tehran

Source: https://www.globalsecurity.org/wmd/library/news/iran/2020/iran-201127-presstv04.htm

Nov 27 – Prominent Iranian physicist Mohsen Fakhrizadeh has been assassinated in a terrorist attack near the capital Tehran.
The Fars news agency reported that he had been targeted on Friday in a multi-pronged attack involving at least one explosion and small fire by a number of assailants in Absard city of Damavand County, Tehran Province.

The attack targeted the vehicle carrying Fakhrizadeh â€" who headed the Iranian Defense Ministry's Organization of Defensive Innovation and Research (SPND), the agency said.
The Defense Ministry's media office said Fakhrizadeh "was severely wounded in the course of clashes between his security team and terrorists, and was transferred to hospital," where he succumbed to his injuries.
Fars said 3-4 people were killed in the shooting, all of whom were said to be terrorists.
Photos and footage shared online of the attack showed bullet holes on the windshield of Fakhrizadeh's car and a pool of blood on the road.

'Serious indications of Israeli role'

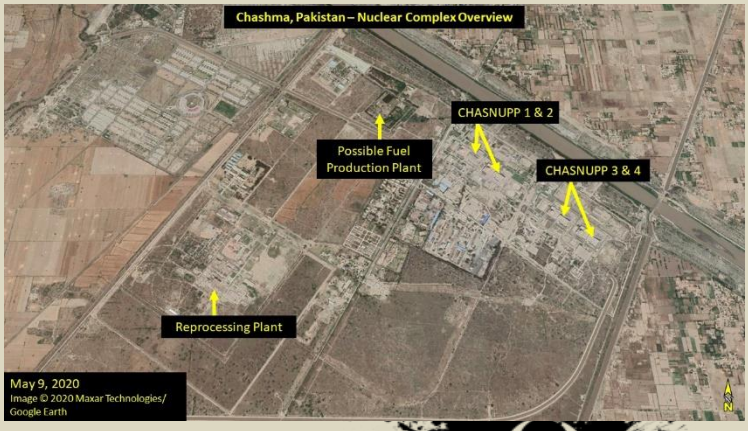
In a statement, Iranian Foreign Ministry Mohammad Javad Zarif roundly condemned the terror attack, saying there were "serious indications" of the Israeli regime's role in the assassination of Fakhrizadeh, a professor of physics at Imam Hussein University of Tehran.
"Terrorists murdered an eminent Iranian scientist today. This cowardice "with serious indications of Israeli role" shows desperate warmongering of perpetrators," he said in a tweet.
The top Iranian diplomat called on the international community, especially the European Union, to "end their shameful double standards & condemn this act of state terror."

▶▶ **Read also:** Assassination of Iranian Scientist Brings US-Israel Closer to War with Iran

New Extension to the Chashma Plutonium Separation Facility

By Neil Hyatt and Sarah Burkhard

Download PDF

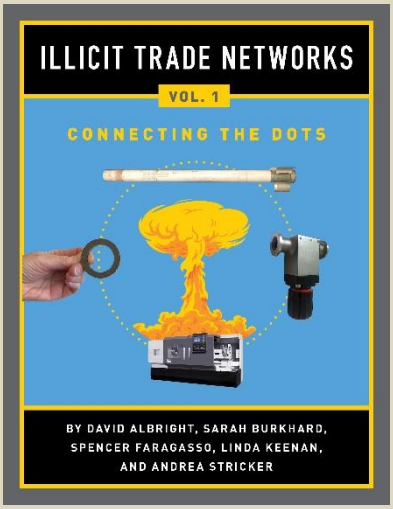


Nov 30 – *Satellite imagery available on Google Earth show that an interesting and previously undocumented expansion of the nuclear fuel reprocessing / plutonium separation facility at the Chashma nuclear complex in Pakistan began in mid-2018. The extension's exterior appears completed as of September 2020. The reprocessing plant was first*

identified by ISIS in 2007 and considered to be potentially operational in 2015. The development of this extension and allied facilities at the Chashma reprocessing plant are analysed herein.

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

***Neil Hyatt** is Professor of Nuclear Materials Chemistry at the University of Sheffield.*



Illicit Trade Networks - Connecting the Dots, Volume 1

Press Release – New Institute Book

By David Albright, Sarah Burkhard, Spencer Faragasso, Linda Keenan, and Andrea Stricker

February 2020

Illicit procurement of strategic commodities is an ongoing threat perpetuated by states that operate outside of global nonproliferation norms and agreements. Such countries rely heavily on outside supply to obtain the commodities needed to build or augment covert or sanctioned nuclear, missile, and conventional military programs.

▶▶ The full book is now available at no cost as a pdf file: View PDF

Cobalt 60 Sources in Mosul: Recovery and Lessons for the Future

Source: https://isis-online.org/isis-reports/detail/cobalt-60-sources-in-mosul-recovery-and-lessons-for-the-future/

July 2017 – This report is covered by an exclusive Washington Post story, "How ISIS Nearly Stumbled on the Ingredients for a 'Dirty Bomb,'" by Joby Warrick and Loveday Morris

Two years ago, in the summer of 2015, the Institute decided to investigate whether Daesh controlled dangerous radioactive material in Iraq or Syria. The result of a few months of study by Sarah Burkhard, a young scientist, and other staff surprised us all. Their investigations found that there were apparently two sources of radioactive cobalt in Mosul that posed a risk of being used in a radiological dispersal device. We could not know if Daesh was aware of these sources and their potential, or had already taken possession of them. We produced a confidential research study that we used to alert the United States and other friendly governments of the situation as we knew it, most of which were also monitoring the situation. At the same time, we decided not to publish any of our results. As we learned more, we updated our study, which remains a confidential report due to its sensitivity.

We are very relieved that these two, older albeit still dangerous, cobalt 60 sources were not found and used by Daesh. They were recovered intact recently. We want to thank in particular Joby Warrick at *The Washington Post*, who we had alerted early on for assistance in researching the fate of these sources. He understood the importance of digging into this story while delaying its publication until the radioactive sources were in safe hands. He and his colleagues at *The Washington Post* recently added greatly to this important story.

Background

Daesh rapidly seized control of the Iraqi city of Mosul in 2014 and inherited with it, unknowingly to the public, two cobalt 60 teletherapy machines carrying highly dangerous nuclear material. These machines were procured years ago in the 1980s or even 1970s for the treatment of cancer and conducting research. We estimated based on open source information that the cobalt 60 had decayed considerably but still had a radioactive strength that would place it in the International Atomic Energy Agency's (IAEA's) category 2 of radioactive sources, described as "very dangerous to the person."[1] In terms of dose strength, the sources could produce a fatal dose to an individual at a meter from the source within 2-4 hours. For individuals within 0.1 meter distance, it could occur within 2-3 minutes.

In comparison, a widely publicly discussed radioactive iridium source that went missing in Iraq in late 2015 was also category 2. (The source was later found and secured.)[2] However, we estimated that at least one of the cobalt-60 sources in Mosul had a dose rate roughly 20 times greater than the missing iridium.

Lessons

This case has several lessons for the future and should serve as a reminder of the risks posed by radioactive sources, many of which are poorly protected or accounted for.

We do not know why Daesh did not use the cobalt 60 sources to make a radiological dispersal device. Our speculations include that since the cobalt 60 comes in metal form and not as a powder, it would be more difficult to use the radioactive cobalt, involving steps that can be very dangerous for unprepared and inexperienced individuals. A more likely possibility is that Daesh did not know about the cobalt 60 sources. Did courageous hospital and university staff work successfully to keep the existence of the sources secret?

Other potential reasons for the lack of use include:

- The sources were judged as not destructive enough for Daesh's goals;
- The use of the sources in a radiological dispersal device in the West did not fit the Daesh idea of how they would want to attack the West; or
- The Daesh leadership was pre-occupied elsewhere and did not learn about the sources in Mosul or have a chance to think through the opportunities offered by the cobalt 60 sources.

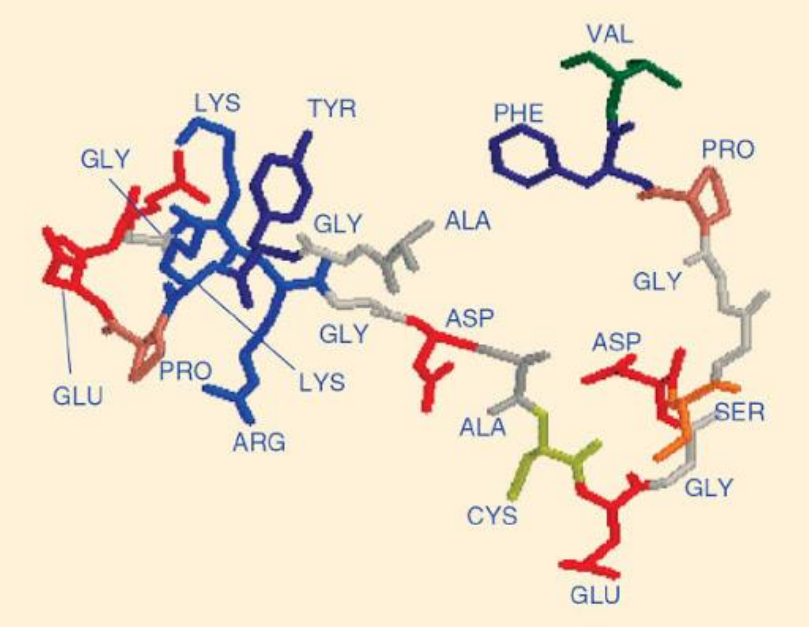
Whatever the actual case, we are relieved that these dangerous sources remained intact and were not seized by Daesh. We may not be so fortunate next time. It is important to learn from this near miss and seek improvements to further reduce the chances of a terrorist group misusing radioactive materials.

This case should lead to reinvigorated efforts to inventory and adequately protect radioactive sources throughout the world. However, as this case highlights, improving physical protection may not be enough. It is also important for the United States and its allies to accelerate programs to identify, consolidate, and remove dangerous radioactive sources, particularly in regions of tension or where terrorists are active. Iraq and other countries in regions of instability and insurgency should receive expedited assistance to remove cobalt 60 sources and receive cobalt-free cancer treatment mechanisms.

BARDA partnering with Chrysalis BioTherapeutics to create peptide capable of countering radiation

Source: https://homelandprepnews.com/stories/58287-barda-partnering-with-chrysalis-biotherapeutics-to-create-peptide-capable-of-countering-radiation/

Dec 03 – The Biomedical Advanced Research and Development Authority (BARDA) is expanding a contract with Chrysalis BioTherapeutics, Inc. to pursue the development of TP508, or **Chrysalin, a peptide** with the potential to counteract injuries resulting from extreme radiation exposure.



Radiation exposure can cause acute and delayed effects on the body, including damage to blood vessels that comprise the circulatory system, provoking inflammation, excessive bleeding or clotting, sepsis, and multi-organ failure. Chrysalin could counter this **by activating stem cells and stimulation of endothelial cells, thereby restoring vascular function**. It could also help reduce inflammation, boost DNA repair, and prevent coagulopathies through nitric oxide signaling.

Chrysalis, established in 2012, will conduct safety studies and other activities required to request emergency use authorization from the U.S. Food and Drug Administration. It will also pursue approval under the FDA Animal Rule.

The parties clearly have nuclear events in mind with the product, reducing overall injury, illness, death, and delayed consequences caused by exposure. This is one of several pioneering efforts Chrysalis is undertaking involving natural regenerative peptides to restore vascular function and activate normal stem cell populations. Such peptides are amino acids that make up proteins in the body, and in the case of Chrysalin, it was derived from the larger thrombin protein released at the point of injury.

Iran Violating 2015 Nuclear Deal Again with Use of Advanced Centrifuges: Reuters

Source: http://www.homelandsecuritynewswire.com/dr20201204-iran-violating-2015-nuclear-deal-again-with-use-of-advanced-centrifuges-reuters

Dec 04 – Iran plans to install more advanced uranium-enriching centrifuges at an underground plant in breach of its troubled deal with major powers, Reuters reported on 4 December, citing a UN nuclear watchdog report.

The confidential International Atomic Energy Agency report obtained by Reuters said Iran plans to install three more clusters of **advanced IR-2m centrifuges** in the underground plant at Natanz, located about 300 kilometers south of the capital, Tehran.

According to its 2015 nuclear deal with major powers, Iran can only use the less-efficient, first-generation IR-1 centrifuges at the underground plant.

Iran recently started uranium enrichment with one cluster of IR-2m machines at Natanz and is planning to install two more clusters, Reuters reported, citing the document.

The breach is the latest in a series of violations by Iran of the nuclear deal in response to President Donald Trump's withdrawal from the agreement and his reimposition of punishing economic sanctions.

Tehran says its breaches can quickly be reversed if Washington's moves are undone. President-elect Joe Biden, who takes office on January 20, said he is willing to rejoin the nuclear agreement if Iran moves back into compliance.

Outgoing U.S. Secretary of State Mike Pompeo said later on December 4 that Iran was "desperately" signaling its willingness to return to the negotiating table to get sanctions relief, though he did not back his claim with any proof.

Dräger Releases X-Site Live Kit for Gas and Radiation Hazard Monitoring

Source: https://www.hstoday.us/industry/industry-news/drager-releases-x-site-live-kit-for-gas-and-radiation-hazard-monitoring/

Dec 03 – Dräger, an international leader in the fields of medical and safety technology, announced the release of the Dräger X-site Live, a state-of-the-art area monitoring kit for gas and radiation hazard monitoring.

The X-site Live is the first industry kit of its kind to offer both gas and radiation detection, as well as FirstNet integration, a nationwide wireless broadband network that provides priority and preemption for First Responders and those who support them.

"We worked in close collaboration with our customers to develop the X-site Live area monitoring solution," said John Wilson, Dräger's senior vice president of sales and marketing for safety solutions in North America. "With their feedback, and Dräger's 70-plus years of experience in developing gas detection devices, we're proud to release a product that will help to safeguard first responders and those who are putting themselves potentially in harm's way to protect the public and their safety in critical situations."

X-site Live Features and Benefits

The Dräger X-site Live comes integrated with a number of practical features and smart benefits including:

- FirstNet network interface for reliable public safety communications
- Smart gateway for Wi-Fi and cellular communication in the cloud
- A re movable X-am 8000, for personal gas monitoring detection that displays up to seven gases at one time
- Live readings that can be sent back to a central monitoring station
- Radiation detection that can also be removed for personal use
- Easy configurability allowing the kit to be up and running in minutes

The multiple benefits and uses of the X-site Live provides applications across multiple areas including fire services, venue protection, hazardous response and others.

The X-site Live is a collaboration between Draeger, Inc. and Safe Environment Engineering, Valencia, California.

European Powers "Deeply Worried" By Iran's Uranium Enrichment Plans

Source: http://www.homelandsecuritynewswire.com/dr20201207-european-powers-deeply-worried-by-irans-uranium-enrichment-plans

Dec 07 – Britain, France, and Germany say Iran's apparent plan to install additional advanced centrifuges at its main nuclear enrichment facility is "deeply worrying" and contrary to the 2015 nuclear deal with world powers. A confidential report by the UN's atomic watchdog, the International Atomic Energy Agency (IAEA), said Iran plans to install three more cascades of advanced IR-2m centrifuges in its underground plant at Natanz.

EDITOR'S COMMENT: Big powers worry about Iran's nuclear ambitions but they do not worry the same about Turkey's similar ambitions! Perhaps it is because they do not sell arms to Iran or because Turkey is a NATO member very close to Pakistan who is a member of the nuclear club. Besides what is the big point about nuclear weapons? Turkey is playing US, France, and perhaps India all possessing nuclear weapons … And there will always be the paradigms of Israel and Pakistan that became nuclear under the nose of those already possessing the nuclear supreme truth.

How to Get Saved from COVID-19 Under Nuclear Bombs

By Manlio Dinucci

Source: https://www.globalresearch.ca/how-get-saved-covid-19-under-nuclear-bombs/5731682

Dec 09 – *FEMA – the United States Government Emergency Management Federal Agency – updated instructions to the population on how to behave in the event of a nuclear attack. The new instructions, provided by the Ready Campaign, keep in mind the Covid-19 pandemic, consequent lockdowns and rules to follow in order to protect ones-self from the virus.*

In order to be ready when an imminent nuclear attack alarm goes off – FEMA warns – you need to know that "Due to COVID-19, many places you may pass on the way to and from work may be closed or may not have regular operating hours". You must therefore first identify "the best places to shelter, they are the basements and the center of large multistory buildings".

In these instructions, FEMA ignores the real effects (scientifically proven) of a nuclear explosion. Even though people on the run are lucky enough to find a Covid-free lockdown place to shelter, they still have no escape. The air displacement caused by the explosion, that generates 800 kmh winds, causes the collapse or burst of even the most solid building. The heat melts the steel, makes the reinforced concrete explode. Even people who find "the best places to shelter" are vaporized, crushed, charred.

The destructive effects of a 1 megaton nuclear bomb (equal to the explosive power of 1 TNT million tons) extend in a circular way up to about 14 km. If a 20-megaton bomb explodes, the destructive effects extend over a range of more than 60 km.

In this situation, FEMA is concerned with protecting people from Covid-19. When the nuclear alarm is raised, it warns: "Check with local authorities to determine which public shelters are open, as shelter locations may have changed due to COVID-19"; at the time of evacuation, "to protect you and your family from Covid-19, bring with you two masks per person and a hand sanitizer that contains at least 60% alcohol"; inside the shelter, "continue to practice social distancing, by wearing a mask and by keeping a distance of at least 6 feet (almost 2 meters) between yourself and people who are not part of your household".

In the event of a nuclear alert, this scenario assumes that 330 million US citizens would not panic, but keep calm, inquire about open shelters, and be concerned about protecting themselves first from Covid-19, bringing along masks and sanitizers, and once in the shelter, maintaining social distancing, with the result being that in a shelter capable of accommodating a thousand people, 200 would be admitted while the others remain outside.

Even if it is absurd that people followed Fema's instructions to protect themselves from Covid-19, they would still be exposed to radioactive fallout in a much larger area than that destroyed by nuclear explosions. An increasing number of apparently unharmed people would begin to show symptoms of radiation syndrome. As there is no possible treatment, the outcome is inevitably fatal.

If radiations hit the nervous system, they cause severe headaches and lethargy, then a state of coma takes over accompanied by convulsions, and death occurs within forty-eight hours. In the case of gastrointestinal radiation syndromes, the victim suffers from vomiting and hemorrhagic diarrhea accompanied by high fever and dies within a week or two.

In this scenario, FEMA is also concerned with the mental state of people. It warns that "the threat of a nuclear explosion can add additional stress to many people who already feel fear and anxiety about Covid-19." Hence, FEMA recommends following the instructions on how to "manage stress during a traumatic event." It thus makes it clear that, in the event of a nuclear attack, US citizens would be assisted by psychologists to teach them how to manage stress while the nuclear bombs explode, by convincing them that thanks to FEMA they were saved from Covid.

***Manlio Dinucci** is a Research Associate of the Centre for Research on Globalization.*

Nuclear notebook: Chinese nuclear forces, 2020

By Hans M. Kristensen and Matt Korda

Source: https://thebulletin.org/premium/2020-12/nuclear-notebook-chinese-nuclear-forces-2020/

Estimated Chinese Nuclear Forces 2020 And 2030*

			2020 Estimate		2030 Projection	
Type	**Fielded**	**Loading**	**Launchers**	**Warheads**	**Launchers**	**Warheads**
Land-based ballistic missiles						
DF-4	1980	1 x 3.3 mt	6	6	0	0
DF-5A	2005	1 x 4-5 mt	10	10	10	10
DF-5B	2015	5 x 200-300 kt MIRV	10	50	10	50
DF-5C	?	5 x 200-300 kt MIRV	0	0	?	?
DF-21A	1996	1 x 200-300 kt	20	20	0	0
DF-21E	2016	1 x 200-300 kt	20	20	40	40
DF-26	2016	1 x 200-300 kt	200	20	300	20
DF-31	2006	1 x 200-300 kt	6	6	0	0
DF-31A	2007	1 x 200-300 kt	36	36	0	0
DF-31AG	2018	1 x 200-300 kt	36	36	72	72
DF-41	(2020)	3 x 200-300 kt MIRV	(16)	(48)	24	72
Subtotal			**344**	**204**	**456**	**264**
Sea-based ballistic missiles						
JL-2	(2015)	1 x 200-300 kt	48	48	72	72
JL-3	(2026)	3 x 200-300 kt			24	72
Subtotal			**48**	**48**	**96**	**144**
Subtotal ballistic missiles			**392**	**252**	**552**	**408**
Air-based weapons						
H-6K	(2015)	1 x bomb	20	20	0	0
H-6N	(2020)	1 x ALBM	(0)	0	10	10
H-20	(2025)	2 x ALCM?	0	0	10	20
Subtotal			**20**	**20**	**20**	**30**
Total			**412**	**272****	**572**	**438**

* *(Corrected table.)* This table builds on estimates published earlier this year but modified for new information included in the 2020 DOD report. The 2030 projection shows what the "more than doubling" of the Chinese stockpile that DOD anticipates over the next decade could potentially look like.
** The DOD report states that China currently maintains an "operational" nuclear warhead stockpile in the low-200s. The estimate probably does not include warheads produced for weapons that are not yet operational, including the DF-41 and JL-2 SLBMs on the two additional SSBNs, and probably does not count bombs for bombers.

Kristensen/Korda, FAS 2020

Dec 07 – China is continuing the nuclear weapons modernization program that it initiated in the 1980s and increased in the 1990s and 2000s, fielding more types and greater numbers of nuclear weapons than ever before. Since our previous Nuclear Notebook on China in June 2019, China has continued fielding the DF-26—a dual-capable, mobile, intermediate-range ballistic missile (IRBM)—and is replacing older road-mobile DF-31A intercontinental ballistic missile (ICBM) launchers with the more maneuverable DF-31AG launcher. China is also in the process of fielding the new DF-41, a road-mobile ICBM that is thought to be capable of carrying multiple independently targetable reentry vehicles (MIRVs) like the old DF-5B. At sea, China has completed construction and deployment of two more ballistic missile submarines and is developing a new type. Additionally, China has recently reassigned a nuclear mission to its bombers and is developing an air-

launched ballistic missile that might have nuclear capability.
We estimate that China has a produced a stockpile of approximately 350 nuclear warheads, of which roughly 272 are for delivery by more than 240 operational land-based ballistic missiles, 48 sea-based ballistic missiles, and 20 nuclear gravity bombs assigned to bombers. The remaining 78 warheads are intended to arm additional land- and sea-based missiles that are in the process of being fielded (see Table 1). This estimate is higher than the "low-200" warheads reported by the Pentagon in its 2020 report to Congress; however, the Pentagon's estimate only refers to "operational" Chinese nuclear warheads, and therefore presumably excludes warheads that are attributed to newer weapons still in development (US Defense Department 2020a). It is also possible that the Pentagon's estimate does not include dormant bomber weapons. Taking those categories into account, the Pentagon's estimate is roughly in line with our own.

US estimates of Chinese nuclear weapons
The US declaration in 2020 that China has in the low-200s operational nuclear warheads was a surprise because the number was lower than expected and much lower than the many hundred—even thousands—of warheads that some have warned about in recent years (Heinrichs 2020, Howe 2020, Schneider 2019, Karber 2011). Although the low estimates have varied, they have generally been correct, while the higher estimates have been incorrect. When rumors about much higher estimates emerged nearly a decade ago, General Robert Kehler, then the commander of US Strategic Command, said, "I do not believe that China has hundreds or thousands more nuclear weapons than what the intelligence community has been saying, [...] that the Chinese arsenal is in the range of several hundred" nuclear warheads (Kristensen 2012).
Kehler's statement about "several hundred" warheads is one of the reasons why we believe that the low-200s estimate listed in the Defense Department report is slightly low. He gave that statement in 2012, when China only had about 60 ICBMs, none of them had been equipped with MIRVs, and the JL-2 missile on the Jin-class ballistic missile submarines was not yet operational.

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

Hans Kristensen *is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the* SIPRI Yearbook *(Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored Nuclear Notebook since 2001.*

Matt Korda *is a research associate for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the* Bulletin*'s Nuclear Notebook with Hans Kristensen. Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. He is also the co-director of Foreign Policy Generation—a group of young people working to develop a progressive foreign policy for the next generation.*

How to Reduce the Risk of Radiological Dirty Bombs?

By Jacob Kamen Ph.D., DABHP
Source: https://nct-magazine.com/nct-magazine-december-2020/how-to-reduce-the-risk-of-radiological-dirty-bombs/

While the CBRN community including civil and military first responders are trained to respond to radiological dirty bomb, the risk of dirty bomb could be reduced by encouraging institutions who have such sources to migrate to Alternative Technologies and dispose these radioactive sources. Due to the unique characteristics of the cesium chloride (Cs-137) used in medical and research irradiators, it is especially susceptible to be used as a dirty bomb. Terror organizations have been trying hard to get their hands-on high activity radioactive materials and use them as Radioactive Dispersal Device (RDD) or dirty bomb. These types of devices are considered as Weapons of Mass Disruption (WMD) and could bring the economy of a densely populated area to its knees. The recent University of Washington Research Center incident in Seattle with a minor Cs-137 leakage, and its cost (about $100 million), is an example of how expensive the total

loss could be. Unfortunately, there are thousands of high radioactive irradiators still being used in Universities and Hospitals. This article describes steps to take to reduce this risk. Mount Sinai Hospital in NYC originally had four of such irradiators with cesium sources. Mount Sinai took steps to reduce the risk of Cs-137 Irradiators by using Alternative Technologies which presently exist in the market. As of January 2018, Mount Sinai in NYC successfully disposed all its Cesium-137 irradiators. The CBRN community could encourage the institutions having such sources in their campus to start using alternative technology and reduce the risk of dirty bomb. Financial incentive is available from the US government offices of DOE-NNSA-ORS under OSRP and CIRP program.

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

Dr. Jacob Kamen *is the Senior Director and the Chief Radiation Safety Officer for the Mount Sinai Health System (MSHS). He also serves as Professor of Radiology. He is board certified by the NRRPT, ABHP and BLS. He earned his doctoral degree in Nuclear Engineering at Columbia University where he served as the president of ANS University Chapter. He spent several years at Brookhaven National Laboratory (BNL), home to seven Nobel Prizes. He was elected as the President of GNYCHP in 2004 and as the Executive Council for 2010 and 2011. He received BLS illumination award given by the Board of Laser Safety for his leadership as well as David Sliney award for laser safety excellence. As an SME, he was invited to speak at various conferences such as ANS, HPS, and IAEA. He has chaired many sessions at both national and international meetings including the Institute for Nuclear Material Management (INMM), HPS, ANS, IAEA, etc. In 2011, he delivered the opening statement at West Point Academy for the GNYHPS meeting following the Fukushima Daiichi nuclear disaster. Subsequently, he was interviewed by Fox News TV in NY as well as the Daily News about Fukushima nuclear accident.*

Satellite Photos Reportedly Show New Construction at Iran Nuclear Facility

Source: https://www.rferl.org/a/iran-satellite-photos-fordow-construction-nuclear/31007540.html

Dec 18 – Satellite imagery obtained by the Associated Press on December 18 shows construction work has begun at a controversial underground **Iranian nuclear facility at Fordow**, the news agency said.

New work at any nuclear facility in Iran is likely to exacerbate international tensions as the outgoing

U.S. administration of Donald Trump continues to exert pressure on Tehran over its nuclear and weapons programs and its activities in the region.

A photo from a week earlier obtained from Maxar Technologies reportedly shows what looks like a freshly dug foundation for a building with dozens of pillars extending into the ground that could provide anti-earthquake support.

Iran's representatives to the United Nations and officials at the International Atomic Energy Agency (IAEA) were not initially available for comment, AP reported.

"Any changes at this site will be carefully watched as a sign of where Iran's nuclear program is headed," said Jeffrey Lewis, an expert at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies.

The head of the International Atomic Energy Agency (IAEA), Rafael Grossi, said on December 17 that if the incoming U.S. administration wanted to revive the 2015 nuclear agreement that Washington pulled out of two years ago, it would have to reach a new deal on reversing Iran's subsequent breaches.

One of the possible breaches involves the resumption, announced a year ago, of uranium-enrichment activities at Fordow.

President-elect Joe Biden has said the United States will rejoin the Joint Comprehensive Plan of Action (JCPOA) "if Iran resumes strict compliance" with the deal, which eased UN sanctions in exchange for curbs on Iran's disputed nuclear activities.

Trump exited the deal in 2018. Biden is due to be sworn in on January 20.

"I cannot imagine that they are going simply to say, 'We are back to square one' because square one is no longer there," Grossi told Reuters at IAEA headquarters on December 17.

Citing "more [nuclear] material" and "more activity, more centrifuges" and other factors, Grossi said that the question of a resumption is "at the political level to decide" and that "undoubtedly" there would have to be a second deal.

"It is clear that there will have to be a protocol or an agreement or an understanding or some ancillary document which will stipulate clearly what we do," Grossi said.

The recent construction site lies northwest of Fordow's underground facility, which is known to house uranium-enrichment technology and is built deep inside a mountain for security reasons.

A Twitter account called Observer IL recently published an image of Fordow showing the work, saying it had come from South Korea's Korea Aerospace Research Institute.

The Korean institute later acknowledged taking the photo, AP said.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

This 3D Printed Bone Brick Could Transform How We Treat Bomb Injuries

By Paulo Bartolo

Source: https://cbrnecentral.com/this-3d-printed-bone-brick-could-transform-how-we-treat-bomb-injuries/25018/

June 2020 – For thousands of Syrian refugees who have suffered horrific blast injuries after being hit by barrel bombs and other devices of death in their war-torn homeland, the only option is amputation. When you see the damage a blast injury can do it's a shock to the system and is so very sad and upsetting.

Barrel bombs have been dropped throughout the long conflict that has torn Syria apart and caused untold misery and pain to so many innocent civilians. At the start of 2018, Amnesty International reported that barrel bombs had killed more than 11,000 civilians in Syria since 2012, injuring many more.

The barrel bomb is a type of improvised explosive device which – according to the UN – is used extensively by the Syrian Air Force. They are made from large oil barrels and are typically filled with TNT, oil and even chunks of steel. Due to the large number of explosives that can be packed into a barrel, the resulting explosion can be devastating.

Even if a person survives such a blast, their limbs are at risk of suffering a large, often jagged break which, even in the best conditions, would be a major challenge to repair. In a fully equipped, state-of-the-art hospital such patients would be able to access expert orthopaedic surgery and a lot of expensive aftercare.

But in a refugee camp, far away from any sophisticated surgical intervention, these types of complex procedures with timely recovery and care implications are just not possible. So at the moment, amputation is unfortunately the most likely outcome in many of these cases.

Many of these bone shattering injuries are untreatable because of the constant risk of infection from procedures carried out in the field and the collapse of the healthcare system. A simpler and cheaper way to help these people needed to be invented and my colleagues and I believe we have done just that.

Andrew Weightman and Paulo Bartolo in the lab. (JillJennings / The University of Manchester, Author provided).

Our treatment uses a temporary, 3D printed "bone brick" to fill the gap. They are made up of polymer and ceramic materials and can be clicked together just like a Lego brick to fit perfectly into whatever gap has been created by the blast injury. The bricks are degradable and allow new tissue to grow around them. This structure will support the load like a normal bone, induce the formation of new bone and, during this process, the bricks will dissolve. The idea is that the surgeon can open a bag of bricks and piece them together to fit that particular defect and promote the bone growth.

The solution has been a long time coming and it was very much the plight of Syrian refugees that inspired it. It struck a very personal chord. I recognise that misery and pain and see my younger self on the faces of the children. I was born and grew up in Mozambique in South-East Africa in 1968. It was the middle of the war of independence and the country was in turmoil.

My family inevitably became caught up in the decade-long conflict that involved the Portuguese community that was living and working in Mozambique and the Frelimo (The Mozambique Liberation Front) resistance movement that were seeking independence and self-rule.

It was 1973 and these were dangerous times. I was about five years old and it was a very frightening and disruptive period of my life. We moved up and down the country as my father's job in civil administration changed and required us to move to the Niassa government base in Vila Cabral (now Lichinga).

One episode sticks out vividly. My one-year-old brother, Jose Manuel, and I were taken from our home in Maragra and moved to a refugee camp in an area of South Africa called Nelspruit, as we tried to escape the escalating violence. We were safe but I was always anxious and scared about the security of our family.

Although we were only in the camp for around a month before we were transferred to start a new life in Portugal when I was six, that experience stayed with me for life. It gave me a strong sense of empathy for others who are being displaced by war. And it would eventually strengthen my commitment to use my bio-medical expertise to try and do something to help other refugees.

Blast Injuries and Amputations

The first time I was made fully aware of the impact of blast injuries in the Syrian conflict was when Amer Shoaib – a consultant orthopaedic surgeon at Manchester Royal infirmary – came to my university to discuss his experience and the problems he faced in treating these injuries in Syrian refugees.

Shoaib is a limb-injury expert with experience of working on the frontline of various conflicts and crisis zones as a humanitarian worker. He told us that in Syria the after effects of blast injuries were sometimes untreatable because of the constant risk of infection. The collapse of the healthcare system has also led to many treatments being done by people who are not, in fact, trained medics.

Shoaib was working in refugee camps in Turkey and I, along with my Manchester research colleagues Andy Weightman and Glenn Cooper, decided we needed to help and apply our expertise. We all wanted to make a difference and we continued our discussion late into the evening. This conversation developed into the idea of the "bone bricks".

A Game-Changer

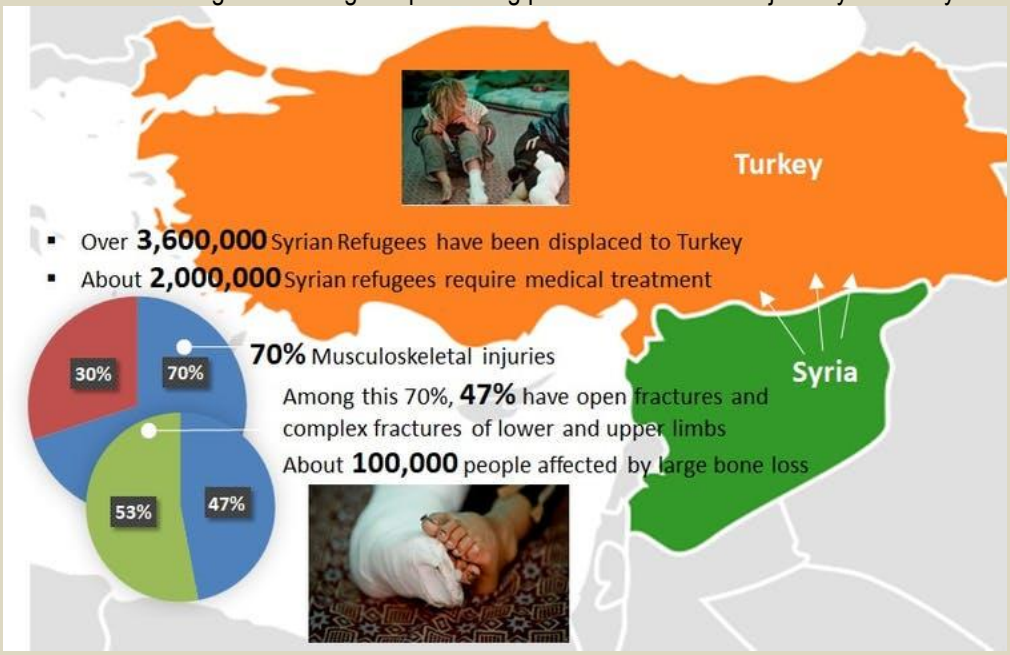
My own academic interests include biofabrication for tissue engineering. This involves fabricating bone, nerve, cartilage and skin through the use of 3D printing. 3D printing technology can now reproduce biocompatible and biodegradable materials that can be used in the human body.

Current grafting techniques have several limitations, including the risk of infection and disease transmission. They are also quite costly and present a high risk of further injury and serious bleeding. This work is centred on creating orthopaedic devices – or scaffolds – that can enable the regeneration of bone tissues to repair fractures.

I had been busy responding to the calls from clinicians to make these tools more agile, smaller in scale and responsive to more personalised healthcare. But the challenge set by the Syrian situation was a game-changer: we had to consider other new factors, such as making the scaffolds even more cost-effective and useable in demanding environments where it is very difficult to manage infection.

Part of our solution to these challenges was to use relatively low-cost 3D printing technology to create bone bricks with a degradable porous structure into which a special infection-fighting paste can be injected. The bone brick prosthesis and paste will prevent infection, promote bone regeneration and create a mechanically stable bone union during the healing period.

The challenge of creating this pioneering prosthesis led us on a journey to Turkey in 2016 where we met with academics, surgeons and medical companies. We were convinced that our proposed new technique could dramatically improve the medical response to life-changing limb injuries in the challenging conditions of these camps. It was clear that our project should be focused on patients within the Syrian refugee community in Turkey where they have found a safe haven from the horrors of war.



Author provided

Once we secured the backing of the Global Challenges Research Fund (a £1.5 billion pot provided by the UK government to support cutting edge research that specifically addresses the challenges faced by developing countries) we began to put our project into motion. As a first step Weightman, Cooper and I visited Sabanci University in Istanbul to meet with our lead collaborator there, Bahattin Koç, who introduced us to a group of clinicians who had been dealing with the refugees and their injuries firsthand and

were able to share their knowledge. Their experiences gave us insight into the challenges of treating serious bone injuries in the field.

Our collaborators in Turkey helped to ensure we shaped the design and specifications of the bone bricks so they aligned as closely as possible to the needs of the frontline clinicians. During our stay in Istanbul, we were constantly reminded of the human cost of the Syrian civil war. We would often witness groups of displaced families, including children, who had fled the conflict and were seeking refuge and the chance to rebuild their lives. What we had seen on TV about Syria, with helicopters dropping bombs, was brought home to us. Some of my colleagues have children the same age as those we want to help and it made us even more determined to do something.

War in Syria

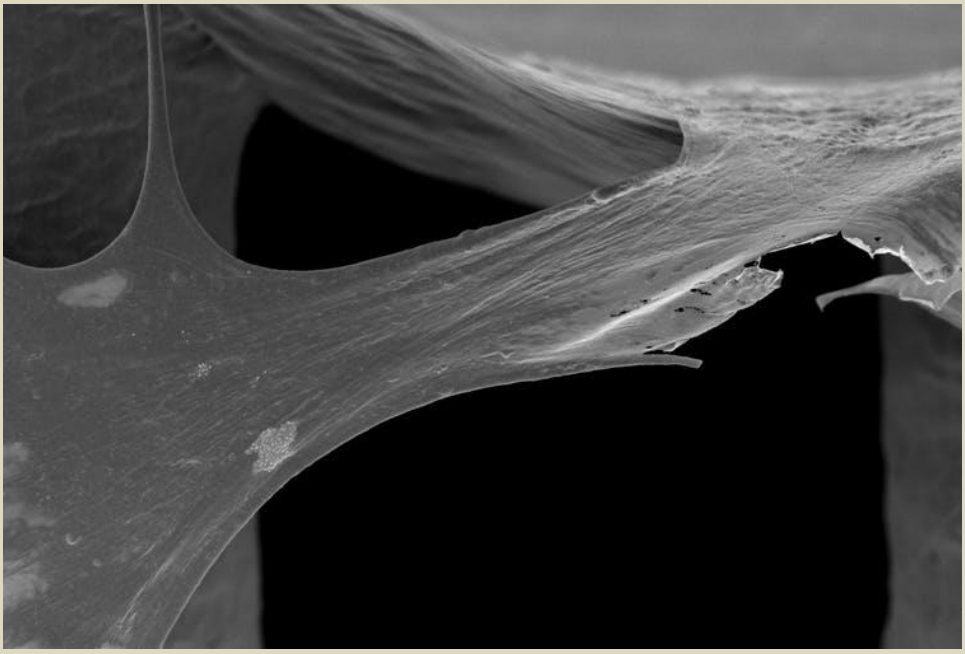
The Syrian conflict has displaced around 3 million refugees into Turkey, accounting for around 4% of its population. Turkey provides free healthcare services to Syrians and, as such, the burden on the healthcare system is significant, with 940,000 patients treated, 780,000 operations and 20.2 million outpatient services taken up between 2011 and 2017 alone.

The Turkish government says it has spent more than US$37 billion hosting Syrian refugees. We hope that our bone bricks innovation can make a contribution to this crisis, helping to mitigate Turkey's healthcare costs and also significantly improve the human cost of this crisis.

Our project is focused on bone injuries that are often caused by blast explosions, which are powerful enough to throw a person many yards and shatter bodies. Shoaib once said to us:

If you look at the way people were injured 100 years ago, 90% were the military and 10% were civilians. It's now the other way around.

This is certainly true for the Syrian crisis where thousands of people are suffering terrible injuries. Given that almost 2 million people have been injured in the Syrian civil war, we estimate that 100,000 people have been affected by large bone loss and of those injured since 2013 there have been more than 30,000 amputations – equating to about 7,500 a year. Amputation has associated physical complications including heart attack, slow wound healing and the constant risk of infection.



Bone brick under x750 magnification. Paulo Bartolo, Author provided

Catastrophic Limb Amputation

Current bone repair techniques are complex. They include:

- The leg or arm being harnessed in a metal fixing device or cage which allows slow-growing bone tissue to reconnect. But this process frequently creates complications caused by metal wires transfixing and cutting through soft tissues as the frame is extended to lengthen the bone. It is a lengthy and meticulous.
- Placing a pin or plate implant to stabilise the bone gap and enable the tissue to reconnect. This procedure requires complex surgery in specialist centres of excellence and can only be considered in extreme and selected cases.
- Bone shortening procedures, where healing is stimulated by removing damaged bone tissue. Or there are forms of bone grafting techniques which use transplanted bone to repair and rebuild damaged bones.

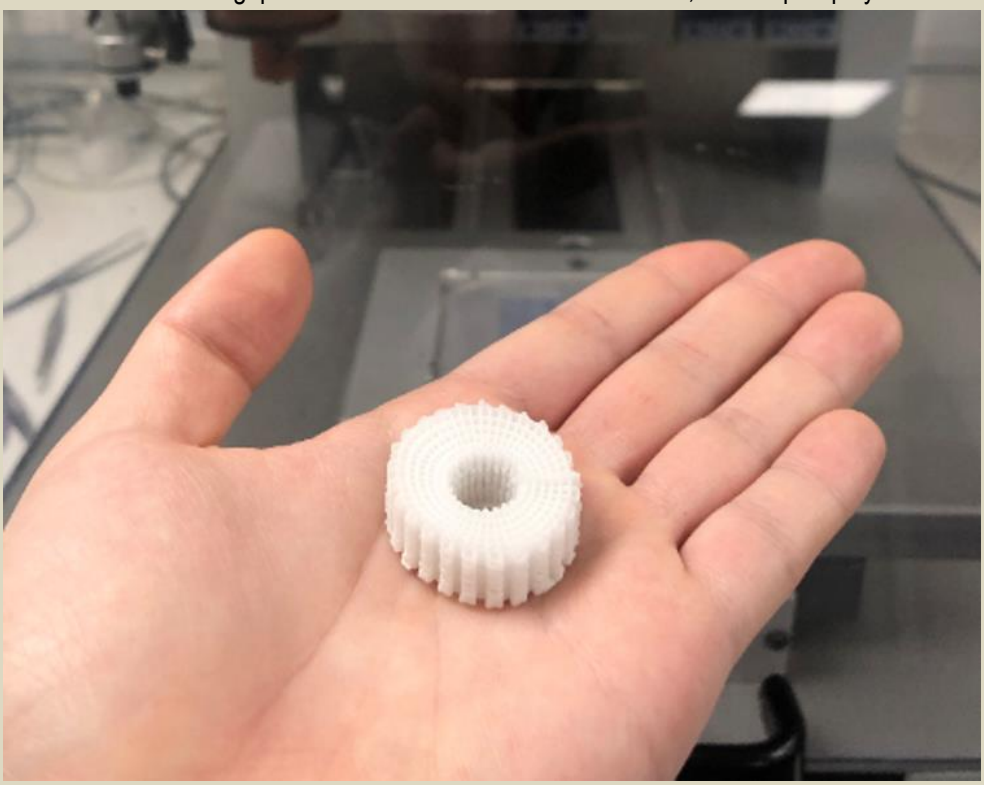
And it must be remembered, traumatic limb amputation is a catastrophic injury and an irreversible act that has a sudden and emotionally devastating impact on the patient. As a consequence, this not only impacts a person's ability to earn a living but also brings very serious psychological issues for the patient because of the cultural stigma associated with limb loss.

External prosthetic limbs after amputation provide some with a solution but they are not suitable for all. Studies show that the long term healthcare costs of amputation are three

times higher than those treated by limb salvage. Clearly, saving a limb offers a better quality of life and functional capacity than amputation and external prosthetics.

Just Like Lego

With many blast injuries, the bone defects are totally impossible to heal. What we are doing is creating a temporary structure using bone bricks to fill the gap. Our treatment uses medical scaffolds, made up of polymer and ceramic materials, which can be clicked together like a Lego brick, creating a degradable structure which then allows new tissue to grow.

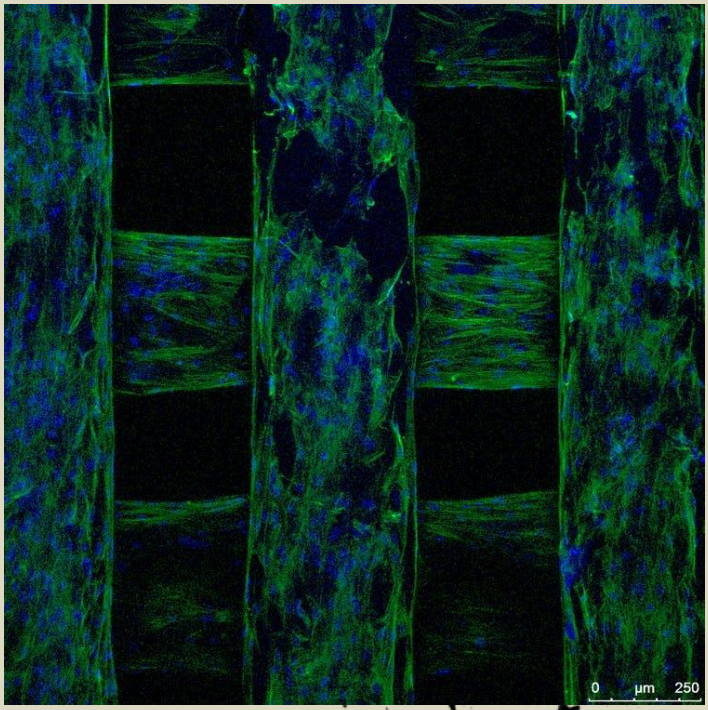


A prototype brick just off the 3D printer at the University of Manchester. Paulo Bartolo, Author provided

We are also developing software to allow the clinician, based on the information on the bone defect, to select the exact number of bone bricks with the specific shape and size and information on how to assemble – just like Lego instructions. The connection between the bone brick design and the 3D printing system is completed. We're now in the process of integrating with the software that will link the scanning of information from the wound area with the identification of the correct type of bone bricks and assembly mechanism.

An antibiotic ceramic paste is stored in a hollow in the middle of the brick and is a highly practical way to combat infection while the limb repairs and hugely improves the chances of success.

The bone brick solution is much more cost effective than current methods of treatment. We expect our limb-saving solution will be less than £200 for a typical 100mm fracture injury. This is far cheaper than current solutions, which can cost between £270 and £1,000 for an artificial limb depending on the type needed.



A bone brick under Electron Microscopy scanning. Paolo Bartolo, Author provided

When Will They Be Used on Humans?

My team and I are entering the final stages of a three-year project. Our team consists of academics and clinicians from Manchester and Turkey, as well as a pool of ten bone injury patients drawn from the UK, Turkey and Syria. We have already evaluated the modular bone bricks system in a computer simulation, created prototypes of the modular bone bricks using 3D printing technologies in the lab, and conducted in-vitro (laboratory) testing of mechanical and biological characterisation of the bricks. This will be followed by in-vivo (animal) testing to prepare the device for regulatory approval and a

pathway to implementation by clinicians. Once all these stages are complete the project we will be ready to trial on human patients. The final stage will then be to translate the research into building a useable, medical device. This will be undertaken by a follow-on clinical trial on about 20 patients with large bone loss, some of which we expect will be drawn from the Syrian refugee community. The project will be subject to strict ethical scrutiny and approval.

We hope this project will lead to further development of emergency healthcare in the developing world and could bring hope to a Syrian refugee community in dire need while their country rebuilds. Our long term hope is that bone bricks will be of use, not only in refugee crises, but also in many other healthcare situations, such as accidents and natural disasters – in both developing and developed nations. For example, in the UK around 2,000 patients a year receive treatment for severe fractures requiring surgical reconstruction for bone loss.

The burden to the health service relating to major traumatic injuries is estimated to be in excess of £0.5bn. In addition, the estimated loss of contribution to the economy due to extended periods of rehabilitation is another £3.5 billion.

We believe the bone brick project could help alleviate some of those economic burdens and drastically improve the patient experience. But it is the plight of the Syrian refugees that continues to inspire and inform this project. We hope that, perhaps in five years' time, bone bricks will be used in the field on humans, finally giving medics and victims an alternative to catastrophic limb amputation.

***Paulo Bartolo** is Chair Professor on Advanced Manufacturing at the* University of Manchester. *This article was written with the assistance of Shaden Jaradat from The University of Manchester. Bone bricks research credits go to Paulo Bartolo, Glen Cooper and Andrew Weightman from The University of Manchester, Bahattin Koc from Sabanci University in Turkey and Gordon Blunn from the University of Portsmouth, with clinical support from Amer Shoaib. The research is funded by the Engineering and Physical Sciences Research Council. The research team is grateful for the excellent work conducted by a large number of post-doctoral research associates, PhD and MSc students.*

Explosion rocks Greek-operated tanker in Saudi port

Source: https://www.aljazeera.com/news/2020/11/25/mine-explodes-damaging-oil-tanker-off-saudi-arabia

Nov 25 – An explosion has rocked a Greek-operated tanker docked at Saudi Arabia's Red Sea port of Shuqaiq, in an attack that a Saudi-led military coalition blamed on Yemen's Houthi rebels.

The owners of the Maltese-flagged tanker Agrari tanker said on Wednesday it was "attacked by an unknown source" while it was preparing to depart from Shuqaiq.

"The Agrari was struck about one metre (three feet) above the waterline and has suffered a breach," said TMS Tankers, the vessel's Greece-based owner.

"It has been confirmed that the crew are safe and there have been no injuries. No pollution has been reported."

A Greek ministry press official said the tanker was flying a Maltese flag and there were 25 crew members onboard including seven Greeks.

The tanker was carrying no cargo when the explosion happened, the ministry added.

British maritime security company Ambrey said the ship was damaged by a mine while berthed at the Shuqaiq Steam Power Plant (SSPP).

"The explosion took place in port limits and punctured the hull of the vessel, which is in ballast," Ambrey said in a statement, adding that the vessel had arrived at Shuqaiq on Monday.

An investigation was under way after Saudi authorities, including the coastguard, boarded the stricken vessel, it added.

Foiled 'terrorist act'

The Saudi Arabia-led coalition fighting the Houthis said the vessel suffered minor damage from the blast, in what it described as a foiled "terrorist act", Al Arabiya reported.

Without naming the vessel, the coalition said the incident occurred when an explosives-laden boat launched by the Houthis was intercepted and destroyed.

The commercial vessel was damaged by shrapnel from the "booby-trapped boat", the coalition was quoted as saying by the Saudi state-run Al-Ekhbariya television.

"The hostile acts of the Houthi militia threaten shipping lanes and global trade," the coalition said.

So far, there has been no comment from the Houthis.

The Red Sea is a vital shipping lane for both cargo and the world's energy supplies.

Rising tensions

The explosion comes amid rising tensions between Saudi Arabia and the Houthis, who recently intensified cross-border attacks on the kingdom.

On Monday, a cruise missile fired by the rebels struck an oil facility in Saudi Arabia's Red Sea city of Jeddah.

On Tuesday, the coalition said it had destroyed five naval mines allegedly laid by Houthis in the southern Red Sea.

Two weeks ago, a fire near a floating platform belonging to the Jazan oil products terminal was contained with no injuries.

That fire was the result of another attempted Houthi attack, in which the coalition intercepted and destroyed two explosive-laden boats in the southern Red Sea.

The military coalition has been battling the Houthis in Yemen since March 2015.

Despite its superior firepower and an investment worth billions of dollars in military hardware, the coalition has struggled to oust the rebels from their northern strongholds, including the capital, Sanaa.

Tens of thousands of people, mostly civilians, have been killed and millions displaced in what the United Nations has called the world's worst humanitarian disaster.

EDITOR'S COMMENT: If I remember well, Iranians used to pond mines in the Arab Gulf in the past. Houthis are Iranian-backed, so … Of course, it might be just accidental but mines do not pop-up like this and for no reason. Certain early detection measures should be taken because this might be the first incident of a new marine tactic aiming to cause serious problems in the global trade. Keep in mind that mines are not on sea surface but are "hidden below and waiting" for the big fish to pass over! In addition, the cost to benefit ratio is very attractive; mines are not difficult to find, buy, make, and if they manage to sink a tanker (more than one required) the impact would be enormous. On the other hand, the mine could be a warning against the ongoing collaboration between Greece, S. Arabia, UAE, and Israel that might stressed one or two global chess players in the area

Thai counter-terrorism unit get explosive deactivation aunav.NEXT robots

Source: https://www.armyrecognition.com/defense_news_december_2020_global_security_army_industry/thail_counter-terrorism_unit_get_explosive_deactivation_aunav.next_robots.html

Dec 02 – Thailand has incorporated seven units of the aunav.NEXT robot. Developed and manufactured entirely in Spain, its two synchronized armsmake it unique on the market.

The customer, a Thai active counter-terrorism unit,was also supplied with seven aunav.VAN command and control vehicles, the rapid intervention and transport unit developed to meet the needs of CBRN and explosive deactivation units. This acquisition allows the counter-terrorism unit to neutralize possible threats in various southern provinces of the country.The aunav.NEXT robot combined with the aunav.VAN units enhance the ability of the customer to safely disable improvised explosive devices hidden in motorcycles or other vehicles.

The continent´s security forces in countries such as Vietnam, China, and India already trust aunav robots. The Spanish manufacturer has more than 200 units sold in 16 countries worldwide.

aunav.NEXT robots ready for delivery to the Thai counter-terrorism unit (Picture source: aunav)

Spanish technology that helps save lives

The aunav.NEXT robot is developed in Spain in collaboration with bomb squad units.It is specifically designed for the deactivation of improvised explosives (IED), ammunition control (EOD), or CBRN (Chemical, Biological, Radiological, and Nuclear) activities. It is an advanced system that effectively combines strength and dexterity thanks to its two synchronized arms, capable of liftingup to 250 kg.

The aunav.VAN is a light transport and rapid intervention vehicle, specifically designed to meet the operational needs of aunav robots as a controlcenterunit at the intervention site.

aunav is part of the Robotics Unit of everis Aerospace, Defense and Security (everis ADS), and designs and manufactures all its products in Spain, at the production center located in Binéfar (Huesca).

Donors Say Beirut's Recovery Will Cost $2.5 Billion

Source: http://www.naharnet.com/stories/en/277340-donors-say-beirut-s-recovery-will-cost-2-5-billion

Dec 04 – The European Union, United Nations and World Bank published the plan four months after the country's worst peacetime disaster on August 4 that killed more than 200 people, wounded thousands and ravaged a huge part of Beirut.

They said the roadmap for the next 18 months was to both help the most vulnerable people with international grants and focus on reconstruction funded by loans and private funds hand-in-hand with sweeping reforms.

"The priority needs of the people-centered recovery track amount to $584 million, of which $426 million are needed for the first year," said a report on the roadmap.

"The costs for the reform and reconstruction track are estimated at $2 billion."

But those behind the plan warned international support for the reconstruction would "depend on the government's ability to demonstrate credible progress on reforms".

In particular, "efforts should include the forensic audit of the central bank, banking sector reform, capital control, exchange rate unification and creation of a credible and sustainable path to fiscal sustainability," the report said.

This would be essential to secure private funding and public sector loans, it added.

The EU, UN and World Bank requested a long list of urgent measures, including a "transparent investigation" into the port blast, and the enacting of "a new Port Sector Law, addressing the port authority's operations as well as customs".

Lebanon is mired in its worst economic crisis in decades.

The value of the local currency has plummeted against the dollar, prices have soared, and poverty has risen to more than half the population.

Lebanon's government resigned after the August explosion, but talks have stalled to form a new cabinet essential to start reforms towards unlocking billions in desperately needed financial aid.

Last month, an international firm pulled out from a forensic audit of the central bank after it did not receive data needed for the mission.

An investigation into the blast launched by Lebanese authorities has led to the arrest of 25 people, including top port and customs officials, but no conclusions have been drawn yet.

Explosives-laden boat hits fuel ship at Saudi port, ministry says

Source: https://www.reuters.com/article/saudi-ship-blast-bw-group-int/explosives-laden-boat-hits-fuel-ship-at-saudi-port-ministry-says-idUSKBN28O0BJ

Dec 14 – **Saudi Arabia said on Monday that a fuel transport ship anchored at a Jeddah terminal was hit by an explosive-laden boat in what it called a terrorist attack, after shipping firm Hafnia said one of its tankers was struck by an "external source".**

A Saudi energy ministry spokesman, in a statement carried on state media, did not mention the name of the vessel or identify who was behind the attack. [L8N2IU3VM]

Hafnia said there was an explosion and a fire while its oil tanker, the **BW Rhine**, was discharging at Jeddah port. The ship's crew put out the fire and no-one was injured, it said, adding that parts of the ship's hull had been damaged.

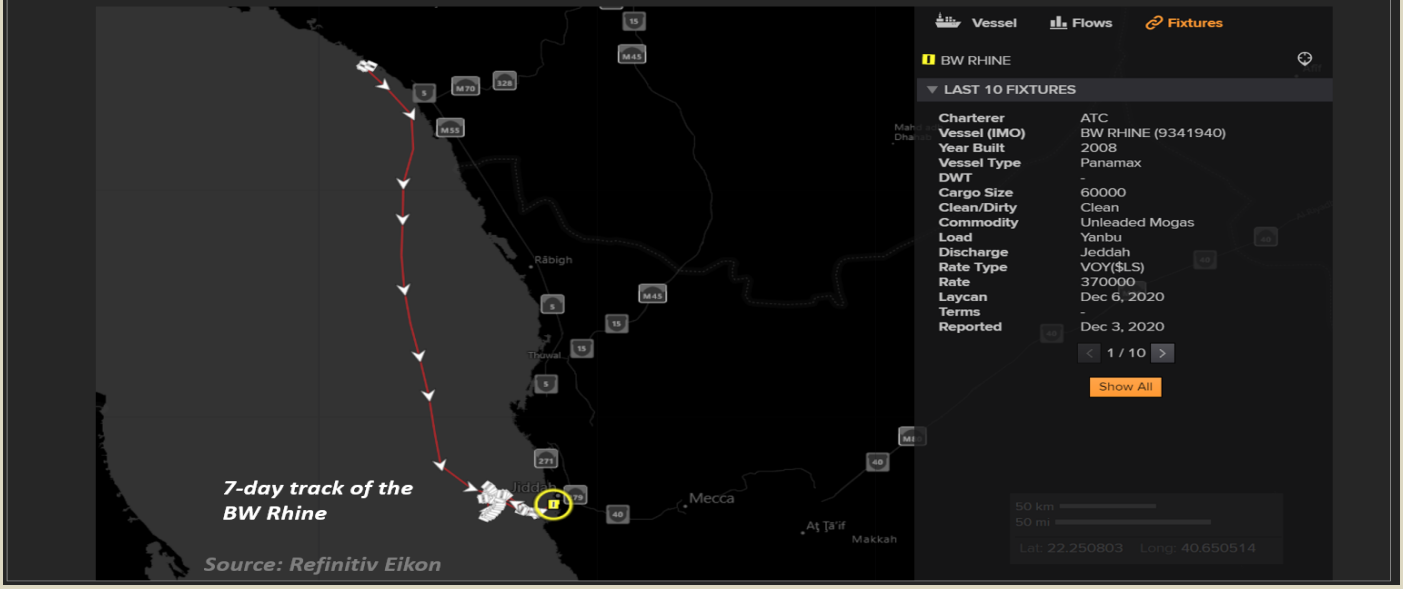
Al Arabiya TV cited the captain of the BW Rhine as saying that **small boats had been spotted ahead of the explosion**, and that one of the vessel's tanks was damaged in the blast.

"BW Rhine has been hit from an external source whilst discharging at Jeddah, Saudi Arabia at approximately 00:40 local time on 14 December 2020, causing an explosion and subsequent fire onboard," Hafnia said in a statement on its website.

The Saudi energy ministry spokesman said the attack resulted in a small fire which emergency units extinguished, but that there was no damage to unloading facilities nor any effect on supplies.

The United Kingdom Maritime Trade Operations said on its website that Jeddah port had reopened after closing following the incident. "These acts of terrorism and vandalism, directed against vital installations, go beyond the Kingdom and its vital facilities, to the security and stability of energy supplies to the world and the global economy," the ministry spokesman said.

Path of the BW Rhine tanker, which was hit by an unidentified object while discharging fuel at Jeddah port, Saudi Arabia
Shipping firm Hafnia says there was an explosion and fire that crew put out. No one was injured.



Shrapnel

He referred to an explosion last month that damaged a **Greek-managed tanker at a Saudi terminal on the Red Sea just north of the Yemeni border.** The Saudi-led military coalition engaged in Yemen had said the vessel suffered minor damage from shrapnel in what it described as a foiled terror attack.

Saudi Arabia last month blamed Yemen's Iran-aligned Houthi movement for a "projectile attack" on a petroleum products distribution plant in Jeddah and for a foiled attack involving explosive-laden boats that caused a limited fire near a floating platform belonging to the Jazan oil products terminal.

A U.S. official, speaking on the condition of anonymity, said that the United States did not have a firm attribution on who was responsible for Monday's incident.

The official said that it was further north than other incidents but initial suspicions fell on the Houthis.

The BW Rhine, owned and operated by Hafnia, is a Singapore-flagged tanker with capacity to carry 60,000-80,000 tonnes of light and middle distillate oil products, according to Hafnia and shipping data on Refinitiv.

The tanker loaded about 60,000 tonnes of gasoline from Yanbu port on Dec. 6, the data showed. It is **currently 84% full,** according to its draft. "It is possible that some oil has escaped from the vessel, but this has not been confirmed and instrumentation currently indicates that oil levels on board are at the same level as before the incident," Hafnia said.

EDITOR'S COMMENT: Somebody in the area has a very good knowledge in speedboads and asymmetric operations. Emergency response plans should be updated and re-evaluated. It could be a new beginning of terrorist attacks (perhaps with collaboration with local pirates that have an excellent knowledge of both Red Sea and Gulf of Aden waters.

ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

C²BRNE DIARY

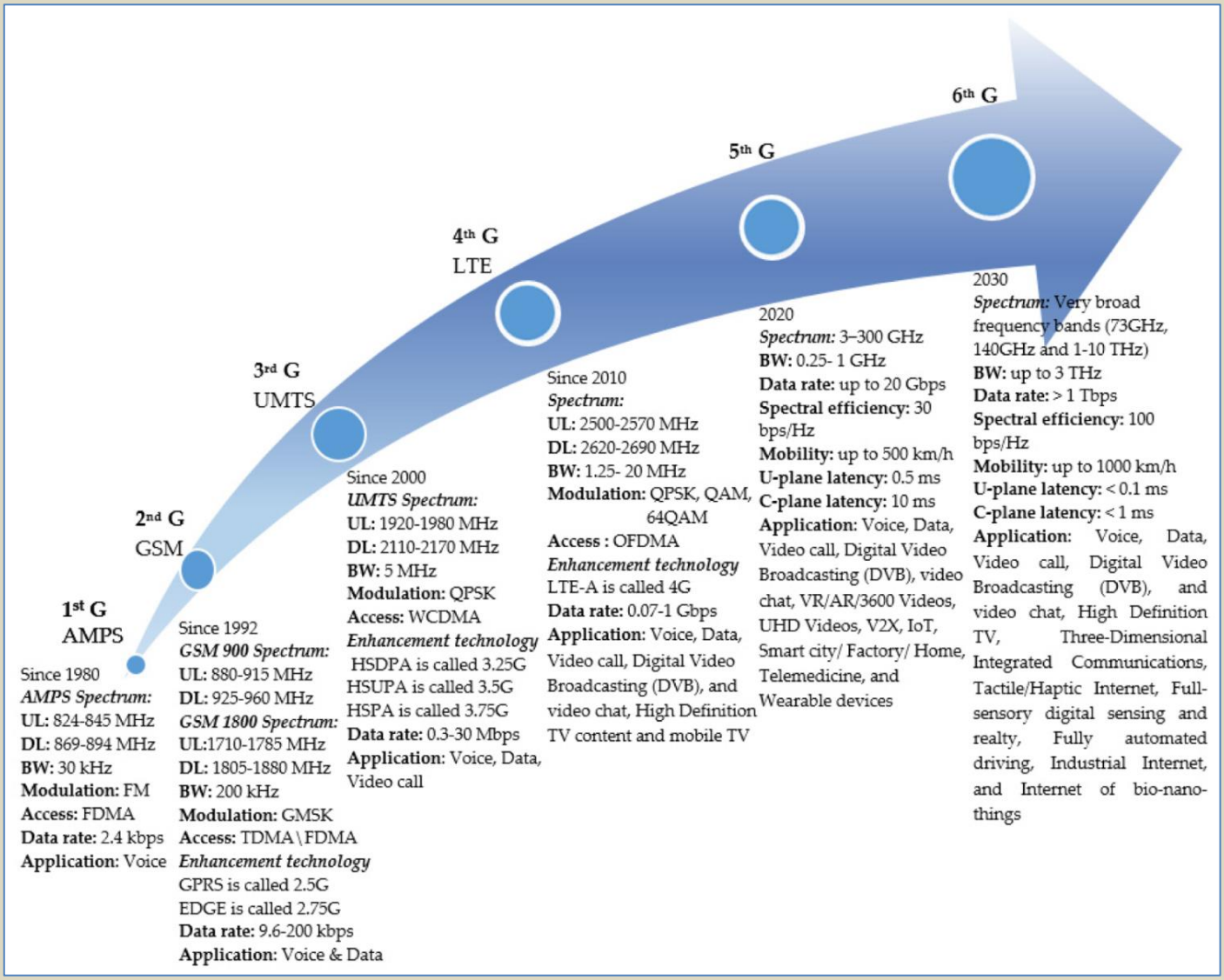
CYBER NEWS

Towards 6G Wireless Communication Networks: Vision, Enabling Technologies and New Paradigm Shifts

Source: https://www.eurasiareview.com/30112020-towards-6g-wireless-communication-networks-vision-enabling-technologies-and-new-paradigm-shifts/

Nov 30 – The fifth generation (5G) wireless communication networks are being deployed worldwide from 2020 and more capabilities are in the process of being standardized, such as mass connectivity, ultra-reliability, and guaranteed low latency.

However, 5G will not meet all requirements of the future in 2030 and beyond, and sixth generation (6G) wireless communication networks are expected to provide global coverage, enhanced spectral/energy/cost efficiency, better intelligence level and security, etc.



To meet these requirements, 6G networks will rely on new enabling technologies, i.e., air interface and transmission technologies and novel network architecture, such as waveform design, multiple access, channel coding schemes, multi-antenna technologies, network slicing, cell-free architecture, and cloud/fog/edge computing.

A long-form review, titled "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts", was published in *SCIENCE CHINA Information Sciences* (Vol. 64, No.1). It is co-authored by Prof. Xiaohu YOU (first and corresponding author) and Prof. Chengxiang WANG (corresponding author) from Southeast University, China, along with other 48 experts and scholars from scientific research institutes, colleges, and companies both at home and abroad.

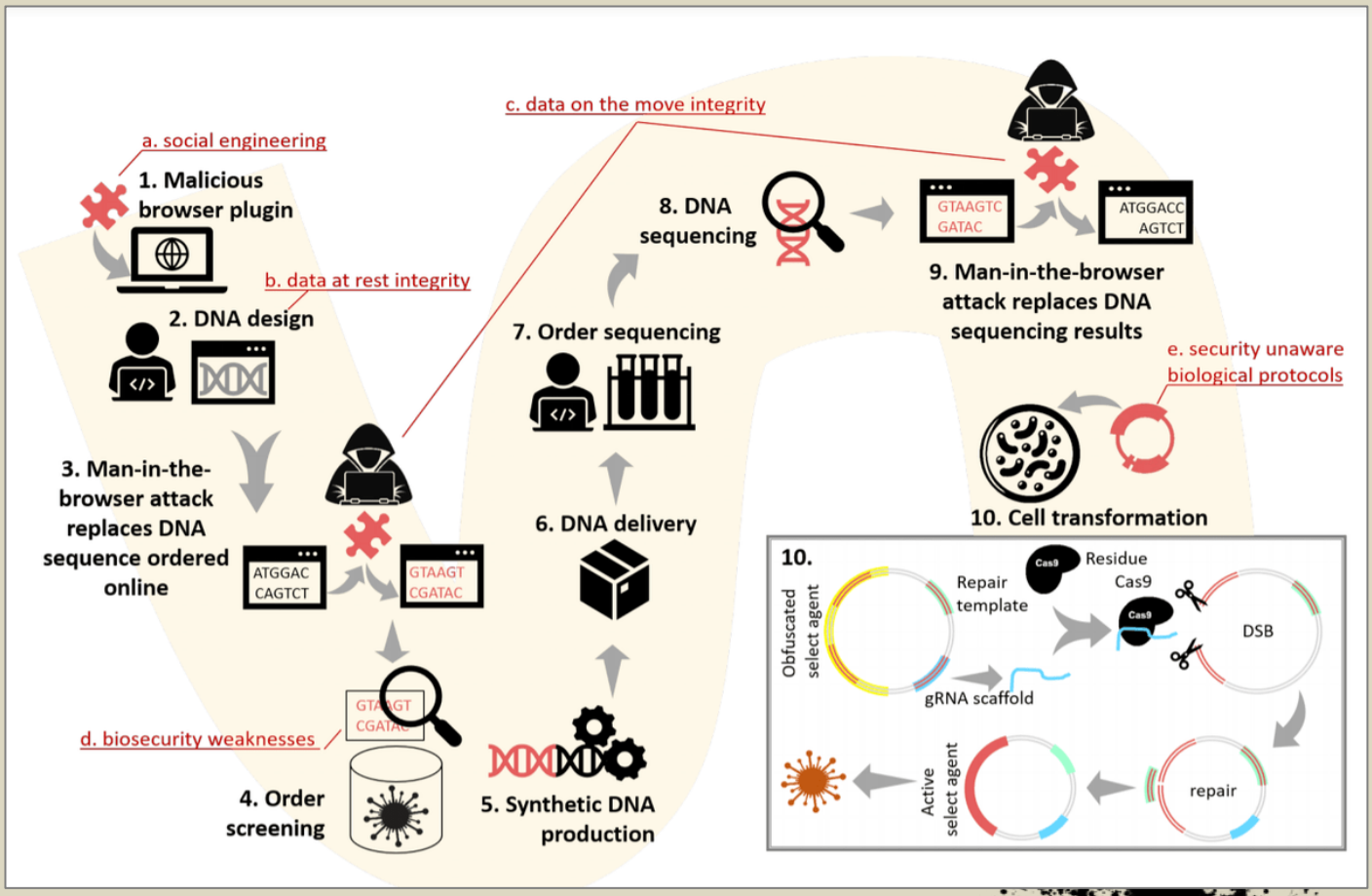
In this article, the vision on 6G is that it will have four new paradigm shifts. First, to satisfy the requirement of global coverage, 6G will not be limited to terrestrial communication networks, which will need to be complemented with non-terrestrial networks such as satellite and unmanned aerial vehicle (UAV) communication networks, thus achieving a space-airground-sea integrated communication network.
Second, all spectra will be fully explored to further increase data rates and connection density, including the sub-6 GHz, millimeter wave (mmWave), terahertz (THz), and optical frequency bands.
Third, facing the big datasets generated by the use of extremely heterogeneous networks, diverse communication scenarios, large numbers of antennas, wide bandwidths, and new service requirements, 6G networks will enable a new range of smart applications with the aid of artificial intelligence (AI) and big data technologies.
Fourth, network security will have to be strengthened when developing 6G networks.
This article provides a comprehensive survey of recent advances and future trends in these four aspects. Clearly, 6G with additional technical requirements beyond those of 5G will enable faster and further communications to the extent that the boundary between physical and cyber worlds disappears.

New Cyberattack Tricks Scientists into Making Dangerous Toxins, Synthetic Viruses

Source: http://www.homelandsecuritynewswire.com/dr20201201-new-cyberattack-tricks-scientists-into-making-dangerous-toxins-synthetic-viruses

Dec 01 – An end-to-end cyber-biological attack, in which unwitting biologists may be tricked into generating dangerous toxins in their labs, has been discovered by Ben-Gurion University of the Negev cyber-researchers.

According to a new paper just published in *Nature Biotechnology*, it is currently believed that a criminal needs to have physical contact with a dangerous substance to produce and deliver it. However, malware could easily replace a short sub-string of the DNA on a bioengineer's computer so that they unintentionally create a toxin producing sequence.



"To regulate both intentional and unintentional generation of dangerous substances, most synthetic gene providers screen DNA orders which is currently the most effective line of defense against such attacks," says Rami Puzis, head of the BGU Complex Networks Analysis Lab, a member of the Department of Software and Information Systems Engineering and Cyber@BGU. California was the first state in 2020 to introduce gene purchase regulation legislation.
"However, outside the state, bioterrorists can buy dangerous DNA, from companies that do not screen the orders," Puzis says. "Unfortunately, the screening guidelines have not been adapted to reflect recent developments in synthetic biology and cyberwarfare."
A weakness in the U.S. Department of Health and Human Services (HHS) guidance for DNA providers allows screening protocols to be circumvented using a generic obfuscation procedure which makes it difficult for the screening software to detect the toxin producing DNA. "Using this technique, our experiments revealed that that 16 out of 50 obfuscated DNA samples were not detected when screened according to the *'best-match'* HHS guidelines," Puzis says.
The researchers also found that accessibility and automation of the synthetic gene engineering workflow, combined with insufficient cybersecurity controls, allow malware to interfere with biological processes within the victim's lab, closing the loop with the possibility of an exploit written into a DNA molecule.
The DNA injection attack demonstrates a significant new threat of malicious code altering biological processes. Although simpler attacks that may harm biological experiments exist, we've chosen to demonstrate a scenario that makes use of multiple weaknesses at three levels of the bioengineering workflow: software, biosecurity screening, and biological protocols. This scenario highlights the opportunities for applying cybersecurity know-how in new contexts such as biosecurity and gene coding.
"This attack scenario underscores the need to harden the synthetic DNA supply chain with protections against cyber-biological threats," Puzis says. "To address these threats, we propose an improved screening algorithm that takes into account in vivo gene editing. We hope this paper sets the stage for robust, adversary resilient DNA sequence screening and cybersecurity-hardened synthetic gene production services when biosecurity screening will be enforced by local regulations worldwide."

IBM Detects Hacking Ploy to Target COVID Vaccine Supply

Source: http://www.homelandsecuritynewswire.com/dr20201204-ibm-detects-hacking-ploy-to-target-covid-vaccine-supply

Dec 04 – Experts from the US tech firm IBM on Thursday said they had detected a cyberespionage operation to target vital information on a World Health Organization (WHO) initiative for distributing the COVID-19 vaccine.
The cybersecurity researchers said they were not sure who was behind the effort, which began in September. They were also unable to say if it had been successful.
IBM said the precision targeting and techniques used by the hackers to cover their tracks bore "the potential hallmarks of nation-state tradecraft."
The hackers had gone through "an exceptional amount of effort," said IBM analyst Claire Zaboeva, who helped draft the report.
The online intruders had meticulously constructed booby-trapped emails sent in the name of an executive with Haier Biomedical, a Chinese firm that specializes in vaccine transport and biological sample storage.
The hackers had researched the correct make, model, and price of various refrigeration units to make the messages seem authentic, Zaboeva said.
"Whoever put together this campaign was intimately aware of whatever products were involved in the supply chain to deliver a vaccine for a global pandemic," she said.
IBM said the hackers had sent the bogus Haier emails to about 10 different organizations, although it only identified one target by name —the **European Commission's Directorate-General for Taxation and Customs Union**. The body handles tax and customs issues across the EU and has helped set rules on the import of vaccines.

The campaign's other targets were in countries including Germany, Italy, South Korea, and Taiwan. They appeared to be associated with the development of the "cold chain" needed to ensure coronavirus vaccines get the nonstop sterile refrigeration they need to be effective. The targets included companies involved in the manufacture of solar panels, used to power vaccine refrigerators in warm countries, and petrochemical products that are used to derive dry ice.

Hackers threaten to disrupt COVID-19 vaccine supply chain

Source: https://thehill.com/policy/cybersecurity/528852-hackers-threaten-to-disrupt-covid-19-vaccine-supply-chain

Dec 06 – Government officials and health-care groups are growing increasingly concerned about nation states and criminal hackers targeting the supply chain for COVID-19 vaccines.

Concerns have been amplified as the U.S. prepares to roll out the first vaccines later this month, with groups involved in creating and shipping the vaccines a prime target for potential cyberattacks.

"We have noticed an uptick in attacks against all aspects of the vaccine supply-chain from research through to manufacturing and distribution," Marc Rogers, the executive director of cybersecurity at software group Okta, told The Hill on Friday.

Rogers, who helps lead the COVID-19 CTI League that tracks and helps defend against cyberattacks aimed at health groups, noted that the League has seen "ramped up" cyberattacks aimed at medical institutions corresponding to increasingly positive news around vaccine development.

"My suspicion is that all parties in the cybercriminal underground from ordinary criminals to nation states recognize that the vaccines represent a golden opportunity and are responding as such," Rogers said.

North Korea has been among such nations, with The Wall Street Journal reporting recently that North Korean hackers targeted at least six pharmaceutical groups in the U.S., the United Kingdom and South Korea involved in developing a vaccine, including Johnson & Johnson and Novavax.

"All CISOs [chief information security officers] in health care are seeing attempted penetrations by nation state actors, not just North Korea, every single minute of every single day," Johnson & Johnson CISO Marene Allison said at the Aspen Institute's virtual Cyber Summit earlier this week.

A spokesperson for Novavax told The Hill in a statement Friday that the company was "aware of ongoing foreign threats identified in the news."

"We are confident we can continue to progress with our COVID-19 vaccine candidate without disruption and that these incursions do not pose a risk to the integrity of our data," the spokesperson said.

But as concerns have grown in recent weeks around the process to store, ship and deliver COVID-19 vaccines once they are approved, hackers are increasingly eyeing non-health care groups in the vaccine supply chain as potential targets.

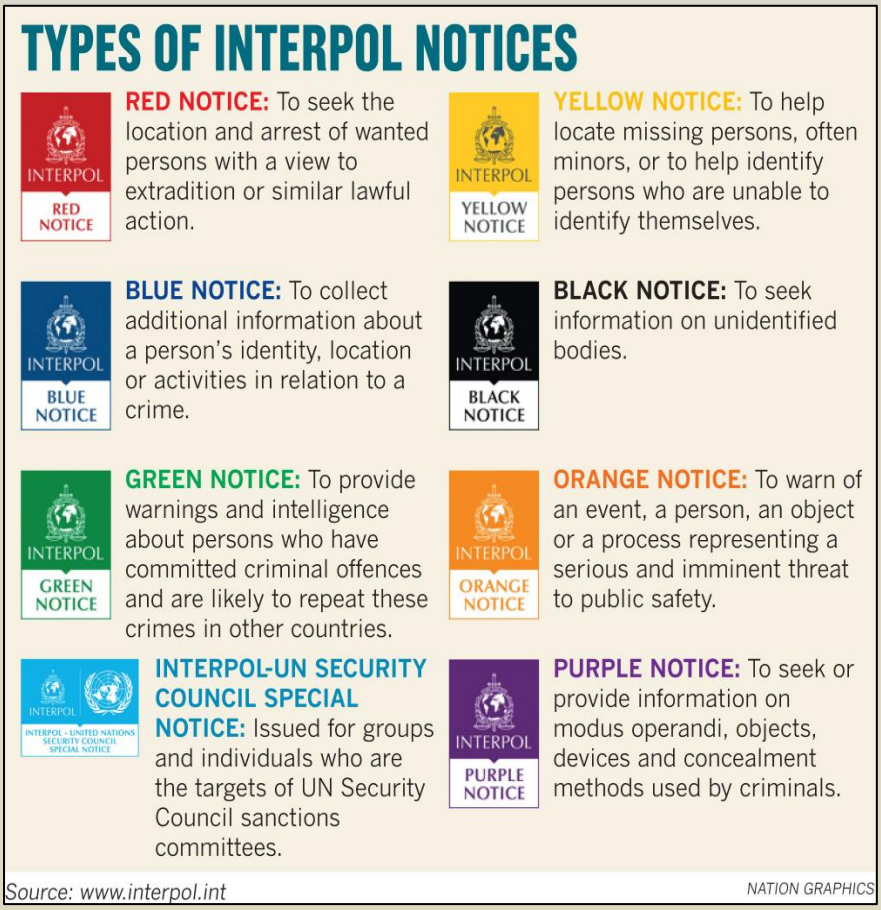
Cold storage groups — which are necessary for shipping and storing COVID-19 vaccine candidates at extremely low temperatures, such as one recently rolled out by Pfizer — have been increasingly in the crosshairs.

A report last week from IBM warned of a "global phishing campaign" targeting groups associated with cold storage for the COVID-19 vaccine process. Researchers wrote that "the precision targeting of executives and key global organizations hold the potential hallmarks of nation-state tradecraft."
The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) put out a corresponding alert encouraging U.S. organizations involved in the Operation Warp Speed vaccine distribution effort to review IBM's findings.
At least one major cold storage group had already been targeted before those alerts were issued.
Americold, the largest cold-storage provider in the U.S. and a global operator of cold storage warehouses, disclosed to the Securities and Exchange Commission (SEC) in November that it had discovered that its networks had been hit by a cyberattack.
"The Company took immediate steps to help contain the incident and implemented business continuity plans, where appropriate, to continue ongoing operations," the company wrote in the filing. "The Company has notified and is working closely with law enforcement, cybersecurity experts and legal counsel."
André Pienaar, founder of the firm C5 Capital, which helped form a group of around 40 major cybersecurity companies known as the Cyber Alliance to Defend Our Healthcare, pointed to the attack on Americold as an example of a weak link in the vaccine supply chain.
"The point of attack in the supply chain that the hackers targeted have been the cold storage facilities," Pienaar told The Hill. "Cold storage companies are dismally underinvested in cybersecurity and the hackers can enter their systems by hacking the industrial controls rather than phishing emails."
Cold storage groups are not the only organizations related to COVID-19 vaccines and treatments that have been targeted.
Meredith Harper, CISO of pharmaceutical group Eli Lilly, which has worked to develop a COVID-19 antibody drug, said at the Aspen Institute summit that her company had seen a major spike in attacks on third-party groups associated with carrying out Eli Lilly's work.
"Probably this year we have done way more incidents around our third parties than we've seen in the last few years," Harper said.
Government officials say they are aware of the threats to the vaccine supply chain and are working to address them.
Acting CISA Director Brandon Wales said that his agency is working with the National Security Agency and the FBI to ensure that the Operation Warp Speed vaccine supply chain process remains secure. He noted that foreign nations had targeted COVID-19 vaccine research and development initiatives since the start of the pandemic.
"There is more that we need to do to push deeper and further into these supply chains, not just the big companies behind the vaccine, but the companies that are going to be essential to get this vaccine from manufacturing through distribution, that last mile to the American people," Wales said at the Aspen Institute summit last week.
Pienaar said that beyond the vaccine supply chain, his group has also tracked threats to patient data collection associated with immunization.
"Effective immunization programs depend on accurate data collection systems and software," Pienaar said. "Our threat intelligence is that this will be the next attack vector for hackers."
Rogers noted that while the impending COVID-19 vaccine approval and rollout is good news for public health, the threat of cyberattacks interrupting the process remains high.
"We may be nearing what looks like the finish line, but now is not the time for us to take the eye off the ball," Rogers said. "We need to double down on vigilance and ensure that key entities in the distribution of these much-needed vaccines are watched and guarded 24x7."

INTERPOL Issues Global Alert on Organized Crime Threat to COVID-19 Vaccines

Source: https://www.hstoday.us/subject-matter-areas/transportation/interpol-issues-global-alert-on-organized-crime-threat-to-covid-19-vaccines/

Dec 05 – INTERPOL has issued a global alert to law enforcement across its 194 member countries warning them to prepare for organized crime networks targeting COVID-19 vaccines, both physically and online.
The **INTERPOL Orange Notice** outlines potential criminal activity in relation to the falsification, theft and illegal advertising of COVID-19 and flu vaccines, with the pandemic having already triggered unprecedented opportunistic and predatory criminal behavior. It also includes examples of crimes where individuals have been advertising, selling and administering fake vaccines.
As a number of COVID-19 vaccines come closer to approval and global distribution, ensuring the safety of the supply chain and identifying illicit websites selling fake products will be essential.



The need for coordination between law enforcement and health regulatory bodies will also play a vital role to ensure the safety of individuals and wellbeing of communities are protected.

"Criminal networks will also be targeting unsuspecting members of the public via fake websites and false cures, which could pose a significant risk to their health, even their lives.

"It is essential that law enforcement is as prepared as possible for what will be an onslaught of all types of criminal activity linked to the COVID-19 vaccine, which is why INTERPOL has issued this global warning," concluded Secretary General Stock.

The Orange Notice follows INTERPOL's updated guidance last month concerning organized crime groups' threat to COVID-19 vaccines, and comes as IBM uncovered a global phishing campaign targeting the vaccine's cold supply chain.

As well as targeting COVID-19 vaccines, as international travel gradually resumes it is likely that testing for the virus will become of greater importance, resulting in a parallel production and distribution of unauthorized and falsified testing kits.

With an increasing number of COVID-related frauds, INTERPOL is also advising members of the public to take special care when going online to search for medical equipment or medicines.

In addition to the dangers of ordering potentially life-threatening products, an analysis by INTERPOL's Cybercrime Unit revealed that of 3,000 websites associated with online pharmacies suspected of selling illicit medicines and medical devices, around 1,700 contained cyber threats, especially phishing and spamming malware.

Always check with national health authorities or the World Health Organization for the latest health advice in relation to COVID-19.

A firm that helps protect businesses and cities from cyberattacks just got hit by one

Source: https://edition.cnn.com/2020/12/08/tech/fireeye-cyberattack/index.html

Dec 08 – The cybersecurity firm FireEye (FEYE) said Tuesday that it had come under cyberattack by "highly sophisticated" actors likely sponsored by a nation-state, in a rare and extremely serious instance of a mainstream security vendor being compromised. The hack could even give the perpetrators the means to launch attacks against other targets.

In an investor disclosure, FireEye said the attack was highly customized to target FireEye's systems and is unlike any the company has responded to in the past.

"Based on his 25 years in cyber security and responding to incidents, Kevin Mandia, our Chief Executive Officer, concluded we are witnessing an attack by a nation with top-tier offensive capabilities," the SEC filing said.

The attacker accessed "certain Red Team assessment tools that we use to test our customers' security," the disclosure continued, implying that many of FireEye's clients, including its government customers, could be indirectly affected by the breach. "We are proactively releasing methods and means to detect the use of our stolen Red Team tools. We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we

have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools."
In a blog post, Mandia said FireEye is working with the FBI and other forensic partners, including Microsoft (MSFT). Matt Gorham, assistant director of the FBI's Cyber Division, said in a statement that "preliminary indications show an actor with a high level of sophistication consistent with a nation state."
Mandia said the attackers tried to access information "related to certain government customers," but that the company has no evidence yet that customer information has been stolen.
None of the stolen cybersecurity tools contained so-called zero-day exploits, Mandia said. Zero-day vulnerabilities are software vulnerabilities that have never been publicly identified or patched, and can be extremely dangerous if weaponized by malicious actors.
The Cybersecurity and Infrastructure Security Agency, an arm of the Department of Homeland Security, said in a statement that it has been working with FireEye to determine the scope of the attack.
"As details are made available, we are working to share and implement countermeasures across the federal networks and with our private sector partners," a CISA spokesperson said.
FireEye is among the world's preeminent cybersecurity firms, selling services designed to prevent, detect and respond to network security attacks. It also conducts extensive research on some of the most sophisticated hacking groups, known in the industry as advanced persistent threats.
Mike Chapple, a cybersecurity expert at the University of Notre Dame and a former National Security Agency official, called the FireEye breach "an extraordinarily significant attack."
"As one of the world's go-to cybersecurity firms, FireEye has a ringside seat for some of the most sophisticated breaches carried out worldwide," Chapple said. "The impact of this breach remains to be seen and depends upon the motivation of the attackers. We might see them go public in an attempt to monetize their work by selling exploits. On the other hand, they might remain in the shadows, stealthily using their new tools to compromise high-value systems."
Shares of FireEye fell more than 7% in after-hours trading Tuesday following the disclosure.

Hackers accessed vaccine documents in cyber-attack on EMA

Source: https://www.theguardian.com/world/2020/dec/09/hackers-accessed-vaccine-documents-in-cyber-attack-on-ema

Dec 09 – German biotech firm BioNTech said on Wednesday that documents relating to the Covid-19 vaccine it has developed with Pfizer were "unlawfully accessed" after a cyber-attack on Europe's medicines regulator.
Earlier, the European Medicines Agency (EMA) – which is responsible for assessing and approving vaccines for the European Union – said it had been targeted in a cyber-attack. It gave no further details.
It was not immediately clear when or how the attack took place, who was responsible or what other information may have been compromised.
Britain's National Cyber Security Centre said it was studying the situation and its impact on the UK, the first country where the Pfizer/BioNTech vaccine has been deployed.
An NCSC spokesperson added: "We are working with international partners to understand the impact of this incident affecting the EU's medicine regulator, but there is currently no evidence to suggest that the UK's medicine regulator has been affected."
The EMA was previously headquartered in London but moved its HQ to Amsterdam in 2019 following the Brexit vote.
Following the disclosure, BioNTech said the EMA had informed it that "that the agency has been subject to a cyber-attack and that some documents relating to the regulatory submission for Pfizer and BioNTech's Covid-19 vaccine candidate … had been unlawfully accessed".
But, it added, "No BioNTech or Pfizer systems have been breached in connection with this incident and we are unaware of any personal data of study participants being accessed."
The EMA gave no further details about the attack, saying only that it was investigating the incident with help from law enforcement. "EMA cannot provide additional details whilst the investigation is ongoing. Further information will be made available in due course," it said in a statement.
Hacking attempts against healthcare and medical organisations have intensified during the pandemic as attackers ranging from state-backed spies to cybercriminals scramble to obtain the latest information about the outbreak.
On separate occasions, hackers linked to China, Iran, North Korea, Russia and Vietnam have been accused of trying to steal information about the virus and its potential treatments.

Cyber Threats – What to Expect in 2021?

Source: https://i-hls.com/archives/105755

Dec 19 – 2020 has been a challenging year from the point of view of cybersecurity, with many organizations reacting to the unexpected impact of the COVID-19 pandemic. Existing threats have continued to evolve while, on the other hand, innovation may bring about better tools to fight cybercrime.

Here are several cyber threat predictions for 2021.

- Remote working needs to be secured – Few organizations were prepared to manage a remote workforce securely, and as they scrambled to set up secure communication channels, cybercriminals uncovered a multitude of fresh attack vectors. While many companies will be planning to invest in securing the remote workforce, there's a risk that they are underestimating the scale and challenge of the task ahead.
- Mobile attacks will proliferate – A steep rise in scams coming through mobile devices is expected. Sophisticated fraud attempts are expected via SMS and WhatsApp, with attackers leveraging devious social engineering techniques to manipulate people into paying money or sharing sensitive data.
- Ransomware will get worse – According to forbes.com, we should expect cybercriminals to be more ruthless in the pursuit of ransom payments, threatening to expose stolen credentials to the public and setting up online stores to sell data. They will also leverage data exfiltration and use stolen employee passwords to force targets into paying up.

- The promise of multi-factor authentication (MFA) may be creating a false sense of security for some organizations, and hackers are set to shatter it in 2021. Once a cybercriminal understands which MFA system you're using, they can fine-tune their attack strategy and sometimes even use your reliance upon it to bypass your defenses.
- As IT systems increasingly converge with operational technology (OT) systems, particularly critical infrastructure, there will be even more data, devices, and unfortunately, lives at risk. Industrial control systems (ICS) will be attacked more, and critical infrastructures will be threatened. Aging and underfunded systems can harbor potential exploits that politically-motivated hacktivists and criminals are certain to find.
- Social engineering tactics and phishing attacks – Health and testing information, government assistance and home working all proved to be fertile ground for phishing attacks. Leveraging important contextual information about users including daily routines, habits, or financial information could make social engineering-based attacks more successful.
- The Internet of Things (IoT) – Over the past few years, the traditional network perimeter has been replaced with multiple edge environments, WAN, multi-cloud, data center, remote worker, IoT, and more, each with its unique risks. One of the most significant advantages to cybercriminals in all of this is that while all of these edges are interconnected many organizations have sacrificed centralized visibility

and unified control in favor of performance and digital transformation, as evaluated by fortinet.com. As a result, cyber adversaries are looking to evolve their attacks by targeting these environments. Expect more use of edge-access trojans and the exploitation of the speed and scale possibilities 5G will enable for advanced swarm-based attacks. These attacks leverage hijacked devices divided into subgroups, each with specialized skills. They target networks or devices as an integrated system and share intelligence in real-time to refine their attack as it is happening.

- Innovation in computing performance as a target – Processing power is important if cybercriminals want to scale future attacks with ML and AI capabilities. Eventually, by compromising edge devices for their processing power, cybercriminals would be able to process massive amounts of data and learn more about how and when edge devices are used.

Collaboration is the new task, asserts fortinet.com. Organizations cannot be expected to defend against cyber adversaries on their own. They will need to know who to inform in the case of an attack so that the "fingerprints" can be properly shared and law enforcement can do its work. Cybersecurity vendors, threat research organizations, and other industry groups need to partner with each other for information sharing, but also with law enforcement to help dismantle adversarial infrastructures to prevent future attacks.

Should Extremist Content Be Taken Down or Should We Talk About It?

By Meira Svirsky (Editor of ClarioProject)
Source: https://clarionproject.org/extremist-content-new-eu-law/

Dec 20 – A recent agreement drafted for the European Union (EU) mandates that social media companies must take down terrorist content within an hour of it being flagged or risk paying enormous fines.

On the face of it, we may automatically agree that this is a good idea considering the fact that propaganda is actually dangerous due to its proven ability to influence people and sway their opinions.

Most of us would also naturally assume that the new rule will apply to ISIS videos, neo-Nazi content and the like.

But will it apply to the Palestinian Authority (PA), which churns out terrorist content on its state-run media channels non-stop for young and old? Or will the PA be given an exemption considering the fact that between 2017 and 2020, the EU's baseline amount of funding for the PA was $1.57 billion?

Will the law apply to Iran, the largest state sponsor of terrorism, and the genocidal content that regularly comes out of its leaders' mouths? Or will the EU merely condemn such sentiments but look the other way on its social media platforms due to its financial investment of billions of euros in the Islamic Republic in the years since the nuclear deal was signed?

Will it apply to Hezbollah, a terrorist organization that most countries in the EU can't even bring themselves to ban completely, possibly due to the fact that it is an Iranian proxy?

Will it apply to Turkey's increasingly authoritarian Islamist leader Recep Tayyip Erdogan, who gives cover and funds to Hamas, slaughters Kurds in Syria and incites religious radicalism to the point of worldwide terror? Or does that also fall under "complicated" territory considering Erdogan's stranglehold on the EU vis-à-vis the immigration/refugee crisis?

Judging from the EU's tepid response to the assassination of Iranian terror leader Qassem Soleimani followed by its full-out condemnation of the killing of Mohsen Fakhrizadeh, head of Iran's covert nuclear weapons program, as a "criminal act – not to mention its failure to condemn Erdogan – we already know the answers to these questions.

So a very real question to ask when the dust settles is: Who defines "terrorist content"?

The relative standards of what constitutes terrorist content in our increasingly transactional world not only serves to call out the hypocrisy of this new EU mandate but represents a slippery slope to the rights of free speech everywhere, including stateside.

While Europeans have never enjoyed the freedoms of speech, expression or religion that form the bedrock of the U.S. constitution, a debate over these freedoms are raging in the public sphere in America as well.

Only in our increasingly woke America, where words are now perceived as "violence" (to the degree that students in colleges around the country need "safe spaces" from them), the term "terrorist content" has been largely replaced by "hateful content."

This, in turn, has prompted ersatz purveyors of American culture to demand that tech companies take down "hateful content" from their platforms.

Take former basketball legend turned cultural commentator Kareem Abdul-Jabbar. Speaking without the least hint of irony (he says he's been commenting about culture and politics for the last 30 years), Abdul-Jabbar wants tech companies to take down content he finds objectionable from celebrities. That content includes everything from conservative ideas to commentary about election fraud to information questioning the safety of the rapidly rolled out and experimental coronavirus vaccine.

"It would be tempting to dismiss this self-mutilation as merely the triggering of overly sensitive 'cancel culture,'" he says about celebrities like J.K. Rowling who go against the current Leftist groupthink. "But some of this public braying does immediate harm to the foundation of society."

(Rowling had the temerity to tweet about biological sex being important.)

Ultimately, Abdul-Jabar and many others like him would like to see celebrities like Rowling canceled altogether, so that "their professional legacies could become brief footnotes to the memory of their collection of mason jars filled with their excreted opinions."

There was a time when cultural purveyors such as Abdul-Jabbar would have been ostracized themselves as extremists due to the centrality of free speech in the American system of liberty, but now they are positioned sturdily in the mainstream.

Take Richard Stengel, President-elect Joe Biden's transition team leader for U.S.-owned media outlets. Writing in *The Washington Post* just last year, Stengel argued for making hate speech a crime.

Stengel gets around the sticky issue of freedom of speech as guaranteed by the U.S. Constitution by presuming to get into the heads of the country's framers.

"… the intellectual underpinning of the First Amendment was engineered for a simpler era," he contends. "The amendment rests on the notion that the truth will win out in what Supreme Court Justice William O. Douglas called 'the marketplace of ideas' … [yet] no one ever quite explained how good ideas drive out bad ones, how truth triumphs over falsehood … [how] truth would prevail in a 'free and open encounter.'"

Ignoring the obvious answer that the country is made up of citizens who are able to think for themselves, Stengel goes on to denigrate the framers' belief that the free exchange of ideas is "necessary for people to make informed choices in a democracy."

Somehow, he says, even if that "magically" happened in the past, Stengel says it isn't possible today: "On the Web, it's not enough to battle falsehood with truth; the truth doesn't always win. In the age of social media, the marketplace model doesn't work."

Stengel then opines that banning hate speech was really the *intent* of the framers:

"Hate speech has a less violent, but nearly as damaging, impact in another way: It diminishes tolerance. It enables discrimination … Isn't that, by definition, speech that undermines the values that the First Amendment was designed to protect: fairness, due process, equality before the law?

"Why shouldn't the states experiment with their own version of hate speech statutes to penalize speech that deliberately insults people based on religion, race, ethnicity and sexual orientation?" he asks.

The ideas of Stengel, Abdul-Jabar and other would-be censors and purveyors of "truth" represent a serious slide into a rabbit hole that historically has been tried and never ended well.

Whether it begins with the hypocrisy of the EU banning "terror content" on social media platforms, the condescending attitude of Stengel toward everyday Americans or the nanny state being proposed by Abdul-Jabar, the endpoint of that route is always totalitarianism.

It's a sticky issue. Yes, ISIS videos and neo-Nazi propaganda can and should be taken down, but let's not kid ourselves into thinking that criminalizing hate speech is a good idea instead of what it really is: a euphemism for silencing our political opponents. Better we should talk "hate" and let truth prevail.

How A Cybersecurity Firm Uncovered the Massive Computer Hack

By Greg Myre and Laurel Wamsley

Source: https://www.npr.org/2020/12/21/948843356/how-a-cybersecurity-firm-uncovered-the-massive-computer-hack

Dec 21 – The first word that hackers had carried out a highly sophisticated intrusion into U.S. computer networks came on Dec. 8, when the cybersecurity firm FireEye announced it had been breached and some of its most valuable tools had been stolen.

"We escalated very quickly from the moment I got the first briefing that, 'Hey, we have a security incident of some magnitude,' " FireEye CEO Kevin Mandia told *All Things Considered* co-host Mary Louise Kelly. "My gut was telling me it was something we needed to put people on right away."

Mandia was right. Within days, the scope of the hack began to emerge.

Multiple U.S. agencies were successfully targeted, including the departments of State, Treasury, Commerce, Energy and Homeland Security as well as the National Institutes of Health.

The hackers attached their malware to a software update from Austin, Texas-based company SolarWinds, which makes software used by many federal agencies and thousands of private companies to monitor their computer networks.

The SVR, Russia's foreign intelligence agency, is considered the most likely culprit, according to Secretary of State Mike Pompeo and some members of Congress who have been briefed by the U.S. intelligence community. But the Trump administration has not formally attributed blame.

"What I've seen is 2020 has been about the hardest year, period, to be an information security officer," Mandia said. "It's time this nation comes up with some doctrine on what we expect nations' rules of engagement to be, and what will our policy, or proportional response, be to folks who violate that doctrine. Because right now there's absolutely an escalation in cyberspace."

Here are excerpts from Mandia's interview:

What was that moment like when you're figuring out it's your cybersecurity company that has been hacked?

If you wrote down the reasons why another nation might want to compromise FireEye, you can come up with some reasons. What we do is we track attackers and quite frankly, we out them. We try to figure out — here's their fingerprints, let's share those fingerprints with everybody so they can't get away with what they're doing.

[Early on] there was enough operational security by the attacker that I knew it was professional. This wasn't the first rodeo for these attackers. In fact, they followed a tradecraft that the more I learned, the more this was a unit that's been operational for a decade or more. They knew what they were doing, they had novel techniques. So we knew we would have to do the full-court press on our investigation. And we did.

Who is behind this attack?

For me, it's definitely a nation. In regards to the supply chain compromise at SolarWinds, they did an innocuous addition of code in October 2019 inside the supply chain, saw that it was provisioned and deployed — so they knew that their techniques on offense to hack the supply chain were efficient and effective. They went live with actual malicious code inside of the SolarWinds in March through June of this year.

So this is somebody who is patient, professional, and what made this interesting to me is I felt they were more interested in staying surreptitious and clandestine than they were about accomplishing their mission.

What nations have this kind of capability?

Not a lot. It's very consistent with what Russia could do. There might be a group out of China that might be able to do it. And that's probably it.

Is there any signature to this attack that would be consistent with other hacks you've seen?

There's probably about six to eight technical details that made me realize this is a nation, and most likely a foreign intelligence service doing this breach. One of them is this: They used an infrastructure to attack FireEye. The IP addresses or systems they use to attack FireEye were not used in any other incident we're aware of.

In other words, the attackers set up an infrastructure to attack FireEye that was wholly unique to attacking FireEye. That takes a lot of maintenance. That takes a lot of coordination. That's an operation — not just a hack. Most threat groups, when they attack, will use shared infrastructure to attack many companies. This group does not do that. That in and of itself made me realize it was an operation.

What should we take from the fact that it was FireEye, a private cybersecurity firm, that alerted the U.S. government — and not the other way around?

We're all in this together, period. And there's different visibility at different places. When the attacks were happening against FireEye, all the IP addresses used to attack us [were] all

inside the United States. And I'm pretty aware that the [National Security Agency] does not do collections within the United States. So we were the ones, kind of on our own, to be able to see this and detect it.

So you're saying you were able to see things that the NSA, despite all of its vast resources, have firewalls against being able to see, domestically?

Well, I wouldn't call it firewalls necessarily. It's just legal remit. You know, when you look at what these attackers do, they're attacking U.S. companies from the United States. That doesn't necessarily mean the attackers are sitting in the United States — but the infrastructure they're setting up to attack companies like FireEye are all in the United States. So the malicious intent may not be visible outside the United States and may only be visible inside.

We have thousands and thousands of computers that we inspected for evidence that they were compromised, and we couldn't get anything earlier in the time frame than a SolarWinds system. We sat there looking at the SolarWinds system saying, "We can't find anything bad on it right now, but it's our earliest evidence of compromise. Something's wrong."

So we then had to turn it over to our reverse engineers. This is something most companies can't do. We went through 14 gig of information, over 18,000 files in the update that we got from SolarWinds, over 4,000 executable files. We decompiled them into millions of lines. And then with real malware analysts, we found the needle in the haystack.

Do we know whether the NSA itself was hacked?

I don't have any idea.

So what now? There's a statement from the FBI and the director of national intelligence and the cybersecurity arm of Homeland Security that says this breach is ongoing.

I think as folks are being notified or learning that they're compromised, they're going to have a lot of work to do. All these organizations are both going to have to investigate what happened and figure out the scale and scope of it, and then they're going to have to eradicate the attackers from their network if they're still active.

Even if they're not active, you're going to flex your muscle a little bit to do a lot of remediation. That's going to take months.

But one thing that's definitely clear to me: The attackers have no idea what is the envelope of behavior, what are the rules of engagement.

We're a nation losing billions of dollars to ransomware. And we are a nation that just had potentially one of the most successful cyberespionage campaigns ever done on it.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Feds Prosecute Drone Pilot for Mid-Air Collision (U.S. v Hernandez)

By Jonathan Rupprecht

Source: https://jrupprechtlaw.com/feds-prosecute-drone-pilot-for-mid-air-collision-u-s-v-hernandez/

On Wednesday, a federal complaint was filed in the Central Federal District Court of California charging Andrew Hernandez with unsafe operation of an unmanned aircraft.

It alleges that around 12:35 a.m. a Los Angeles Police Department helicopter arrived in response to a request for air support by officers investigating a burglary at a pharmacy.

While hovering, an Officer Lomax observed from the helicopter what appeared to be a "drone and pulled the helicopter up in an attempt to put the helicopter out of the drone's flight path. Despite Officer Lomax's efforts to avoid the drone, the drone struck the bottom of the LAPD helicopter."

The helicopter initiated an emergency landing by flying over to LAPD Hooper Heliport. After landing, Officer Lomax "observed damage to the helicopter's nose, antenna, and the bottom cowlings."

Officers interviewed a witness who lived near the pharmacy who indicated that the residents of a nearby house flew drones frequently. A pull of DMV records indicated the defendant lived at the house indicated by the witness.

Officers around the pharmacy located portions of the drone and found a serial number on one of the portions. A warrant was obtained to search the drone's camera and SD card. On it they found among other pictures a picture of the suspect holding a drone controller near the license plate on the vehicle registered to him.

A warrant was obtained to search the suspect's house. After Miranda warnings were given, the defendant told officers he heard a helicopter and "was curious, got his drone, and flew his drone to see what was going on. . . . He stated that it [was] hard to see the drone at night, but that he recalled seeing the drone's green light facing him as it was ascending." He looked down for a couple seconds at the drone controller and as he "looked up again at his drone, he saw the drone being 'smacked' by the helicopter, which was hovering."

The digital evidence led a trail back to the defendant. And before some drone pilot thinks this is unlikely to happen to them, consider 14 CFR 107.7(b) which says, the drone pilot "must, upon request, allow the [FAA] to make any test or inspection of the small unmanned aircraft system[.]"

18 USC Section 39B(a)(2) makes it a crime for any person who operates an unmanned aircraft and "Recklessly interferes with, or disrupts the operation of, an aircraft carrying 1 or more occupants operating in the special aircraft jurisdiction of the United States, in a manner that poses an imminent safety hazard to such occupants[.]" A violation shall be punished by a fine and/or imprisonment for not more than 1 year; however, if the person causes serious bodily injury or death during the commission of an offense, they can be fined and/or imprisoned for a term of up to 10 years.

The Department of Justice has been stepping up efforts in dealing with drones:

- This year the DOJ has announced filing charges against two drone pilots who flew their drones in flight restrictions in Oregon.
- The DOJ also announced they filed charges against a drone pilot in Miami who flew in flight restrictions during the Super Bowl.
- In April, 2020, the Attorney General put out some counter UAS guidance which requires authorized FBI personnel to be "properly trained on the use of the technology or equipment and on their responsibilities under this Guidance." The criminal complaint gives us more info regarding the FBI's counter UAS efforts because in the complaint it stated that the FBI special agent involved in this case has since July 2020 "been a member of the newly-formed FBI Wildland Fire Counter-Unmanned Aircraft System ("CUAS") Team, for which [he] received training specific to drones."

As I've told people multiple times, make sure you are flying lawfully all the time, even when people are not around, because your flight logs and pictures could cause you problems. Just look at the defendant in this case who had a selfie picture on the drone's SD card of him holding the drone controller and standing next to a vehicle registered to him.

I predict we will see more and more of these types of investigations happening where law enforcement will use pictures and flight logs to try and determine certain facts and who is the suspect.

The big take-away from this case is: any pictures you take, can and will be held against you.

▶▶ **The copy of the criminal complaint is located here.**

Jonathan Rupprecht, Esq. *brings his commercial pilot/flight instructor and legal experience to the table to help businesses and individuals implement their ideas in the rapidly growing and changing unmanned aircraft systems (UAS) industry. Jonathan went to Embry-Riddle Aeronautical University, graduating with a bachelor of science (*Magna cum Laude*). He later wrote a book on drone law which lead into him co-authoring an American Bar Association legal treatise on drone law with his focus on the history of unmanned aircraft, the FAA rulemaking process, and the proposed commercial drone regulations. Jonathan co-founded the Unmanned Systems Legal Association which aims to be the premier international association of lawyers focusing on drone law.*

Turkish firm develops AI-powered software for drone swarms

Source: https://www.c4isrnet.com/unmanned/2020/11/24/turkish-firm-develops-ai-powered-software-for-drone-swarms/

These Intel Shooting Star drones are for entertainment, but some countries are eager to adapt drone swarms for battle. (Joey Swafford/U.S. Air Force)

Nov 24 — A privately owned Turkish company says it has developed an artificial intelligence-based software for swarm drones.
MilSOFT announced Nov. 19 it developed the software after four years of research, and the the technology could be used in both fixed- and rotary-wing drone platforms.
A government aerospace official said swarm drones would be used in Turkey's future unmanned aerial combat concept due to their low hardware costs and stealth technology.
"These drones could be ideal in asymmetrical warfare. They are quick, cost-effective and easy to operate," the official said. "Most importantly, they are assets designed to minimize human loss in asymmetrical warfare."
The Turkish military has been operating a big fleet of tactical and armed drones primarily in combat against Kurdish militants in Turkey's southeast provinces but also in cross-border

operations in northern Syria and Iraq. Turkish drones have also been used in Libya's civil war and, most recently, in conflict between Armenia and Azerbaijan.
Many countries have yet to try drone swarm technology in a simulated, controlled environment. Turkey is among those that have the technology and the ability to test it in the field during operations.
Turkey's top procurement office, the Presidency for Defense Industries, launched its Swarm UAV Technology Development and Demonstration program with a view to develop algorithms and software for the use of unmanned platforms with a swarm capability. The program is also meant to involve micro-scale companies as well as small and medium-sized enterprises.
MilSOFT has specialized in software solutions since 1998, and it is one of the participants of the government-run program. It has been offering products to the Turkish military for tasks including identifying detection by automatic moving target technology using AI, and machine-learning techniques with image-processing algorithms.
The company said with the integration of intelligence and image evaluation products, drone swarms can be updated with additional capabilities such as reconnaissance, detection, recognition, search and rescue, and vehicle tracking.
MilSOFT's software-based solution will allow drone swarms to be launched from aerial, land and naval platforms, and the images they obtain will enter a central command system. In the meantime, the drone flocks will transfer images between different military units with a relay function.
AI technology can help catch elements that cannot be caught by the human eye and enable multiple attack capabilities by arming vehicles in operation.
MilSOFT's AI-based software is also expected to enable swarm drones to perform frontal attacks on command from helicopters and provide operational support to other friendly platforms. The drones can reportedly operate autonomously from the beginning to the end of a mission, and can be instantly monitored and controlled via intelligence applications.
The UAVs have a flight time of more than half an hour and a payload capacity of 1 kilogram (2.2 pounds). The vehicles work with landing gear that can land on rough terrain.
While five UAVs are currently used in a herd in the field, this number can reach up to 25 in a controlled environment. MilSOFT aims to make a drone swarm of 50 operational vehicles.
Communication between the drones is also provided by MilSOFT's own technology. Vehicles can communicate with each other from up to 500 meters. There is also a 10-kilometer network solution for data transfers.
MilSOFT plans to integrate its technology for underwater and surface platforms as well as land vehicles.

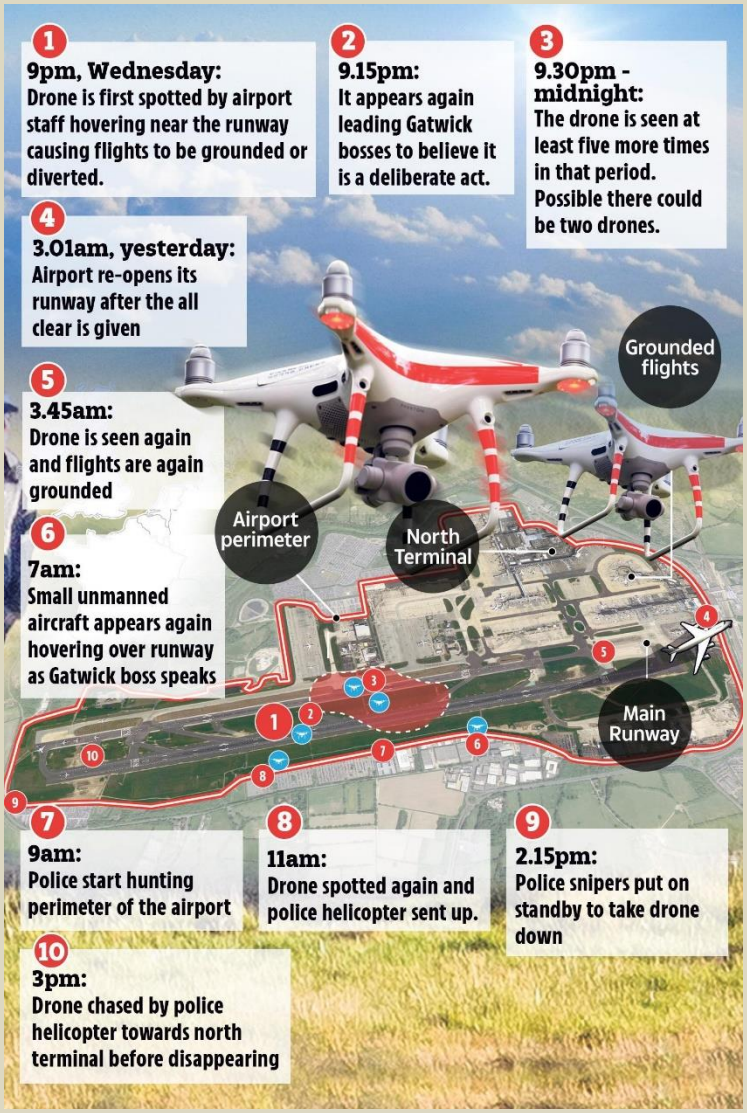
The mystery of the Gatwick drone

by Samira Shackle
Source: https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

Dec 01 - Soon after 9pm on Wednesday 19 December 2018, an airport security officer who had just finished his shift at Gatwick airport was standing at a bus stop on site, waiting to go home, when he saw something strange. He immediately called the Gatwick control centre and reported what he had seen: two drones. One was hovering above a vehicle inside the airport complex, and the other was flying alongside the nearby perimeter fence. The message was relayed to senior management. Unauthorised drone activity is considered a danger to aircraft and passengers because of the risk of collision. Within minutes, Gatwick's only runway had been closed and all flights were suspended.

Over the next half hour, 20 police and airport security vehicles drove around the airport, lights flashing and sirens blaring, with the intention of scaring whoever was operating the drones. It didn't work. By 9.30pm, six more sightings had been logged by the Gatwick control centre, five of them from police officers. Inside the airport, thousands of passengers waited to set off on their Christmas holidays. In the sky above, planes circled, waiting to land. Some were at the end of long journeys, and more than a dozen aircraft were soon dangerously low on fuel.
About an hour after the first sighting, Eddie Mitchell, a news photographer, was on his way to the airport to cover the shutdown when he remembered that he had two drones in his car. Fearing that he might come under suspicion, he rang the police: "I said: 'I'm heading to

Gatwick, please don't think it's me!'" Mitchell is licensed by the Civil Aviation Authority (CAA) to fly drones commercially, sometimes in his capacity as a cameraman, sometimes for official bodies such as the fire brigade. But he had good reason to be cautious. Four years earlier, in December 2014, he was trying to get aerial footage of a fire close to Gatwick when police arrested him. His drone was confiscated and he was held for five hours. (He later won compensation for wrongful arrest.)



By midnight, 58 flights had been diverted or cancelled. But there hadn't been any drone sightings for an hour, and Gatwick tried to reopen the runway. And then, suddenly, the drones reappeared. "We had the feeling that it was going to last all night," I was told by a former Gatwick employee who did not want to give her name. She was right: into the next day, every time staff prepared to reopen the runway, more sightings were reported. Staff and police speculated that the drone operator had gained access to the flight radar system, or was somehow listening into police or airport communications.

Some feared the drones were being operated by terrorists. "Drones can be transformed into flying suicide vests," said David Dunn, a drone expert at Birmingham University. In the previous two years, there had been multiple terror attacks around Europe, including the suicide bombing at the Manchester Arena 18 months earlier, which killed 22 people. It had been reported that Isis had used consumer drones to drop grenades in Iraq. After the failed attempt at reopening, Sussex police alerted the Metropolitan police's counter-terrorism unit. "We were under siege," the former employee told me. The drones seemed to be taunting them. "It started to feel like a national emergency."

By about 9.30 the following morning, Sussex police had called in officers from five other police forces to help with the search. A helicopter and several police drones went up to search for rogue drones – to no avail. At 10.20am, police told reporters that although this was a "deliberate act to disrupt the airport", there was "absolutely no indication to suggest this is terror-related". There was speculation that it could be an environmental protest, or even an "inside job" – sabotage by a disgruntled ex-employee. Whoever it was, the impact on Gatwick – Britain's second-biggest airport, with 46 million people passing through each year – was seismic. Later that day, Gatwick CEO Stewart Wingate said that the drone flights were "highly targeted" and had "been designed to close the airport and bring maximum disruption in the run up to Christmas".

Mitchell, the photographer, was observing all this. "It was panic stations," he told me. Although the atmosphere in the airport was frenetic, for the photographers – Mitchell remembers there being about 30 of them – it was a long and boring day. None of them caught sight of any drones, and Mitchell was beginning to doubt whether there was one.

At about 5pm, Mitchell was parked at the end of the runway with a colleague when something caught his eye: a red and green light, hovering in the distance. This was it. He reported the drone to police, before jumping out of the car to start snapping. "I thought, we've got it, and the idiot flying it," he said. "That was the money shot."

But when he opened up the image on his computer, ready to send to his editors, he realised he'd made a mistake. The image did not show a drone. It was a helicopter hovering 10 miles away; between the darkness and the distance, his eyes had played a trick on him. "If I'm making a mistake – and I fly drones two or three times a week – then God help us, because others will have no idea," he said. He called police to retract his reported sighting.

At 6pm, military trucks arrived at Gatwick with an anti-drone system designed for battlefield operation, and installed it on the roof of the south terminal. This system can track and disable drones; it works by jamming the radio frequency connecting the drone to its controller. At 9.30pm, Gatwick's chief operating officer Chris Woodroofe announced that the airport would remain closed overnight because of new drone sightings. The military system was operational by around 10pm. It did not pick up a single thing.

In the early hours of Friday 21 December, the runway reopened for the 10th time. At 5.58am, a plane from East Midlands airport landed at Gatwick. The drone incident was over.
The airport had been closed for 33 hours. More than 1,000 flights had been cancelled, and more than 140,000 passengers affected. "It showed the serious risk of drone intrusion, and how quickly that could bring an airport to its knees," said John Strickland, an aviation consultant. In total, 170 drone sightings were reported, 115 of which were later deemed "credible" by police. But neither Mitchell, nor any of the news crews camped out for two days, had managed to get a photo or video. Neither had any of the thousands of passengers and airport staff on site; no one who reported a sighting had captured an image on their phone.
The Gatwick incident was the first time a major airport was shut down by drones, and it distilled deep cultural anxieties – from the threat of terrorism and unconventional attacks by hostile states, to our fear of new technology. Two years later, it remains unsolved, despite a police operation that lasted 18 months, cost £800,000 and involved five different forces. Conspiracy theories abound online: people claim that the incident was a setup by companies selling counter-drone systems to market their products, that it was a coverup for a cyber-attack on the airport, or that it was staged to bring down the share price ahead of a Gatwick share sale (a week after the drone incident, a majority stake was sold to a French airport group).
Despite lack of evidence – or indeed any leads or convincing motives – Sussex police and Gatwick maintain it was a sophisticated, malicious and well-planned attack. On social media, meanwhile, the Gatwick drone has become a punchline, with many casting doubts on its very existence.
Richard Ryan knows more about drones than most – he is a barrister specialising in drone law at Blakiston's Chambers, as well as being a registered commercial drone operator. At the time of the Gatwick incident, he lived in Horley, just a mile away from the airport. When he heard the news, his first thought was: "It was only a matter of time." Despite his enthusiasm about the transformative possibilities of drones, he had long worried that someone might put them to sinister use.
A day or two after the airport reopened, Sussex police asked Ryan to come in for an interview. Ryan quickly established that they were not interested in his professional expertise: they wanted to ascertain whether he had been involved. "I told them that, upon consideration, I don't think it's a valuable use of our time, because simply put, it wasn't me," he recalled. "I've previously worked for the UAS Unit at the Civil Aviation Authority. I'm qualified and responsible in terms of my drone use." The next day, police put a note through his letterbox saying they had visited.
He was not the only local resident to receive police attention. At about 10pm on 21 December, 12 armed police officers stormed a house in Crawley, a few miles from the airport, and arrested married couple Paul Gait and Elaine Kirk on suspicion of "disrupting services of civil aviation aerodrome to endanger or likely to endanger safety of operations or persons". Gait, an ex-soldier and window fitter, was a model aircraft enthusiast. Their names leaked to the press. The Daily Mail's front page the next day splashed on the story, with a photo of the couple next to the headline: "Are these the morons who ruined Christmas?"
They were not, it turned out, the morons who ruined Christmas. During the 36 hours they were held at the police station, it was established that they had been at work while the drones were flying, and despite Gait's collection of remote-controlled helicopters, they didn't own a drone. (Kirk's ex-husband told the Mirror that it was unlikely she was involved because "she hates toy aircraft".)
They were released without charge. Gait delivered a tearful statement to the hordes of reporters outside their home: "As you can probably imagine, we are feeling completely violated. Our home has been searched and our privacy and identity completely exposed."
While Gait and Kirk were in police custody, there seemed to be another breakthrough in the case when a member of the public found a damaged drone in Horley, near Gatwick's perimeter fence. A forensics team looked for fingerprints, and digital data that could show where it had flown to and from. But on analysing this data, police ruled out its involvement.
The Gatwick drone incident led news broadcasts and front pages for days. It had cost airlines around £50m, and there were fears that it could spark copycat attacks if the culprit wasn't found. That weekend, the Sunday Times ran a story warning that terrorist groups were planning to attack airports using drones.
As the days passed and no one claimed responsibility, the theory that environmental activists were to blame seemed less and less likely. But the investigation appeared to be floundering. In the weeks after the incident, police visited Simon Dale, who runs a drone retail and repair shop, to gather background information about drones that might help their investigation. "The parameters they were describing didn't make sense," he told me. "[The drone] was apparently flying in and out of buildings close to terminal buildings, almost taunting the tower by one account, which would be very hard to do. They said you'd have to have intimate knowledge of the buildings, so the idea someone was tens of miles away doesn't add up. They were asking us if it could be controlled over 3G. It seemed quite far-fetched."
Military drones such as the Reaper or the Predator are capable of flying hundreds of kilometres and staying in the air for more than 24 hours at a stretch. But most drones do not have anything approaching this capability: they vary in size, but most are, even with their arms extended, no bigger than a laptop. They struggle to fly in wind or rain, and have limited battery life. Top-tier consumer drones can travel for up to five miles, but have a maximum flight time of about 30 minutes. Custom-built

drones might manage up to a couple of hours, but not much more: larger batteries add weight, which uses up more battery. "If someone were flying drones for hours, they'd need a carload of batteries," Ryan told me.

On 23 December, a few days after the incident, DCS Jason Tingley of Sussex police publicly expressed what many were thinking when he said: "We are working with human beings saying they have seen something." Gatwick is one of the most heavily monitored patches of land in the UK, but no hard evidence had been found. Tingley admitted that there was "always a possibility that there may not have been any genuine drone activity in the first place".

This did not go down well. The following day, Sussex police released a statement reiterating that sightings remained at the forefront of their investigation. On 29 December, Giles York, the Sussex police chief constable, went on the BBC's Today programme, saying he was "absolutely certain a drone was flying throughout the period the airport was closed". He told presenters that 115 sightings had been corroborated, and that 92 of these had come from "credible" people. But he inadvertently muddied the water further, saying: "Of course, we will have launched our own Sussex police drones at the time with a view to investigate, with a view to engage, with a view to survey the area looking for the drone, so there could be some level of confusion there."

Strangely, despite the lack of evidence, the possibility that this might have been a case of human error does not appear to have been entertained for long. Through Crimestoppers, Gatwick offered a £50,000 reward for anyone with information. The investigation marched on.

Drone enthusiast Ian Hudson started filing freedom of information requests (FOIs) in the first half of 2018, seven months before the Gatwick incident. His first few were aimed at local police forces near his home in Yorkshire. How many times had a drone been reported for flying near a school? Or taking contraband into prisons? Had there been prosecutions?

Hudson wanted hard data to counteract what he saw as scare stories about drones. Alongside his day job in IT, Hudson runs a popular drone-related Twitter account, @UAVHive, and is part of Britain's close-knit community of drone hobbyists, who gather on message boards to swap opinions about the latest tech and share photos taken from great heights. Hudson is sceptical of overblown fears about new technology. Back when mobile phones were becoming popular, Hudson worked in customer service for BT. "I was on the receiving end of worries about how they can burn your brain," he told me. "I think people fear drones because they're new."

On a cold day in September, I stood in a field outside Bradford with Hudson and a group of five local drone flyers. They were all men, mostly in their 30s or 40s, and had got to know each other via hobbyist Facebook groups. They handled their drones with immense care, joking that the machines might be blown away for ever in such high winds. In the presence of a drone, the first thing you notice is the sound – a deep, mechanical thrum as its small, helicopter-like blades spin to propel it into the air. One man, a commercial operator who uses drones for roof inspections, had brought along goggles that allow you to see through the drone's camera. I put them on, and as the drone took wobbly flight, I was transported over the hills and valleys that lay beyond.

A few years ago, a T-shirt became popular among Britain's drone flyers. "Before you ask", it says. "It's a drone. Yes, it was expensive. Yes, it has a camera. About 25 minutes. Over a mile away. No, you can't fly it." Since the Gatwick incident, the men told me, people who see

them flying drones are often more hostile than before. I heard several drone flyers repeat some variation of a new saying: "Gatwick drone? There's more evidence for the Loch Ness monster."
Civilian use of drones is expanding all the time, as technology improves and costs fall. Back in the 60s, remote-controlled model aircraft became available to consumers, thanks to breakthroughs in transistor technology, and an enthusiastic community sprang up, similar to that surrounding drones today. The CAA estimates that there are currently about 130,000 drone flyers in the UK, operating drones ranging from flimsy toys that sell for £50, up to much more sophisticated machines costing £1,000 or more.
Drones were developed as weapons. Their usage in war hugely increased after 2001, when the US deployed them in Afghanistan and Pakistan. Their association with warfare gives them a sinister edge in the popular imagination, as does the hornet-like buzzing sound they make in flight. There are concerns about their potential use in smuggling drugs or weapons; and the risks to privacy posed by flying cameras. In October 2018, seven men were jailed after using drones to fly £550,000 worth of drugs into prisons in the Midlands and the north-west. In Donbas, Russian-backed separatists have weaponised consumer drones to drop grenades on Ukrainian government trenches.
With his FOIs, Hudson aimed to show that such incidents are rare. His urge to dispel fears about drones comes from a deep enthusiasm about the possibilities that they offer. Drones can deliver medicine to hard-to-reach areas and survey fires to aid rescue missions. They have mundane uses, too; in roof inspections, they save the cost of scaffolding or the risk of climbing a very tall ladder, in the oil and gas industry they are used for remote monitoring of platforms and oil spills. As far back as 2013, Jeff Bezos floated the idea of drone-based Amazon deliveries.
The men at the drone meetup near Bradford were mostly interested in photography – they showed me aerial shots of the ocean and spectacular landscapes. "I'd just never get to see this perspective without a drone," one man told me, a sense of wonder in his voice.
Drone enthusiasts speak scathingly of rulebreakers: this is a self-policing community. They worry that misuse will lead to more regulation, which will hamper their activity. "If someone is doing mischief, which you'll find on YouTube or whatever, people immediately report them to the police and the CAA," said Hudson. "There's no tolerance of people being daft with drones – there'll be laws made and it'll affect everyone who has one."
When Hudson first heard about Gatwick, "I thought this was some absolute idiot and I wanted them caught." But then he realised "the basic facts don't add up". Sussex police had mentioned lights in the corroborated sightings. But if someone had planned the attack, to the extent that they had procured scores of batteries and hacked the drone's in-built geofencing software – which uses GPS to stop drones from flying into restricted zones such as airports or prisons – then why would they leave the lights on? "You'd disable them," said Hudson.
Hudson looked at publicly available information: photographs taken during the incident, and statements by Sussex police. Since then, he has identified inconsistencies that he believes undermine the claim that there were drones at Gatwick. Soon after we first spoke, Hudson sent me a long email, including a timeline of tweets and photographs posted during the incident, highlighting contradictions. ("Did he send you four A4 pages with closely typed text and diagrams?" another drone-flyer joked. "It's one of Ian's pet subjects.")
The photos he included showed military counter-drone systems being set up on 20 December, the second day of the shutdown – and tweets by Sussex police mentioning sightings after this point, right into the early hours of 21 December. This included one cluster by "credible" witnesses – airport staff and police officers.
After it was set up, the military system should have picked up any drone activity – but nothing was recorded. Hudson wanted answers: "I want to be able to say: 'Wait a minute, these credible witnesses aren't all credible.'"
In July 2019, about six months after the incident, Hudson filed his first FoI to Sussex police: "Can you confirm the date and time of the final sighting of the December 2018 drone at Gatwick?" Under the Freedom of Information Act, public bodies have to respond within 20 working days. Often this is refused, on grounds of national security or the time it will take to find the information. But Sussex police did not even send a refusal.
Gary Mortimer, editor of the popular drone site sUAS News, and a general enthusiast for flying objects (at different points, he has been a hot air balloon pilot and a member of the air force), joined Hudson in filing FoI requests. Apart from a response to a simple question about the cost of the investigation, their requests were almost always ignored or rebuffed. Ryan, the barrister, filed an FoI of his own with Sussex police. It included 14 questions. "I wanted to understand: how on earth did I get on their list?" he told me. These, too, went unanswered, and remain so today.
Soon after the incident, Mortimer had published a blog post questioning whether the supposed drone might have been "a cover for some other operation". But he also wondered if the real explanation might be more mundane. "One option is that something that wasn't a drone was reported, and then the next day, police flew their aircraft there and people saw that," he said to me. "Then it's Chicken Little and the sky falling in."
In the months following the Gatwick incident, there was a flurry of alleged drone sightings at airports around the world – though each only resulted in shutdowns of an hour or so. In January 2019, it was Heathrow, and Newark in the US; in February 2019, Dubai. Anxiety about malicious uses of drones intensified in September 2019, when a splinter group of

Extinction Rebellion announced plans to shut down Heathrow by flying drones on the runway. The organisers were arrested and no drones were flown. Soon afterwards, the retailer John Lewis said it would stop selling drones due to the risk of misuse. "It feels like people are turning against drones, even though most flyers just want to photograph nice landscapes," one hobbyist told me.

Before the Gatwick incident, there were already calls for the government to address the potential threat of drone misuse; the British Airline Pilots Association was one prominent voice. In January 2019, parliament published the results of a major drone consultation and brought in more regulation, including compulsory registration for drones over a certain weight, and greater police powers to land and seize them. This had been under way before Gatwick, but the incident focused political attention. In the weeks that followed, Gatwick and Heathrow spent £5m on counter-drone systems. A more far-reaching drones bill is on its way through parliament.

In theory, it should be fairly easy to assess how often drones get close to planes, but in fact, this is disputed. When two aircraft come too close to each other, the incident is known as an "airprox". Pilots or air traffic controllers report such incidents to the UK Airprox Board, which exists to enhance air safety by reporting "the circumstances, causes and risks of collision" in UK airspace. It recorded 280 such events in 2017, 40% of which related to drones. The overall number of reported incidents has increased by a third since 2016.

In late 2018, Simon Dale, the drone retailer, set up a website called Airprox Reality Check, where he digs into the data for drone sightings reported to the board, assessing what else might have been in the area. "More often than not, it's a full-sized helicopter," he said.

In the US, the Federal Aviation Authority said it gets more than 100 reports every month from citizens who believe they've seen a drone near a plane or an airport. Back in 2015, the Academy of Model Aeronautics analysed these sightings and found that just 3.5% actually involved a near-miss between aircraft and a drone.

Sussex police and Gatwick Airport both firmly stuck to the line that the December 2018 drone sightings were credible, since they were reported by police officers and airport employees who knew what they were seeing. "We can all accept that some of the sightings were wrong – that's obvious," said the former Gatwick employee who did not want to be named. "But these were colleagues who had been working at airports for 20, 30 years, and knew how serious it was."

Back in the 60s, Percy Walker, the director of Britain's Ministry of Aviation accident inspection branch, said that eyewitnesses to aviation accidents are "almost always wrong". Subsequent academic studies support the notion that it is difficult for the human eye to accurately assess fast-moving, distant objects. If people often think they have seen a drone when they have, in fact, seen something else, then what else could have happened at Gatwick?

In April 1954, a strange phenomenon swept across the town of Bellingham, Seattle, and other communities in Washington state. People began to observe "windshield pits" on their cars – minor damage that, when magnified, can look like a tiny crater in the surface of the glass, usually caused by sand or other small debris colliding with the windscreen at high speed. As the phenomenon was reported in the press, more people noticed marks and chips on their screens. A few weeks before the sightings began, the US had exploded a huge hydrogen bomb in the Pacific Ocean, and many blamed these nuclear tests. Others believed a nearby navy communication tower was warping the glass. Residents panicked. By 15 April, almost 3,000 windscreens had been affected, and the mayor asked for assistance from President Eisenhower.

Today, the Seattle windshield pitting epidemic is often cited as an example of mass panic, in which people attributed a sinister cause to something that had been there, unnoticed, all along. Two days after the appeal to the president, Seattle police issued a statement saying that the pitting epidemic was "95% public hysteria". Sightings suddenly stopped.

This kind of mass panic has been documented throughout history, and all over the world. More recently, the "Croydon cat killer" was alleged to have brutally murdered hundreds of cats in and around London, leaving the bodies, in the words of one journalist, "in places children are sure to find them". The alarm was raised by a cat shelter, and reports in the local press were picked up nationally and then internationally – despite the fact that there was no discernible pattern, or evidence of human involvement. As the story gained prominence, more people reported cat murders: ultimately, more than 500 were called in. But after an investigation spanning several years, in September 2018, the Metropolitan police concluded that the cats had been hit by cars or eaten by foxes.

Is it possible that something similar happened at Gatwick? "In a state of anxiety, we often focus attention on innocuous stimuli," said Gary Small, professor of psychiatry at UCLA and an expert in mass hysteria. "There's a lot of anxiety about terrorism. There's a lot of anxiety about drones."

In the year that followed the Gatwick drone incident, police knocked on 1,200 doors, took 222 witness statements and identified 96 persons of interest. But on 27 September 2019, Sussex police formally closed the investigation, saying that "without new information coming to light, there are no further realistic lines of inquiry". The force said that the incident was not terror-related, and that there was "no evidence to suggest it was either state sponsored, campaign or interest-group led". The force cited "corroborated witness statements" in its conclusion that at least two drones were in operation through this period, and that it was a "serious and deliberate criminal act designed to endanger airport operations and the safety of the travelling public".

In June 2020, Sussex police settled out of court with Paul Gait and Elaine Kirk, agreeing to award the couple £200,000 in damages and legal fees for their wrongful arrest. No one else has been charged over the drone incident, and the couple's legal team said that "serious doubts remain as to whether there were, in fact, any drones flown over the airport".
In public, the airport and police stuck firm to the idea that there was definitely a drone incursion. But privately, some have doubts. "We work on evidence, and I haven't seen any. That's really all there is to say," one police officer with knowledge of the case told me.
Still, many people remain convinced. Dunn, the professor at Birmingham University who studies the security risks posed by drones, said "there is a circuit of people interested in this topic", referring to drone researchers and airport personnel, "and they're fairly categoric that while the later sightings may have been a crane, initially there were absolutely drones".
At the time, there was no clear guidance on what an airport should do in the event of a drone incursion, accidental or hostile, so closing the airport was a reasonable decision. "It's not an industry that can take a flippant view about any threat to safety, and there can be a high price for that," said John Strickland, the aviation consultant.
"Pre-Gatwick, it was like the blind leading the blind, because nobody really knew what to do. But since Gatwick, a lot of bright people have focused on how to solve this problem," says Richard Gill, CEO of Drone Defence, a security consultancy that provides counter-drone technology to governments and big corporations. This view is shared across the industry. "While we may never know what really happened at Gatwick," says Adam Lisberg, the corporate communications director at drone manufacturer DJI, "it was the event that forced the aviation and drone industries around the world to find solutions so that a single drone sighting doesn't close down an airport."
Few people disapprove of improving systems for keeping airports safe, but hobbyists feel that suspicion is being cast on anyone who flies a drone at all. In Bradford, one man told me he had sold his drone – it was too difficult to find areas where flying was permitted. Even Ian Hudson told me that he barely flies his drones any more. "It's just too much hassle," he said.
But drones remain a passion – and he is persevering with his FOIs. He recently got a tranche of heavily redacted emails from the Department for Transport, showing discussion of counter-drone systems in the days that followed the incident, but nothing directly related to the investigation. Sussex police, in particular, has been remarkably unresponsive. "There's been no explanation, and it just comes across as people covering arses," Hudson said. "I want to get to the truth."
Most people with any interest in the Gatwick drone have already made their mind up. Either the initial sighting was a mistake, and subsequent sightings were the result of mass panic or confirmation bias, as proved by the technical unfeasibility of what was described. Or there was a drone, and the same technical challenges are evidence that it was an extremely sophisticated attack, one that we should be wary of dismissing.
"I cannot rule out the capabilities of a mystery drone, but the more seemingly magical powers ascribed to it, the more sceptical you become," said Lisberg. "Every time a bit of information challenges the initial version, it seems to confirm how sneaky it really was. You find yourself doing mental gymnastics. At a certain point, you're really chasing drones."

Samira Shackle *is editor of the New Humanist and a regular contributor to the Guardian long read. Her book Karachi Vice will be published by Granta in February 2021.*

Drones come to the rescue in Covid battle at sea

Source: https://splash247.com/drones-come-to-the-rescue-in-covid-battle-at-sea/

Dec 03 – The ancient Greek poet Menandros stated "το δις εξαμαρτείν ουκ ανδρός σοφού", namely you are not wise if you repeat the same mistake. This is a saying that is even more important nowadays that most countries are currently experiencing the second wave of the Covid-19 pandemic. Although Covid-19 has resulted in significant socio-economic impacts upon every nation, we have observed a relatively uninterrupted flow of commerce primarily due to seaborne transportation of goods and services.
Safe conduct of the maritime operations should always be performed within a safety and environmental protection framework that can be enhanced by implementation of newly proven technologies. The case of mobilising drones was assessed on this basis and their effect on safety was examined with seafarer health and well-being being the prevailing critical parameters. Even with the recent positive news about the Covid-19 vaccine, we all need to maintain our protection and safety efforts.
The future of drones being used to provide goods and services to ships will one day be routine for the maritime industry. Additionally, drone technology will require a regulatory framework that includes robust guidelines, policies and operational procedures to ensure their safe and secure integration into the maritime logistics network.

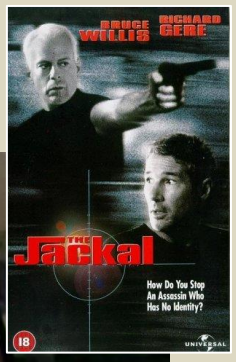
Based on the above and upon completion of the desktop assessment with the involvement of American Club represented by Dr William Moore and the Hellenic Drones company, a full- scale test was recently conducted at the port of Elefsis, Greece. A project drone was selected and a kit of rapid Covid-19 tests for 20 persons was transported to a roro vessel that was anchored two nautical miles away from the port. The distance was successfully covered within four minutes without the physical interference of the human element, a need that has been created since the evolution of the Covid-19 pandemic becoming a health and safety challenge to the maritime industry and especially the ship's crew.

This full-scale test was the first of its kind and could serve as the basis for the remote delivery of Covid-19 test kits and vaccines to thousands of seafarers. This option of mobilizing drone technology should be properly considered to meet the logistical challenges the world faces as it combats Covid-19.

With several local or national lockdowns, travel restrictions and increased number of incidents and deaths, everyone should provide every possible support, effort and solution(s) to ensure we tackle this problem safely and efficiently in order to ensure safe maritime operations and minimise losses.

How Easy Is it to Build a Robot Assassin?

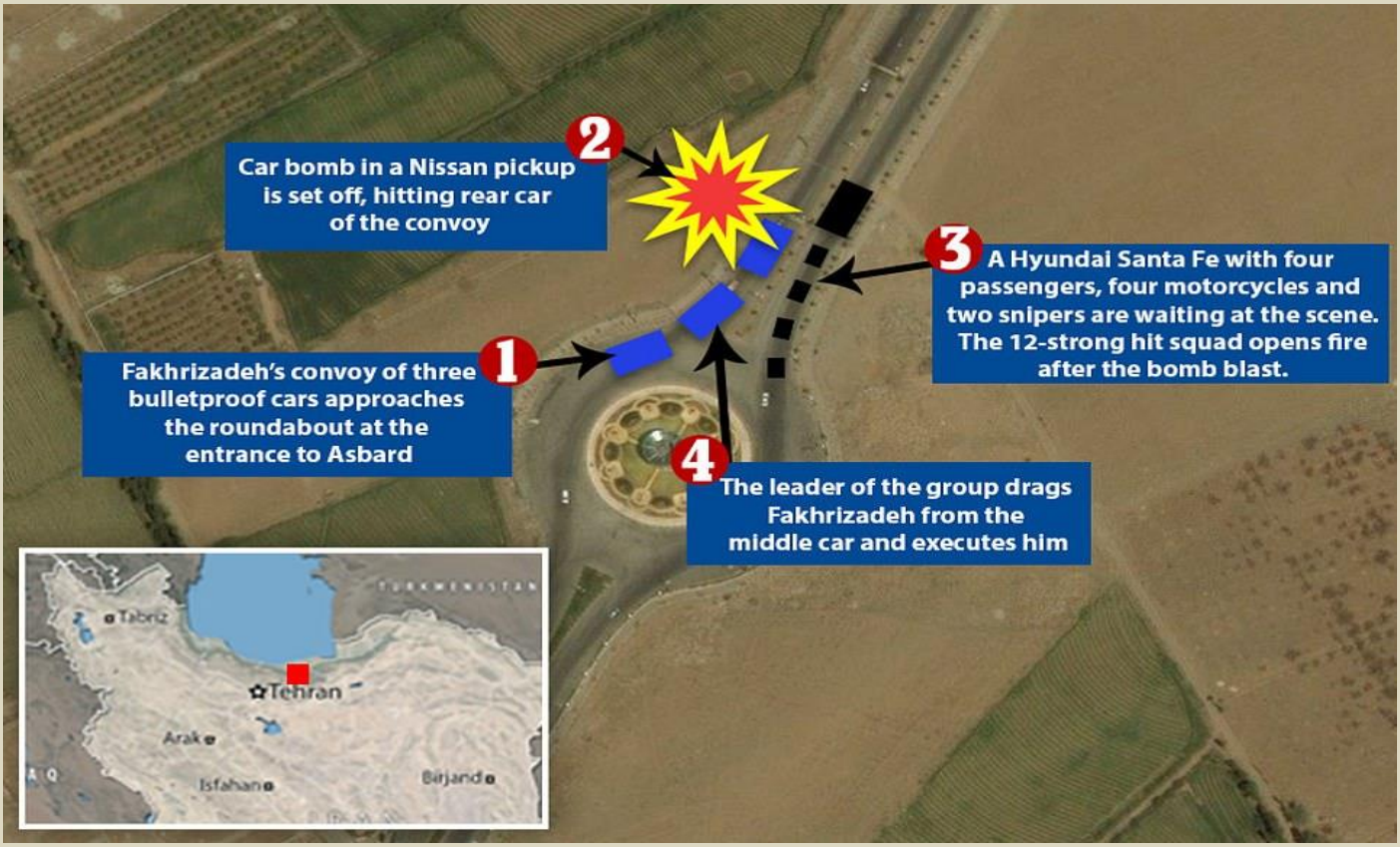
Source: http://www.homelandsecuritynewswire.com/dr20201204-how-easy-is-it-to-build-a-robot-assassin



Dec 04 – Someone—almost certainly Israel—recently assassinated Mohsen Fakhrizadeh, the leading scientist behind the Iranian nuclear program. The latest reporting from Iran suggests that the assassins employed a remotely controlled machine gun mounted on a pickup truck. Nicholas Weaver writes in *Lawfare* that if this reporting proves correct, the death of Fakhrizadeh will not be the first instance of successful or attempted assassination-by-robot: In 2018, Venezuelan President Nicolás Maduro survived a possible

attempt on his life carried out by small drones armed with explosives. And the U.S., in targeting Iranian Major General Qassem Soleimani with a drone strike, has made clear that it is not above the use of such tools in modern statecraft.
So how hard is it to build such a tool? How expensive?
Weaver writes:

> Unfortunately, the answer is "hard but doable" and "not much money"—with the further complication that in a few years, it will probably be possible to pick up the necessary equipment online from vendors like Banggood. I know, because this field is something of a hobby for me. For three years, I've been trying to build an autonomous computing package for drone-hunting drones, and this work has familiarized me with the relevant technology.
>
> **It doesn't take much for a robot to kill an exposed person. 200 grams (seven ounces)—not that much more than a baseball—is enough explosive to kill anyone within five meters (15 feet). A small ground or air vehicle can easily carry that payload, creating a robotic assassin.**



Amazing new details of the Fakhrizadeh assassination emerge in the Iranian press: IRGC affiliated Fars news reports the assassination was done using an automatic machine gun operated with a remote control and not with gunmen who were on the ground. According to the report Fakhrizadeh and his wife were on their way to spend the weekend at their house in a Tehran suburb. There were three security cars with them and at a certain point the leading car left the motorcade to do a preliminary security check of the house. Right after the car at the front of the motorcade left shots were fired on Fakhrizadeh's car and it stopped. Fakhrizadeh stepped out of the car thinking his car hit an object on the road or there was a problem with the engine. At that point shots were fired again from a Nisan pickup truck which stopped 150 meters from Fakhrizadeh's car. The shots were fired from an automatic machine gun which was mounted on the pickup truck and operated by remote control. Fakhrizadeh was hit by three bullets – one hit him in the spine. Seconds later the Nisan pickup truck exploded in what looks like a self destruct mechanism. According to Fars news Iranian security forces identified the owner of the pickup truck who left Iran on October 29th. Fars reported the assassination operation lasted only three minutes and was all done by remote control with no gunmen on the ground.

Weaver notes that currently, the remote control needed to maneuver such an assassin is easily defeated with broad-spectrum jamming, which interferes with the radio signals necessary for communication. "In order to avoid this problem, successful robotic assassins will need to be autonomous, capable of identifying targets and attacking without any human intervention," he notes.

Likewise, a drone-hunting drone needs to be autonomous because it needs to deal with autonomous—and therefore fast-thinking—adversary drones. "Basically, to fight autonomous robot assassins, I need to build autonomous robot assassins to assassinate the autonomous robot assassins."

> **The available hardware and most of the software pieces are already available—it's simply a matter of assembling everything together on a single circuit board. Combining a low cost hardware autopilot, a powerful compute module, a GPS receiver, a cellular modem and a machine-learning accelerator all on the same board—and getting it to fit in a small footprint—is a fun design exercise.**

The software is also widely available.

> And this is where the modern supply chain comes in. Every piece I'm using is already widely available in scattered pieces—and providing a single integrated package would be useful for so many tasks, not just offensive ones. The same software and hardware needed for killer drones can just as easily act as a synthetic peregrine and chase away birds from a vineyard or keep a continual watch for wildfires. Because the benign market is so large, I suspect that the "brains" needed for small autonomous robots will be available in integrated packages in less than five years.
>
> **Scary times may be ahead. Will it soon become dangerous for world leaders to walk in open air while in office?**

UPDATE: According to Iranian news agency Tasnim the machine gun was satellite driven and the smart camera used a face recognition software allowing to kill the target but not the woman sitting 25cm apart.

ISIS Used Open-Market Suppliers, including in U.S., in Quest to Develop V-1 Superdrone

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/airport-aviation-security/isis-used-open-market-suppliers-including-in-u-s-in-quest-to-develop-v-1-superdrone/

Dec 08 – Weapons designers working for the Islamic State posing as fictitious front companies procured technology from suppliers in the United States, Canada, Hong Kong, Britain and beyond with many in the complex chain skirting authorities and some still operating, according to a new report.

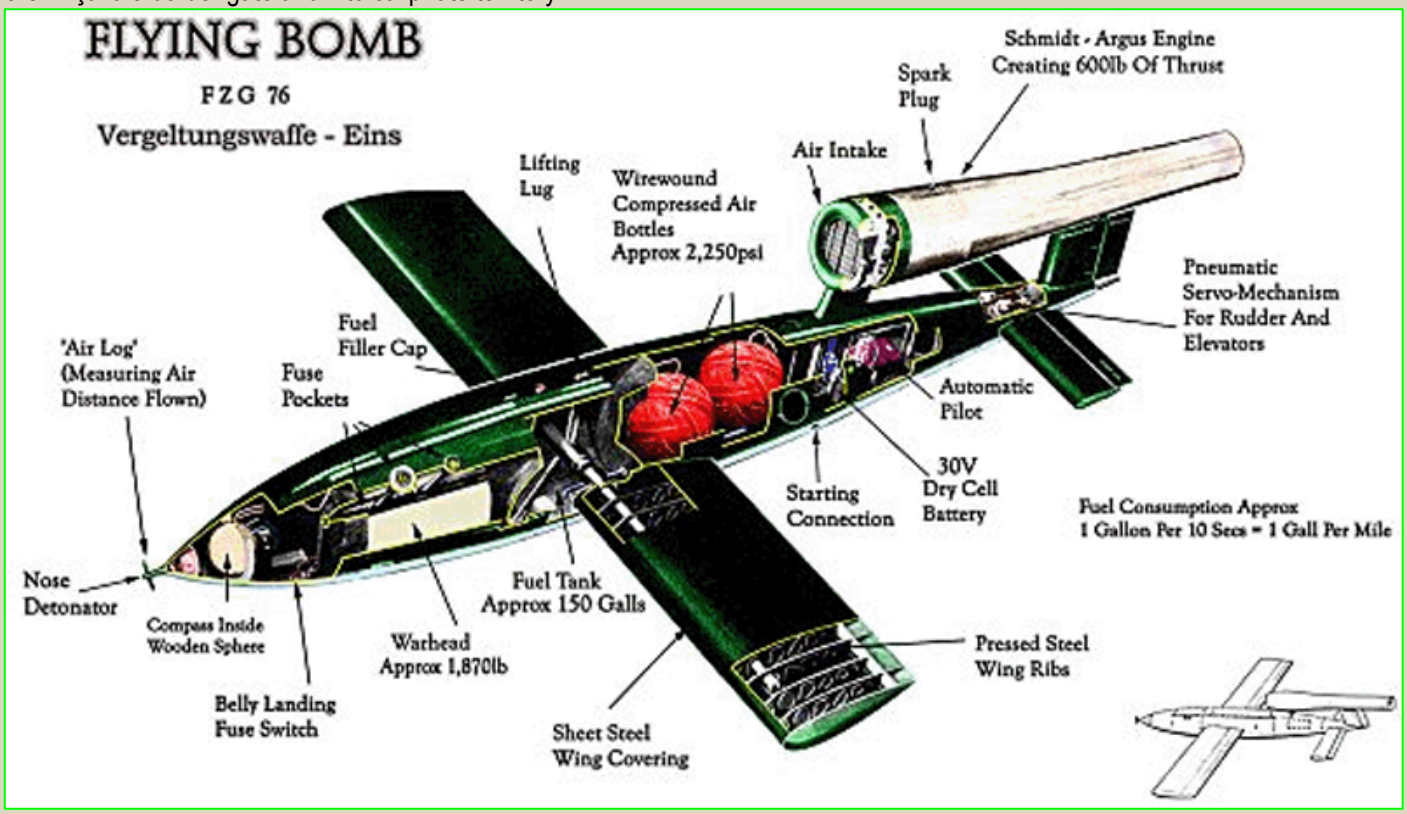
UK-based Conflict Armament Research, which tracks the weapons trade in conflict areas, said their 18-month investigation also revealed that ISIS had been developing and bought plans for "pulsejet" engines to power large, high-speed drones intended to act like the **V-1 flying bombs of World War II**, with an ISIS military production document stating that "we are working on applying the V-1 engine used by Hitler to attack Great Britain."

Before Syrian Democratic Forces and Iraqi forces recaptured caliphate territory from ISIS, operatives of the terror group also pretended they were working on systems to track weather balloons and monitor crop-spraying in order to procure on the open market software and hardware for an automated anti-aircraft system.

Weapons components ultimately made it into ISIS territory through linked, family-owned companies and individuals acting as supply chain "choke points" around Siverek and Akçakale in southern Turkey, though there is no evidence they were aware that they were funneling goods to ISIS, says the CAR report. Still, some of these companies made purchases that didn't make sense given their business, such as a small cell phone store acquiring six tons of aluminum paste from a chemical distributor.

ISIS members along the supply chain also facilitated acquisitions, including one operating a business in the UK who bought "high-specification motion-control units from a North American company," but the payment — more than $18,000 — came from an unrelated limo service in Istanbul. "The same UK company purchased rocket and unmanned aerial vehicle (UAV) components from companies in North America and Germany but asked the sellers to ship them to the address of a mobile phone shop in Şanlıurfa, close to the Turkish-Syrian border," the report adds.

CAR said that from 2014 to 2017 ISIS forces in Iraq and Syria "established one of the most sophisticated production capabilities for improvised weapons and improvised explosive devices (IEDs) of any non-state group to date," and "production became increasingly technically advanced and quasi-industrialised" thanks to international procurement of materials that "moved remarkably rapidly though IS forces' supply chains." A report from the Islamic State Border Crossing Security Department recovered by Syrian opposition forces in 2015 said ISIS coordinated with established border smugglers who paid local Turkish officials to allow goods to flow through the Akçakale border gate and into caliphate territory.



Investigators identified more than 50 companies in at least 20 countries that "produced or distributed goods that IS forces subsequently used to make IEDs, UAVs, and improvised weapon systems," including "manufacturers and distributors of chemicals used in the production of explosives or chemical agents; manufacturers of items used as containers for IEDs and IED main charges; producers of commercial explosives; and companies making products ranging from electronic components to complete, commercial off-the-shelf UAV systems." Last year, CAR began probing how the ISIS networks operated and duped unwitting suppliers.

Most of the ISIS weapons systems under development "have yet to be observed in the field" but weapon specialists with the terror group "acquired expertise; designed systems and software by engaging unwitting suppliers; and built functional prototypes using materials and components procured" through "global and online marketplaces."

Seven quadcopter drones used by ISIS in Iraq were traced by CAR back to independent distributors in Kuwait, Lebanon, Singapore, Turkey, and Uzbekistan. Development of the "pulsejet" UAV goes as far back as 2015, when that August an individual posing as "David Soren" of Advance Technology Global Ltd. ordered plans from a U.S. company catering to hobbyists for a pulsejet engine capable of 50 pounds of thrust. The buyer "emailed the company's owner to ask whether the engine could be used to power a 40-kg model airplane."

Two years later, an Iraqi operation in Mosul discovered a fully constructed pulsejet engine nearly seven feet long with a machined air-intake head and a motorbike spark plug for ignition. The design differed somewhat from the plans "David Soren" purchased, indicating the ISIS designers had additional technical sources. CAR has not found evidence of the ISIS propulsion system being incorporated into a drone, and separately documented ISIS workshops with components to construct a UAV with a 10-foot wingspan.

In the 2015 development of an anti-aircraft system, "a UK-registered front company established by an IS weapon designer entered into contracts with suppliers of machine vision software and hardware, including high-specification cameras and motion control units, based in North America and Asia," said the report. "…The system envisaged using cameras mounted on moving platforms. When the system located a flying object, all the cameras in the system were intended to 'lock on and track that object' physically using heavy-duty pan/tilt motion-control units. This design may have been intended to allow the system to be used to mount weapons as well as cameras."

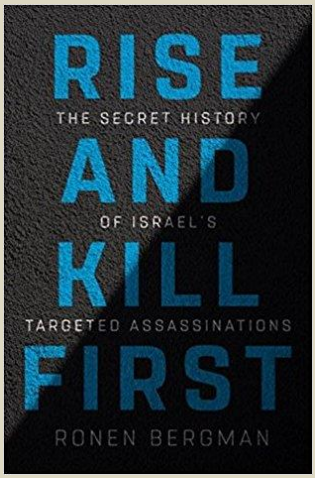
That front company communicated with suppliers only over email, third-party websites, and VoIP calls/chat, used at least three pseudonymous email addresses with two of the email accounts coming from Turkish IP addresses, and used Western Union to pay suppliers through an individual in Hong Kong still unknown to investigators.
CAR has no evidence that the anti-aircraft system was completed by ISIS technicians, and noted that "some suppliers ended their contracts prematurely after becoming suspicious about the front company's identity and intentions."
The ISIS purchases displayed multiple red flags that taken together "indicate that individuals and companies may be working outside their standard course of business," the report said, stressing the need for "suppliers to conduct additional due diligence."
"Importantly, the supply chains described in this report were not reliant on territorial control or on capturing commercial goods or facilities. Although IS forces may no longer hold territory, remaining IS cells in Iraq and Syria became increasingly active in 2020," the report concluded. "Disrupting their procurement efforts by spotting transactional red flags will therefore remain an important tool against the resurgence of IS forces and their successors."
CAR expects to issue a report in the future on its investigation into the procurement mechanisms that ISIS used to acquire commercial explosives, especially detonators and detonating cord.

***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.*

Guns, Drones and Poison: The New Age of Assassination

By Paul Maddrell
Source: http://www.homelandsecuritynewswire.com/guns-drones-and-poison-new-age-assassination

Dec 14 – Nobody has officially claimed responsibility for deploying the satellite-controlled machine-gun with "artificial intelligence" used to assassinate Iranian nuclear scientist Mohsen Fakhrizadeh in Tehran at the end of November.



But you would get fairly short odds were you to bet on it being the Mossad, Israel's aggressive – and notoriously inventive – foreign intelligence service.
Israel has been carrying out what it calls "targeted killings" ever since its foundation in 1948. In his book, Rise and Kill First, leading Israeli journalist Ronen Bergman estimates the number of targeted killings at approximately 2,700.
Israel's intelligence agencies are renowned for the inventiveness of their assassinations. Wadi Haddad, the director of foreign operations of the Popular Front for the Liberation of Palestine (PFLP), was murdered in 1978 with poison in his toothpaste. Yahya Ayyash, "the Engineer" who masterminded a number of Hamas suicide bombings in Israel, was killed in 1995 by an explosive charge placed in his cellphone.
Imad Mughniyeh, Hezbollah's chief of staff, was killed by a car bomb in Damascus in February 2008. According to Bergman, the Israelis might have killed Iranian general Qasem Soleimani with Mughniyeh, but only had the United States' agreement to killing Mughniyeh.
Of course, it's not just Israel which disposes of its foes via extra-judicial killings. We are living in the greatest-ever age of assassination as states, fearful of the twin threats of terrorism and weapons of mass destruction, are using increasingly sophisticated intelligence to track and kill dangerous people and deprive other states of dangerous knowledge.

New Technology
The modern era of assassination began on 9/11 when the US realized how exposed it was to mass casualties from terrorist attacks on its soil. The "war on terror" took both crude and more subtle forms, the former being the invasions of Afghanistan and Iraq, the latter including an airborne assassination program enabled by new technology.
The drone has been a very effective assassin of terrorists. The first killings by drone took place in Yemen in 2002 – and, by the end of 2013 US drones and aircraft had killed between 719 and 929 people in Yemen alone. Meanwhile between 2004 and the end of 2013, the number of people killed by drone in Pakistan was between 2,080 and 3,428.
Special forces have been used to kill key targets such as Osama Bin Laden in Pakistan in 2011 and Abu Bakr al-Baghdadi in Syria in 2019. In finally killing Quds Force commander Qasem Soleimani in a drone strike in Baghdad in January 2020, the US took the radical step of eliminating a key state actor it considered to be a terrorist. The killing was deemed unlawful by the United Nations.

Russian president Vladimir Putin has also been ruthless, particularly when it comes to eliminating political foes. The attempted murder, by nerve agent, of former intelligence officer and British spy Sergei Skripal in Salisbury, south-west England, in 2018 and the successful murder of former Russian intelligence officer Alexander Litvinenko by polonium-210 slipped into a cup of tea in a London hotel in 2006 are merely the most high-profile killings in a chain of assassinations during Putin's presidency. Among his victims have been opposition politicians and journalists, as well as veteran fighters from the bitter war in Chechnya who had been designated as terrorists by Moscow.

Preventing Proliferation

Since the 1940s, the world's leading powers have tried to prevent their enemies from developing weapons of mass destruction. Assassination to prevent the development of these technologies was pioneered by Britain in the second world war. One night in August 1943 the Royal Air Force bombed the German missile development and testing site at Peenemünde, on the Baltic. The RAF targeted the living quarters of the scientists, engineers and technicians with the aim of killing as many as possible. Approximately 130 German scientific workers were killed in the attack.

Britain and the US also feared that Nazi Germany might be developing an atomic bomb. In 1944 an American agent was dispatched to Switzerland to attend a lecture by Germany's leading nuclear physicist, the Nobel Prize-winning Werner Heisenberg.

The agent was armed and had orders to assassinate Heisenberg if anything the physicist said indicated that Nazi Germany was close to developing an atomic bomb. In the event Heisenberg's lecture gave no hint of this, which is why he survived his visit to Switzerland.

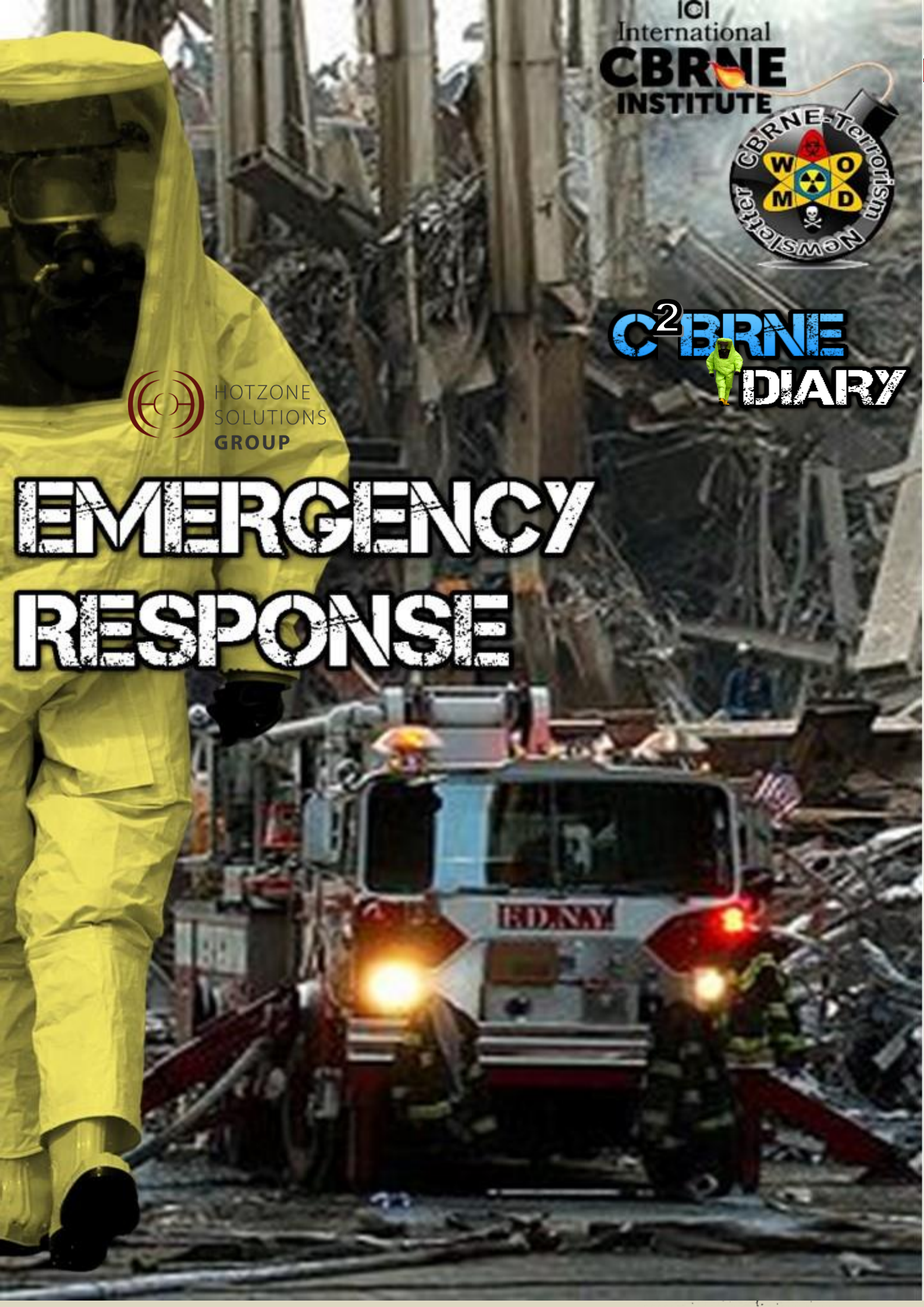
Israel has also used assassination to try to prevent its neighbors from developing missiles and nuclear weapons. In the 1960s, it tried to obstruct Egypt's missile development project by murdering German engineers working on it. In 1980-1981 scientists and engineers working on Iraq's nuclear weapons project were murdered while outside Iraq.

In 1990 the Israelis killed Canadian scientist Dr Gerald Bull, who was manufacturing for Saddam Hussein a "supergun", the largest cannon ever assembled, which would have fired rocket-assisted projectiles thousands of kilometers. Bull's murder ended the project.

Since 2007 Israel has tried to kill Iranian nuclear scientists: four have been assassinated, and an attempt made on the life of a fifth. Israel has never accepted responsibility for the assassinations but is universally thought to be behind them. Killing a small number of scientists won't stop the project.

Assassination is as old as politics itself. But the increase in terrorism and the spread of the technology and know-how for the development of weapons of mass destruction are increasing its use. For the foreseeable future states will continue to assassinate terrorists and scientific workers employed on WMD projects because they regard them as dangerous.

***Paul Maddrell** is Lecturer in International History and International Relations, Loughborough University.*


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

Ebike ambulance hits the streets of Paris

Source (+video): https://newatlas.com/bicycles/ebike-ambulance-emergency-bike/

Nov 24 – Because bikes can skirt around traffic jams – and park just about anywhere – they're often faster than cars on congested city streets. That's why bicycle couriers exist, and it's also why the Emergency Bikes ebike ambulance was created.

The vehicle was designed by PR/tech development firm Wunderman Thompson Paris, in partnership with French electric mobility company Ecox Enterprises. Additional input was provided by UMP (Paris Emergency Services) and cargo bike manufacturer Urban Arrow, the latter of which provided the cargo ebike that serves as the base.

Added onto that bike is a 150-liter insulated storage box for medical supplies, a 140-decibel horn, a high-intensity flashing blue LED, medical symbols on the wheel covers, anti-puncture tires, a GPS unit that allows for location tracking, and a USB port for powering portable devices.

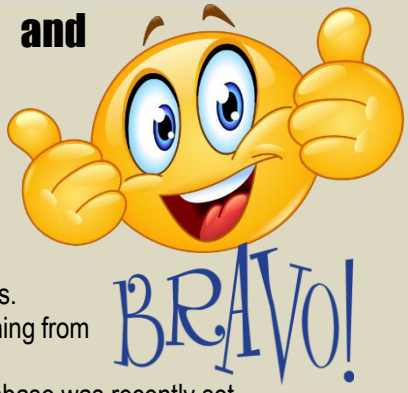
The bottom bracket motor is powered by two 500-Wh lithium batteries, reportedly providing an electric-assisted pedalling range of up to 160 km (99 miles). Hydraulic disc brakes give the bike plenty of stopping power.

According to their designers, Emergency Bikes can reach urban Paris locations approximately twice as fast as traditional ambulances (Wunderman Thompson Paris)

A Wunderman Thompson representative tells us that Emergency Bikes are currently available "to any emergency service that is interested," and that several such groups have already requested bikes.

In fact, a doctor who tested the prototype in Paris this summer has since bought the first production bike, and now uses it on a daily basis when responding to emergency calls within the city. Needless to say, conventional ambulances are still required for transporting patients to the hospital.

Thousands of UAE frontline workers to undergo crisis and disaster training



Source: https://www.thenationalnews.com/uae/health/thousands-of-uae-frontline-workers-to-undergo-crisis-and-disaster-training-1.1131465

Dec 19 – First responders, medics and others will be equipped to handle 'natural disasters, fires and nuclear incidents'

Thousands of frontline workers will undergo training to prepare them to respond to major disasters.

Medical staff and other essential personnel will each receive 60 hours of training to handle everything from "infectious disease and airborne viruses to natural disasters, fires and nuclear incidents".

The announcement of the **'Jaheziya' training initiative** - meaning Readiness - came after a database was recently set up to register 80,000 essential staff that could be called upon in a crisis.

The initiative was announced by the Sheikha Fatima bint Mubarak Volunteer Programme and the Frontline Heroes Office, which was set up to ensure the welfare of crucial personnel during the pandemic.

We have a responsibility to our people to protect the UAE from potential threats today and for generations to come
Sheikh Sultan bin Tahnoun, Frontline Heroes Office

Those who complete programme will receive an internationally-recognised certification from a group of US and UK disaster management institutions.

Noura Al Suwaidi, secretary general of the General Women's Union, one of the initiative's organisers, said the training would "unify all medical and non-medical emergency responders, as well as our volunteer networks, to be able to work more effectively as a single, cohesive unit to respond to emergency situations".

The first courses are set to start in January.

Trainees will be required to take exams to obtain the certificates, and the best performing candidates will be nominated to participate undergo training to become instructors.

"As a nation, we have a responsibility to our people to invest in and maintain the highest level of emergency and disaster response capabilities to protect the UAE from potential threats to public safety today and for generations to come," said Sheikh Sultan bin Tahnoun, chairman of the board of the Frontline Heroes Office.

"At the same time, we owe it to our frontline professionals to provide them with the highest standards of professional training available both for their career development as well as to best enable them to deliver on the commitment they make every day to serve their nation."

The programme is available to all medical professionals, ambulance and rescue team members, plus staff working in a wide range of crisis response departments, and all professionals and volunteers on the Frontline Heroes Office registry.

The registry includes the names, specialisms and contact details of 80,000 frontline workers deemed essential in the fight against Covid-19.

They include healthcare practitioners, police, essential service providers, crisis managers, security and emergency service providers, humanitarian agencies, sanitation personnel and volunteers.

Members can benefit from financial support to help with living costs, including help with school fees and housing costs, along with various promotions and discounts in recognition of the role they play.

The Frontline Heroes Office was set up in July by decree of the President, Sheikh Khalifa, and was tasked with ensuring critical personnel are "nationally recognised and celebrated".

EDITOR'S COMMENT: The epitome of "lessons learned"! **BRAVO UAE!!!**

Inside the warehouse containing some of the nation's most critical supplies and vaccines

By Priscilla Alvarez and Kristen Holmes, CNN

Source: https://www.weny.com/story/43084266/inside-the-warehouse-containing-some-of-the-nations-most-critical-supplies-and-vaccines

Dec 20 – The warehouse is like any other with row upon row of products stacked on top of one another with identifying barcodes. But it's unique in that it contains critical items to protect the United States in the event of an attack or disaster. And this year, the warehouse became a flashpoint in the Covid-19 pandemic.

The Strategic National Stockpile dates back to 1999, when fears of a bioterrorism attack coinciding with the Y2K computer switch were front and center, and serves as the country's repository of emergency medical countermeasures. But hit with a global pandemic and nationwide demand for supplies, the stockpile, which is maintained by the Department of Health and Human Services, was deemed inadequate.

"The nation agreed: We weren't where we needed to be," said Steven Adams, acting director of the Strategic National Stockpile, adding there are ongoing discussions to better position the stockpile to respond to national need.

Adams said his team has had four briefings with the Biden transition team, adding that so far there has been no disconnect with the incoming administration over long-term plans for the stockpile.

CNN received inside access to one of the federal stockpile warehouses, which are spread out across the country, and agreed not to disclose the location for national security reasons.

In a nearly 300,000-square-foot warehouse that CNN visited, HHS holds roughly $2.3 billion worth of products including vaccines for smallpox and anthrax, medical supplies, ventilators, Covid-19 testing supplies and personal protective equipment.

Earlier this year, as the pandemic gripped the US, personnel worked around the clock to deploy supplies, with trailer trucks on the standby for speedy distribution, according to David Allen, deputy chief for SNS Operational Logistics Branch.

The stockpile was never intended -- or funded -- to bear enough equipment for a pandemic, but it still became a point of contention between states and the administration, and eventually, prompted HHS to rethink the country's stockpile.
In January, there were 12 million N-95 masks -- which are, and continue to be, in high demand in total. As of December 18, overall, there are 194 million N-95 masks in inventory. There were similar surges with surgical masks, gowns and gloves. For example, there were 4 million gowns/ coveralls in the federal stockpile in January, compared to 173 million currently in inventory.
The administration is also investing half a billion dollars in domestic glove manufacturing, according to Paul Mango, deputy chief of staff for policy at HHS, referring to the steps the administration is taking to bolster the federal supply stockpile.
The replenishing of the Strategic National Stockpile -- and plans to improve it -- comes at a time when there's a significant increase in coronavirus cases across states and as hospitals try to proceed with elected procedures, which had previously been put on hold and similarly require personal protective equipment.
The worsening situation has again raised the question: Can the federal stockpile meet demand if supply shortages arise again? The short answer, according to HHS officials, is yes, citing new visibility into the supply chain and any chokepoints, as well as the flow of products currently coming in. Key to those efforts, officials say, is continuing to ramp up domestic production of supplies.
"We want to hand these on to the next administration and make sure America never has to go through what we went through again," Mango said.

Previously dubbed the National Pharmaceutical Stockpile, the idea behind the stockpile was to establish and maintain a sufficient supply of medicine and medical equipment in strategic locations around the US to be able to quickly help state and local communities in the wake of an attack with agents such as anthrax, smallpox, plague or other pathogens.
That Y2K attack never came. But the stockpile was tapped following another disaster soon thereafter: On September 11, 2001, planes delivering stockpile supplies to New York City were the only flights allowed in American skies other than military aircraft and Air Force One.
In the wake of 9/11, the stockpile was given its current name: Strategic National Stockpile. It was used again in the early 2000s in response to a series of anthrax attacks around the US and ultimately supplied with enough medication to treat up to 12 million people.

In the years since, the SNS has been used in response to a variety of disasters, from outbreaks of Zika, Ebola and botulism to flooding and major hurricanes, including Katrina, Sandy and Maria.

The Covid-19 pandemic put additional strain on the stockpile, since it didn't have the quantity of personal protective equipment and ventilators needed at the moment. To remedy that, HHS has shored up millions of items stored in warehouses nationwide, including the one CNN gained access to.

Experts agree that there's more inventory than had previously been stocked, but questions remain over how much is enough and whether stockpiling is the ultimate solution.

"There's more inventory in more categories than there ever has been in the stockpile," said Chaun Powell, who leads the disaster response team at Premier, a healthcare improvement company. "Stockpiling in general has contributed to the fact that we're in a better position. We still don't think stockpiling is a long term solution."

Instead, experts have floated more sophisticated IT solutions that provide visibility into the supply chain to identify where problems might crop up and which could allow for quicker solutions. Adams and Mango touted the progress the department has made in advancing systems to have more transparency into the supply chain.

The Biden transition team has also begun to engage with experts on supply preparedness, taking into future production, including whether use of the Defense Production Act is necessary, and stockpile needs, according to Powell who's been involved in discussions with the Biden transition team.

"They need to get a situational understanding of what's in it, what's on backorder, who they're contracting with," said Dr. Georges Benjamin, executive director of the American Public Health Association. "They need to get a bird's eye view of the whole national situation -- federal, state, local."

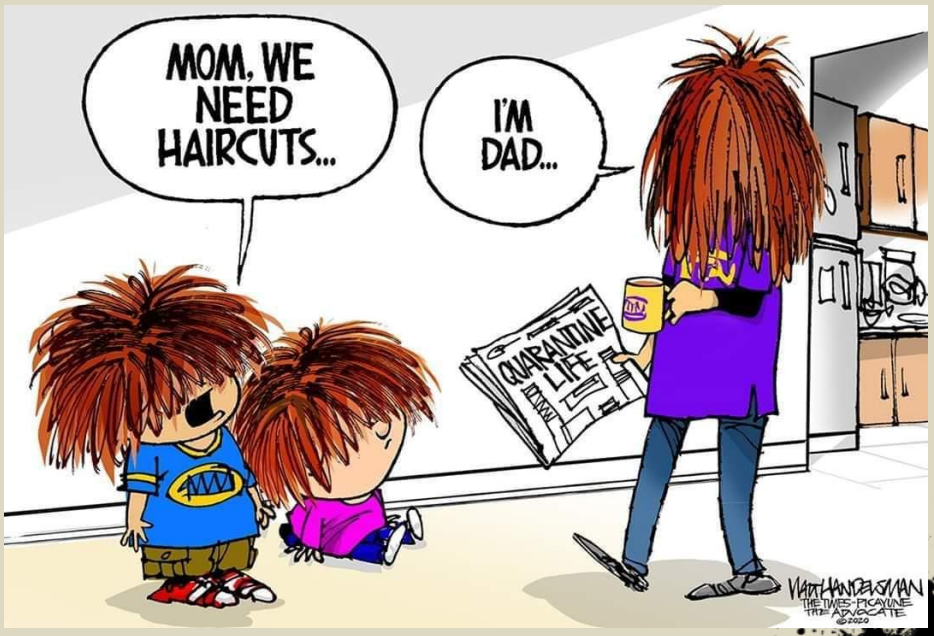
President Donald Trump repeatedly said it was incumbent on states, not the federal government, to meet local supply needs, but over time, the administration has worked toward bettering the stockpile to avoid shortages like those seen earlier this year. But Trump's comments also prompted states to build up their own supply stockpiles.

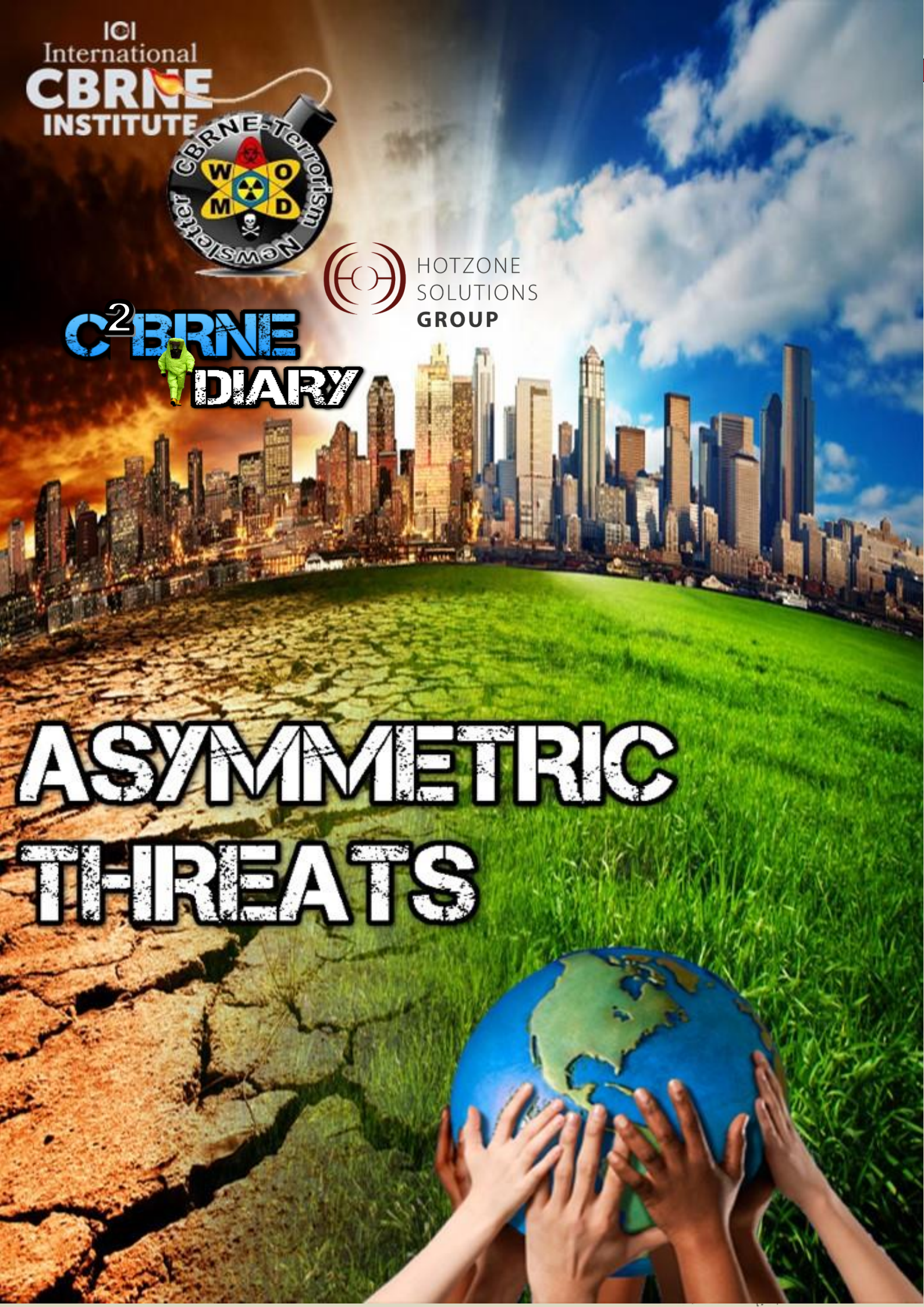
Steven Batson, South Carolina Emergency Management Division's chief of staff, told CNN the state has a 30-day stockpile for the first time -- an effort that started over the summer.

Batson said the state is "happy with the federal planning effort," adding, "Nothing like experiential learning to figure out what works and what doesn't."

Similarly, California has worked with private sector vendors to set up a supply stockpile "so that healthcare and essential workers in California do not face the same supply shortages and exorbitant pricing that has characterized the early days of the pandemic," according to Brian Ferguson, the deputy director for crisis communication and public affairs for Gov. Gavin Newsom's office.

If local capacity is exceeded, then states can rely on the federal supply stockpile. And this time, officials say, they're better prepared to respond to pandemic-related demands.




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

Understanding Contemporary Asymmetric Threats

By Nikola Brzica

Croatian International Relations Review 24(83):34-51(2018)

Source: https://www.researchgate.net/publication/328633110_Understanding_Contemporary_Asymmetric_Threats

Abstract

In the 21 st century, warfare has evolved into a challenge that many countries are ill prepared to face. In contrast to the warfare of yesterday, victory is not defined by defeating an opposing military force, but rather defeating their ability to pursue political objectives by violent, often unconventional, means. Increasingly, these unconventional means are based on asymmetries between the two opposing forces. A plethora of definitions for the term 'asymmetric conflict' exist, but they can largely be summarized by a general idea that one side in a conflict, due to its own failings or its opponents' strength, is unable to achieve its political aims through conventional (i.e. symmetric) military means. Because of this, the weaker side uses new ideas, weapons and tactics in a manner that is not expected, exploiting surprise to undermine the relative strength(s) of their opponent (Lele, 2014). The character of contemporary asymmetric threats can be analyzed through a framework of several key characteristics, which will be described in this paper. Understanding this framework, particularly in light of the horizontal transfer of technology, tactics, organization structure and procedures between emerging asymmetric threats may contribute to better understanding of such threats.

Should conventional terrorist bombings be considered weapons of mass destruction terrorism?

By Bryan R. Early, Erika G. Martin, Brian Nussbaum, and Kathleen Deloughery

Dynamics of Asymmetric Conflict Journal | Volume 10, 2017 - Issue 1 Pages 54-73

Source: https://www.tandfonline.com/doi/abs/10.1080/17467586.2017.1349327

Abstract

Since weapons of mass destruction (WMD) are typically thought of as chemical, biological, radiological, or nuclear (CBRN) weapons, the designation of conventional bombings as WMD terrorism under US law has generated controversy and can affect how policymakers plan for future attacks. Using quantitative data on terrorist attacks, federal planning documents, and the academic literature, we argue that placing the conventional terrorist bombings in the same legal category as CBRN terrorism confuses two distinct terrorist threats with different risks of occurrence, casualty profiles, consequences, and emergency response requirements. We explore the logical and practical reasons why such threat conflation could create policy problems. We conclude that the current definition of WMD terrorism under US law that aggregates conventional terrorist bombings with CBRN terrorism should be revised.

Hybrid Threats and Asymmetric Warfare: What to do?

By Col (ret) Karl Hickman (Swedish Defence University), Dr Mikael Weissmann (Swedish Defence University), Dr Niklas Nilsson (Swedish Defence University), Dr Sascha-Dominik Bachman (Bournemouth University), Dr Håkan Gunneriusson (Swedish Defence University) and Per Thunholm (Center for Asymmetric Threat Studies (CATS)

Conference Proceedings | February 2018

Source: https://www.diva-portal.org/smash/get/diva2:1186265/FULLTEXT01.pdf

Do we really need big war vessels in the Aegean Sea with hundrends of big and small islands?

Source: https://www.intracomdefense.com/

The Greek companies Intracom Defense (IDE) and Barracuda developped a USV designated USV-747. The vessel can operate with winds up to 7 Beaufort and has a range of 500nm. Its armament consists of either a 40mm grenade launcher, a .50cal MG or a light anti-submarine torpedo.

HOTZONE SOLUTIONS GROUP

HAPPY new year 2021

A holistic approach in CBRNe operations

Consultation

Products

Training

www.hotzonesolutions.org