# 2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

April 2019


www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

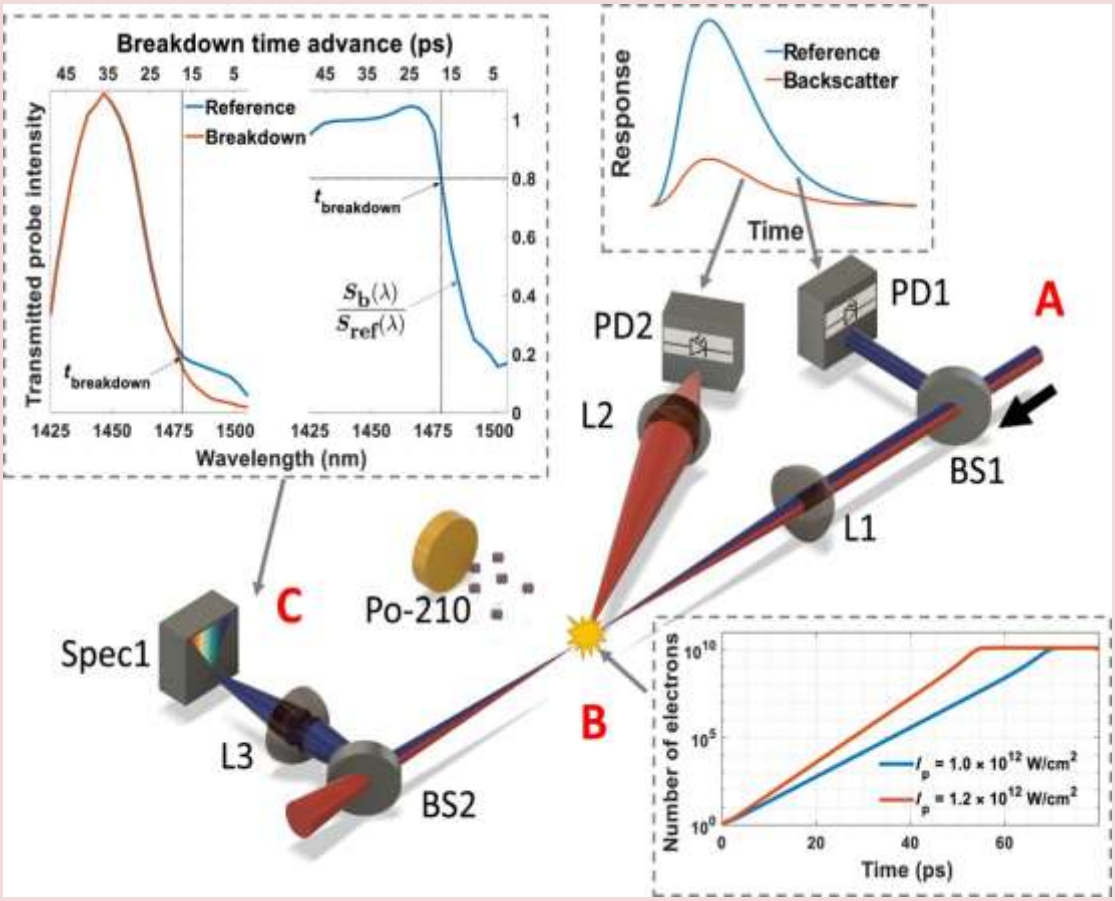
CBRNE-Terrorism Newsletter

C²BRNE DIARY

# DIRTY R-NEWS

# Detecting radioactive material remotely

Source1: http://www.homelandsecuritynewswire.com/dr20190325-detecting-radioactive-material-remotely
Source 2: http://advances.sciencemag.org/content/5/3/eaav6804




**(A)** Copropagating 50-ps (FWHM) λ = 3.9 μm pump and 70-ps (full width) chirped 1.45-μm probe pulses are generated in an OPCPA system (see Materials and Methods for details). Beamsplitter BS1 splits off >99% of the λ = 1.45 μm probe and sends it to PbSe photodetector PD1 for a probe pulse energy reference. This signal is also proportional to the λ = 3.9 μm pump energy (sample trace shown) because of the optical parametric amplification process. **(B)** Ionizing radiation (5.3-MeV α-particles) from an 18-mm-diameter Po-210 foil source generates a population of free electrons and $O_2^-$ ions in the focal region of lens L1, seeding collisional avalanche ionization driven by the λ = 3.9 μm pump. At lower average seed density, a seed electron is less likely to appear in a region of highest laser intensity in the focal volume, and thus, a local breakdown will take longer as shown in the simulation panel. The evolving avalanche breakdown plasma backscatters a portion of the λ = 3.9 μm pump pulse, which is collected by lens L2 onto PbSe photodetector PD2, with a sample trace shown. **(C)** The chirped λ = 1.45 μm probe is transmitted through the plasma, separated from the 3.9-μm pump by beamsplitter BS2 and collected by lens L3 onto InGaAs spectrometer Spec1. The spectral components of the chirped probe pulse correspond to specific time delays, as shown by the shared wavelength and time axis on the inset figure. The rapidly increasing plasma density cuts off the chirped probe at the breakdown time, taken to be the wavelength interval (and corresponding time) where the ratio $S_b(\lambda)/S_{ref}(\lambda)$ is reduced by 20%, where $S_{ref}(\lambda)$ is the probe reference spectrum and $S_b(\lambda)$ is the probe spectrum transmitted through the breakdown region.

Mar 25 – Physicists at the University of Maryland have developed a powerful new method to detect radioactive material. **By using an infrared laser beam to induce a phenomenon known as an electron avalanche breakdown near the material, the new technique is able to detect shielded material from a distance.** The method improves upon current technologies that require close proximity to the radioactive material.

With additional engineering advancements, the method could be scaled up and used to scan trucks and shipping containers at ports of entry, providing a powerful new tool to detect concealed, dangerous radioactive material. The researchers described their proof-of-concept experiments in a research paper published in the journal *Science Advances*.

"Traditional detection methods rely on a radioactive decay particle interacting directly with a detector. All of these methods decline in sensitivity with distance," said Robert Schwartz, a physics graduate student at UMD and the lead author of the research paper. "The benefit of our method is that it is inherently a remote process. With further development, it could detect radioactive material inside a box from the length of a football field."

As radioactive material emits decay particles, the particles strip electrons from—or ionize—nearby atoms in the air, creating a small number of free electrons that quickly attach to oxygen molecules. UMD says that by focusing an infrared laser beam into this area, Schwartz and his colleagues easily detached these electrons from their oxygen molecules, seeding an avalanche-like rapid increase in free electrons that is relatively easy to detect.

"An electron avalanche can start with a single seed electron. Because the air near a radioactive source has some charged oxygen molecules—even outside a shielded container—it provides an opportunity to seed an avalanche by applying an intense laser field," said Howard Milchberg, a professor of physics and electrical and computer engineering at UMD and senior author of the research paper. "Electron avalanches were among the first demonstrations after the laser was invented. This is not a new phenomenon, but we are the first to use an infrared laser to seed an avalanche breakdown for radiation detection. The laser's infrared wavelength is important, because it can easily and specifically detach electrons from oxygen ions."

Applying an intense, infrared laser field causes the free electrons caught in the beam to oscillate and collide with atoms nearby. When these collisions become energetic enough, they can rip more electrons away from the atoms.

"A simple view of avalanche is that after one collision, you have two electrons. Then, this happens again and you have four. Then the whole thing cascades until you have full ionization, where all atoms in the system have at least one electron removed," explained Milchberg, who also has an appointment at UMD's Institute for Research in Electronics and Applied Physics (IREAP).

As the air in the laser's path begins to ionize, it has a measurable effect on the infrared light reflected, or backscattered, toward a detector. By tracking these changes, Schwartz, Milchberg and their colleagues were able to determine when the air began to ionize and how long it took to reach full ionization.

"Timing of ionization is one of the most sensitive ways to detect initial electron density," said Daniel Woodbury, a physics graduate student at UMD and a co-author of the research paper. "We're using a relatively weak probe laser pulse, but it's 'chirped,' meaning that shorter wavelengths pass though the avalanching air first, then longer ones. By measuring the spectral components of the infrared light that passes through versus what is reflected, we can determine when ionization starts and reaches its endpoint."

The researchers note that their method is highly specific and sensitive to the detection of radioactive material. Without a laser pulse, radioactive material alone will not induce an electron avalanche. Similarly, a laser pulse alone will not induce an avalanche, without the seed electrons created by the radioactive material.

While the method remains a proof-of-concept exercise for now, the researchers envision further engineering developments that they hope will enable practical applications to enhance security at ports of entry across the globe.

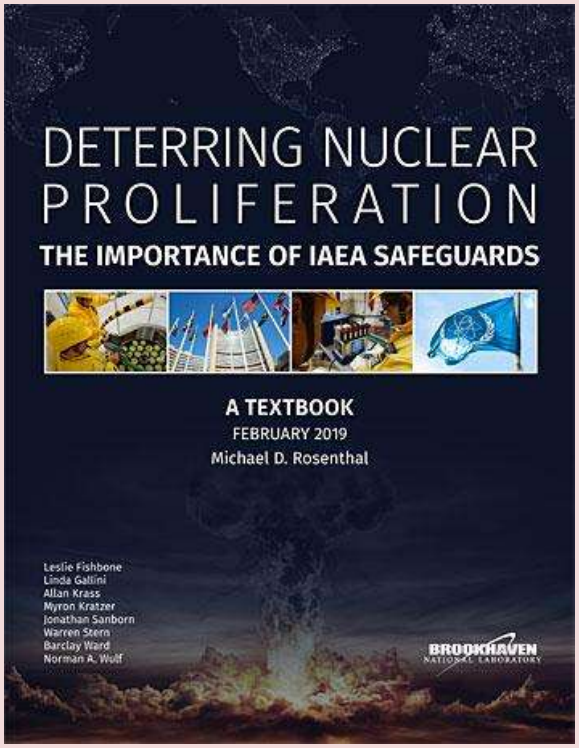
"Right now, we're working with a lab-sized laser, but in 10 years or so, engineers may be able to fit a system like this inside a van," Schwartz said. "Anywhere you can park a truck, you can deploy such a system. This would provide a very powerful tool to monitor activity at ports."

*— Read more in Robert M. Schwartz et al., "Remote detection of radioactive material using mid-IR laser–driven electron avalanche," Science Advances 5, no. 3 (22 March 2019).*

# Second edition of Nuclear Nonproliferation Textbook

Source: http://www.homelandsecuritynewswire.com/dr20190325-second-edition-of-nuclear-nonproliferation-textbook

Mar 25 – The U.S. Department of Energy's (DOE) Brookhaven National Laboratory published the second edition of *Deterring Nuclear Proliferation: The Importance of IAEA Safeguards*. The textbook provides a history of the origins of the International Atomic Energy Agency (IAEA) and an introduction to the ways in which IAEA verifies nation states' nuclear nonproliferation commitments.




"This book will benefit students studying or professionals working in the field of nuclear nonproliferation, and it will give anyone entering the field a running start," said primary author and Brookhaven Lab contractor Michael Rosenthal, who formerly served as head of Brookhaven's Division of Nonproliferation and Safeguards and as a member of the Senior Executive Service within the U.S. Department of State and U.S. Arms Control and Disarmament Agency.

Rosenthal and the other co-authors—Leslie Fishbone, Linda Gallini, the late Allan Krass, Myron Kratzer, Jonathan Sanborn, Warren Stern, Barclay Ward, and Norman Wulf—are all experts in nuclear nonproliferation and international security. They have played key nonproliferation roles at the IAEA, U.S. Department of State, U.S. Atomic Energy Commission, U.S. Arms Control and Disarmament Agency, Brookhaven, and universities.

Brookhaven says that the new edition describes important changes to the implementation of IAEA safeguards since the first edition was published in 2013. Safeguards are technical measures for verifying that states are honoring their international legal commitments to the peaceful use of nuclear energy. Traditionally, the safeguards approach focused primarily on the monitoring of nuclear facilities. Today, the IAEA has adopted a state-level approach, which takes into account a state's nuclear, and nuclear-related, activities and capabilities as a whole.

The second edition also chronicles the IAEA's role in implementing safeguards in Iran. The section includes a historical look at the sequence of events that culminated in the negotiation of a multilateral agreement that places strict bounds on Iran's nuclear program. The IAEA continues to verify that Iran is complying with its international and multilateral commitments to limit its nuclear program to peaceful purposes.

The book has been praised by several leaders engaged in efforts to ensure the nonproliferation of nuclear weapons.

"Today, policymakers and practitioners who lack basic understanding of the history, rationale, and technical details of the complex architecture of the international nuclear nonproliferation regime and the role of the IAEA safeguards system are grappling with urgent proliferation challenges with one arm tied behind their back," said Ambassador Susan Burk, former Special Representative of the President of the United States for Nuclear Nonproliferation. "Fortunately, *Deterring Nuclear Proliferation: The Importance of IAEA Safeguards,* fills that knowledge gap. It is a unique resource for understanding the IAEA and is a must-read for security professionals developing and implementing U.S. nuclear nonproliferation policy, and for anyone interested in understanding how the nonproliferation regime that we take for granted works to reduce nuclear dangers."

According to Daryl G. Kimball, executive director of the Arms Control Association and publisher of the journal Arms Control Today, "The latest edition of *Deterring Nuclear Proliferation: The Importance of IAEA Safeguards* is an invaluable, comprehensive guide to the evolving nuclear safeguards system that undergirds the international nuclear nonproliferation regime. Whether you are a scholar or researcher, a diplomat, a regulator, a student, or an expert practitioner, you will find this book to be a valuable and authoritative resource."

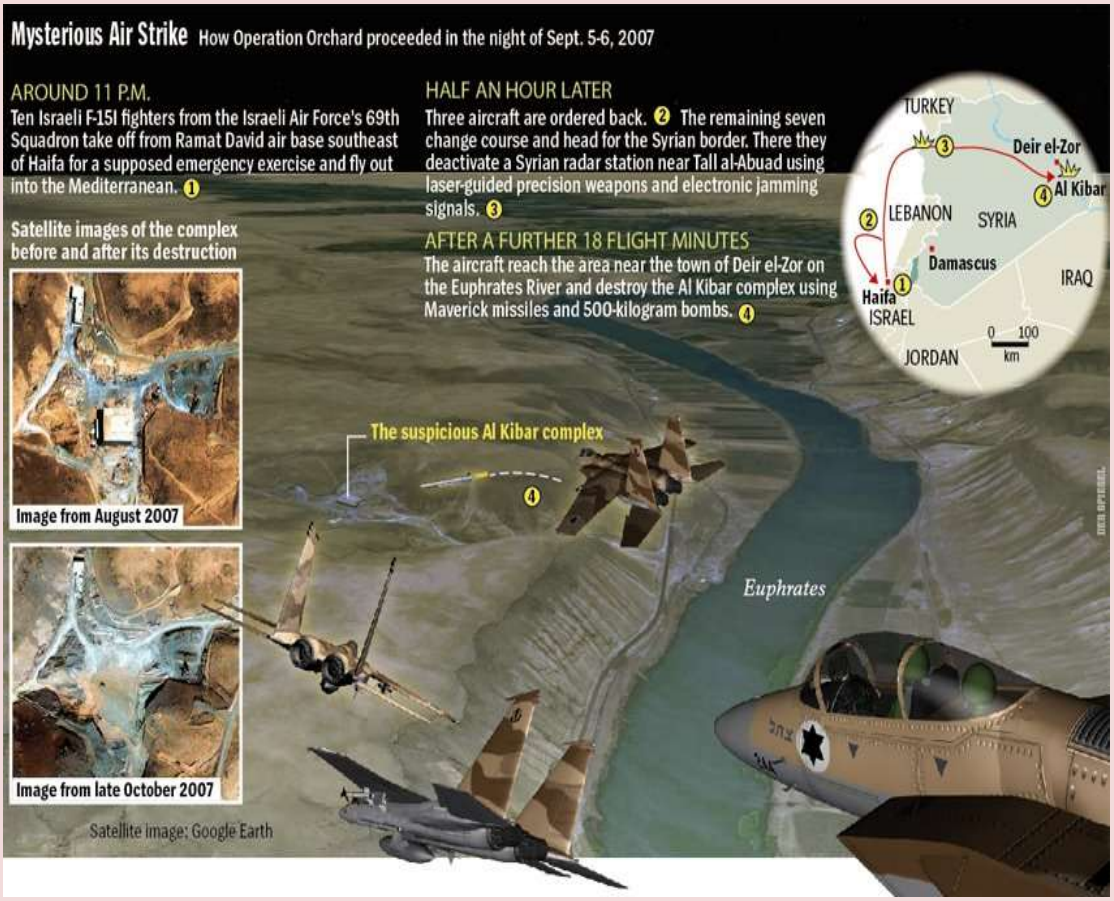
And Christian Kessler, who was a senior U.S. State Department official and nuclear expert, adjunct professor at the University of Washington and Stony Brook University, and member of the U.N. Security Council's Panel of Experts on Iran, wrote, *"Deterring Nuclear Proliferation: The Importance of IAEA Safeguards* examines the legal, political, and technical factors that shaped evolution of the international system to halt the spread of nuclear weapons, written by a team of experts who helped shape that evolution. Both detailed and comprehensive, it is a unique and uniquely authoritative resource for scholars, educators, and students seeking to learn how we got from Hiroshima to today."

A pre-release version of the book is available for download as a free e-book by individuals with .gov and .edu email addresses. Brookhaven notes that if people who do not have a .gov or .edu email address but intend to use the book for governmental or educational purposes, should request a copy from wstern@bnl.gov.

## Did Israel destroy Syria's nuclear weapons program?

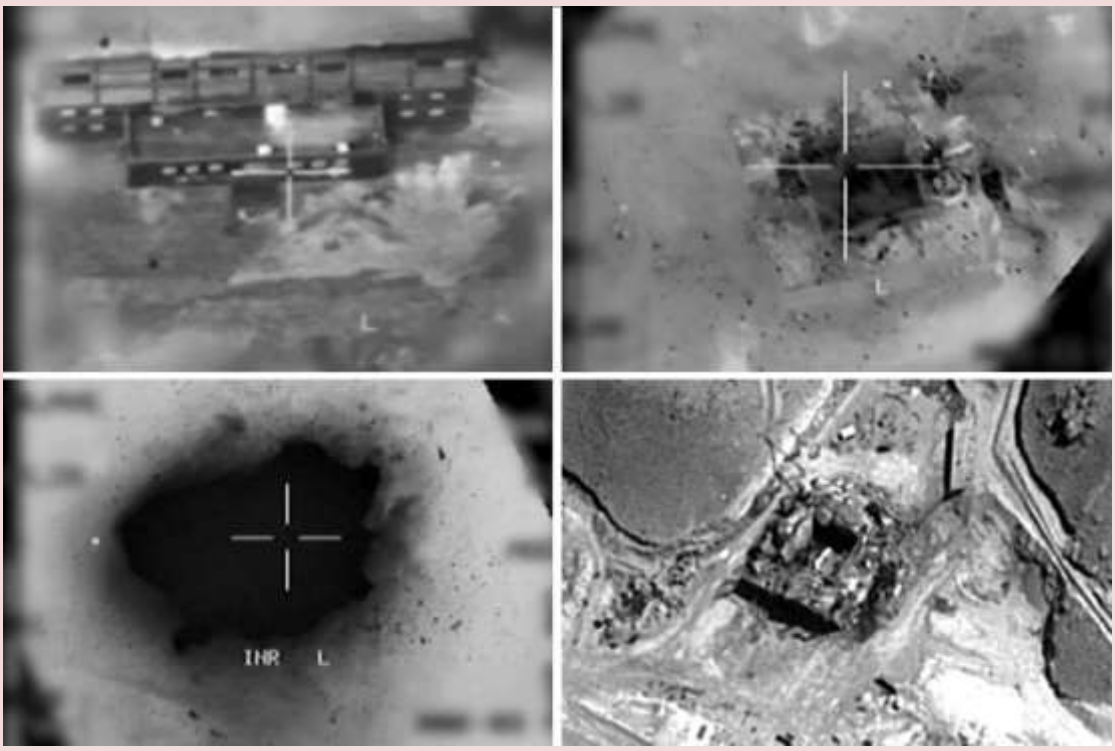
Source: https://www.almasdarnews.com/article/did-israel-destroy-syrias-nuclear-weapons-program/

Apr 07 – Israel put an end to Syria's alleged nuclear ambitions in 2006 when they bombed the country's secret site near the Iraqi border.
Dubbed "Operation Orchard" or "Operation Outside the Box", Israeli F-15 and F-16 warplanes bombed an alleged nuclear site some 30 kilometers outside of Deir Ezzor city in Syria's eastern region.




While Israel kept this attack quiet for over a decade, they finally broke their silence in March 2017 when they claimed responsibility for the bombing. General Ali Reza Askari first confirmed the bombing in 2007 after he defected to the United States in 2007.

"Askari provided highly valuable information. Among other things, he reported details about the Syrian nuclear program that had been financed by Iran and built by the North Koreans. They were constructing




a graphite-moderated reactor named Al Kibar that was supposed to produce weapons-grade plutonium," tbe War is Boring publication claimed.
While the U.S. did not play a part in the Israeli bombing of the alleged nuclear site, they did monitor the attack using their electronic surveillance equipment.

**The Attack**
According to War is Boring, the Israeli special forces commando from the IDF's most elite unit, Sayeret Matkal, managed to infiltrate and collect intelligence at the nuclear construction site.
"On Sept. 5, after weeks of clandestine political debates in Israel's security cabinet, the IDF got the green light for Operation Orchard. In the same night, 10 F-15 and F-16 fighter jets took off at Israel's Ramat David air base. First, they flew northwards along the Mediterranean coast, and then suddenly, they turned east along the Syrian-Turkish border. Blinding Syrian air-defense systems with electronic countermeasures and destroying a radar station, they entered into Syria's air space," the publication, the publication claimed, adding that "around 12:45 in the morning, the pilots reported the successful execution of the operation. The Syrian nuclear reactor was destroyed before it could go online. The Israeli war planes returned home unharmed."

**Syria's Response**
Syria officially denied the site was a nuclear facility, despite a great deal of speculation regarding the Israeli attack.
"Is it logical? A nuclear site did not have protection with surface to air defences? A nuclear site within the footprint of satellites in the middle of Syria in an open area in the desert?" Syrian President Bashar Al-Assad told Qatar's al-Watan newspaper in an interview shortly after the Israeli attack.
"The truth is that the raid was at a military site under construction," Assad said in the interview. "We are against mass destruction weapons for Israel, Iran or others."
"Where would we use it? On Israel it would kill the Palestinians. I do not see this as logical," the Syrian President said, adding "why did they raid it, we do not know what data they had,

but they know and they see through satellites; they have raided an incomplete site that did not have any personnel or anything. It was empty."
The Syrian government has maintained that this facility was never used for nuclear research or the development of these weapons, despite Israel's claims.

**Today**
As of today, the site is currently under the control of the Syrian Democratic Forces (SDF) who managed to capture the area during an offensive against the Islamic State (ISIS/ISIL/IS/Daesh).
While the site is out of Syrian government control in eastern Syria, it still remains somewhat intact.
As seen in Israel's recent attacks on Damascus and Homs, the Syrian government has quite a few sites that are masked as construction sites, which could have indeed been military research buildings.
Furthermore, Israel's attack on the Osirak Nuclear Reactor near Baghdad in 1981 showed their meticulous research and willingness to prevent their enemies from attaining nuclear capabilities.
Since Deir Ezzor is quite far from their border, as was the Osirak Nuclear Reactor, Israel would be taking a major risk to hit a construction site without some kind of proof that it is being used to produce internationally prohibited weapons.
What exactly was being developed at this site in eastern Deir Ezzor is up for debate; however, it appears Israel had known about it for quite some time before actually attacking it.

## First satellite images of Saudi nuclear plant show completion

Source: https://www.globalsecurity.org/wmd/library/news/saudi/saudi-190403-presstv01.htm

Apr 03 – New satellite images show that Saudi Arabia has almost completed the building of its first nuclear reactor, according to a report by Bloomberg written based on the images by Google Earth.

The report, published on Wednesday, noted that the construction of the facility, which is located in the southwest corner of the King Abdulaziz City for Science and Technology in Riyadh, is alarming, because the country has not accepted the international rules and frameworks needed to ensure that civilian atomic programs aren't used to build weapons.

"There's a very high probability these images show the country's first nuclear facility," former International Atomic Energy Agency (IAEA) director Robert Kelley told Bloomberg. "It means that Saudi Arabia has to


get its safeguards in order."

Meanwhile, Bloomberg quoted the Saudi energy ministry as saying in a statement that the facility is being built with transparency and is in full compliance with the international agreements.

Saudi Arabia has signed the IAEA's so-called Small Quantities Protocol, but it hasn't adopted the rules and procedures that would allow nuclear inspectors to access potential sites of interest.

This comes as a bipartisan group of American lawmakers have raised concerns about Washington's nuclear dealings with Saudi Arabia.

In a letter drafted to US Energy Secretary Rick Perry on Tuesday, Senators Robert Menendez, the senior Democrat on the Senate Foreign Relations Committee, and Republican committee member Marco Rubio questioned the recent approvals for American companies to share nuclear energy information with Saudi Arabia.

The senators specifically pointed to Riyadh's insistence on forgoing Washington's so-called 123 agreement, a set of nonproliferation standards required by Section 123 of the US Atomic Energy Act of 1954.

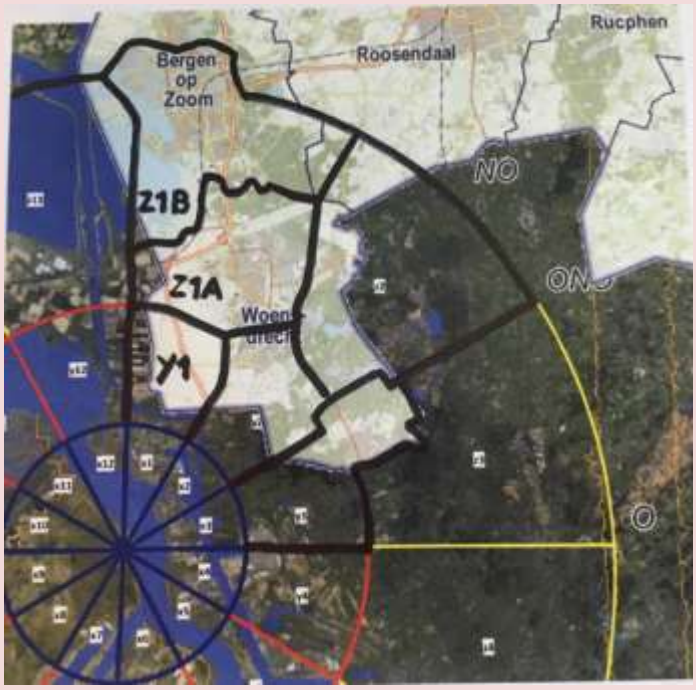
The 123 agreement, often referred to as Washington's "gold standard" for foreign civil nuclear cooperation, prevents the foreign entity from enriching uranium or reprocessing plutonium made in reactors - two routes to making nuclear weapons.

Negotiations between the US and Saudi Arabia for nuclear cooperation came to a halt under the administration of former President Barack Obama, after Riyadh refused to accept Washington's proposed standards.
In its never-ending quest for more money, the administration of President Donald Trump resumed the talks and is reportedly considering a deal that would allow Riyadh to enrich and reprocess uranium and pave the way for American companies to build nuclear reactors in the kingdom.
In February, a report by a congressional committee revealed that the Trump administration was trying to bypass Congress to transfer sensitive nuclear power technology to Saudi Arabia.
Iran's Foreign Minister Mohammad Javad Zarif at the time decried the US "hypocrisy" over the planned nuclear sale to the Saudi regime.
In March 2018, Saudi Crown Prince Mohammed bin Salman said that the kingdom would be quick to develop nuclear weapons if Iran – which Riyadh views as its arch rival in the region – did so.
Iran does not pursue nuclear weapons, and under a 2015 international deal, it has placed its entire nuclear program under enhanced 24/7 monitoring by the United Nations' atomic watchdog, which has repeatedly confirmed the peaceful nature of Iran's nuclear program.

## Case Study: Lessons from the Evacuation of Chernobyl's Area

**By Thorsten Hackl**
Source: http://nct-magazine.com/nct-magazine-april-2019/case-study-lessons-from-the-evacuation-of-chernobyl-area/

I am not sure why I keep returning to this place. We walk around the deserted village. Stray dogs are following us, but we don't mind. This is our fifth visit to the exclusion zone in 6 years. Every year we organize a study trip for radiation protection experts and CBRN experts and we try to show them what happened and why it did happen. We follow our guide around the abandoned buildings. We visit the docks, where we find some hot spots near the harbor house and on the lake we see the wrecks of ships in the distance. After visiting the town square and the swimming pool, we drive to the reactor building. On our way, we pass reactors 5 and 6, which were under construction at the time of the incident. In the reactor we visit the control room, the turbine hall and several other places. Our dosimeters keep beeping. We are not worried, as we are all radiation protection experts. We are however fascinated, walking through the catacombs of the world's most famous reactor. In a way we feel like dark tourists, visiting a place where a terrible tragedy took place. On the other hand, we feel like fanatics, who want to know as much as possible about the disaster and the consequences.




In 2003, I started working in the field of nuclear safety when I became a radiation protection expert for the fire department of Mid-West Brabant in the Netherlands. In the Netherlands we have a few nuclear reactors for scientific purposes and only one for nuclear energy. South of the Netherlands, there are 4 reactors in Doel, Belgium. When the wind comes from the South West, The Netherlands could receive the possible plume from a reactor incident at one of those reactors. That is the reason why our fire department wanted to have a trained radiation protection expert. Over the years nothing really bad happened,

and I did my retraining during several exercises and visited some courses abroad in Belgium (SCK) and Vienna (IAEA).

**▶▶ Read the rest of this article at source's URL.**

***Thorsten Hackl*** *became a fire officer in 1999 and specialized in hazardous materials incident management. He is an active on duty Hazmat Scientific Officer. In 2003 he became a Radiation Protection expert for the South of The Netherlands. Mr. Hackl loves training people in hazmat and nuclear safety and trained +1000 first responders. Next to firsts responders, he trained incident commanders, hazmat advisors and other rescue personnel. He have participated in several national exercises concerning nuclear safety. And since 2009 Mr. Hackl is an active member in the EU Civil Protection Mechanism. He has trained CBRN modules during EU exercises and was an Observer at the Curiex 2013 nuclear exercise in Spain. Over the years Mr. Hackl worked for the national nuclear authority (ANVS), he has been manager at a dispatch center and went on mission for the IAEA. In 2017 he lead a team of Dutch experts on an Emergency Preparedness and Response mission to Fukushima.*

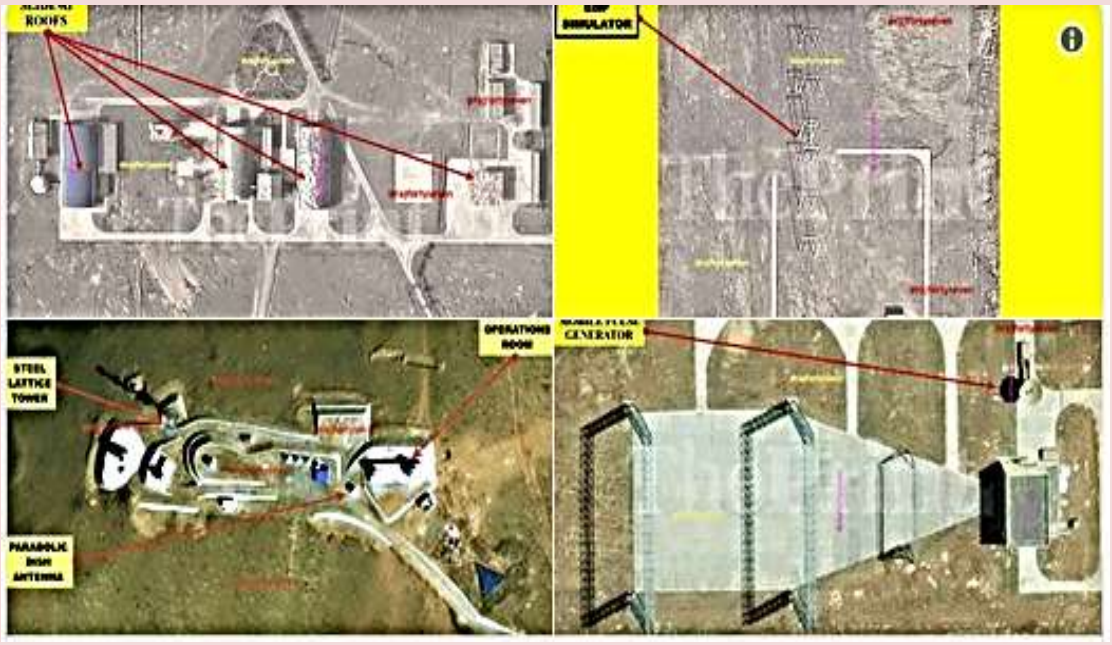
## As China Talks Peace in Space, Researcher Shows Secret Chinese Anti-Satellite, EMP Bases

**By Joshua Philipp**

Source: https://www.theepochtimes.com/as-china-talks-peace-in-space-researcher-shows-secret-chinese-anti-satellite-emp-bases_2868172.html

Apr 12 – Satellite imagery has revealed a secret anti-satellite weapons base in China, as well as electromagnetic pulse (EMP) weapons testing facilities. This news is making the rounds online even as the Chinese regime is criticizing India for its space weapons programs, and is calling for peace in space.

The discovery was made by retired Indian Army Col. Vinayak Bhat, who specializes in satellite image analysis focused on China. He noted in India's The Print news website that the Chinese Communist Party (CCP) now has several of these facilities, including in Tibet and Xinjiang.




Bhat wrote that the facilities have tracking equipment, and it is believed the anti-satellite laser weapons stationed in buildings with sliding roofs can be used for varying purposes that include blinding or destroying satellites.

The EMP weapons facilities, meanwhile, appear to be for testing. They include some simulated electrical infrastructure and nearby facilities housing the weapons. Included in one image is what appears to be a mobile EMP generator.
These images are being circulated just after India tested an anti-satellite missile and destroyed a satellite March 27. The test sent debris hurtling through orbit.
After the recent test, the CCP came out playing the peacekeeper. According to The Times of India, Chinese Foreign Ministry spokesman Hong Lei said at a press conference, "Outer space is shared by the entire mankind. Every country has the right to make peaceful exploration and use of outer space."
In reality, the CCP has been highly aggressive with its military space programs. It tested its first anti-satellite weapon in May 2005, and shocked the space community in 2007 when it used a missile to destroy its Feng Yun 1-C weather satellite, and sent over 3,000 pieces of debris into low-earth orbit.
The CCP has continued testing its anti-satellite weapons since then, and the secret laser weapons facilities revealed by satellite imagery are just small pieces of the bigger picture.
In its 2015 Annual Report to the Congress, the U.S.-China Economic and Security Review Commission warned that "China's recent space activities indicate that it is developing co-orbital anti-satellite systems to target U.S. space assets."
Militarily, space is regarded as the "ultimate high ground." Weapons placed in orbit could allegedly target missiles on earth as they launch, nuclear weapons could be detonated in orbit for destructive EMP without the need for launch, and satellites crucial for military communications and targeting can be destroyed.
Under the CCP's unconventional warfare programs designed to destroy the weakest links of the U.S. military, weapons of these types are regarded as highly valuable. CCP military doctrine such as its Assassin's Mace or "Trump Card" program describe such weapons directly.
In 2014, Chinese Ret. Lt. Gen. Wang Hongguang threatened the United States with these weapons systems in the CCP's state-run Global Times news outlet. Wang said that the CCP would use these weapons suddenly, and warned Americans in their "pride and arrogance" to "not get trampled beneath us."
Public information on the CCP's Assassin's Mace weapons are thin, but a 2011 report from the National Ground Intelligence Center said, "These modern Trump Card and Assassin's Mace weapons will permit China's low-technology forces to prevail over U.S. high-technology forces in a localized conflict."
According to a recent Government Accountability Office report, on April 3, little has changed. It says, "China and Russia in particular are developing a variety of means to exploit perceived U.S. reliance on space-based systems and challenge the U.S. position in space."
It's in this context that President Donald Trump signed an executive order on March 26 to harden U.S. critical infrastructure to protect against EMP attacks. It's also in this context that Trump is pushing for a Space Force military branch that would consolidate U.S. military space programs.

***Joshua Philipp*** *is an award-winning investigative reporter and a senior editor at The Epoch Times. He is a recognized expert on unrestricted warfare, asymmetrical hybrid warfare, subversion, and historical perspectives on today's issues. His 10-plus years of research and investigations on the Chinese Communist Party, subversion, and related topics gives him unique insight into the global threat and political landscape.*

## Are 'Game of Thrones's' dragons the equivalent of nuclear weapons? We don't think so.

**By Michael C. Horowitz and Matthew Fuhrmann**
Source: https://www.washingtonpost.com/politics/2019/04/12/are-game-throness-dragons-equivalent-nuclear-weapons-we-dont-think-so/

Apr 12 – In case you haven't heard, "Game of Thrones" returns to HBO on Sunday for its final six episodes. Political science has had a lot to say about the series, from alliance politics in the War of the Five Kings to questions of gender and regime type. It can also help us understand the role of the show's three dragons: Drogon, Rhaegal and Viserion.

George R.R. Martin, the author of the books that inspired the TV series, once referred to dragons as the "nuclear deterrent" of Westeros. In this view, dragons, like nuclear weapons, deter others from attacking, because they can cause mass destruction by raining fire from above. As we saw in the last season, Jamie Lannister hesitated to take his army to war against Daenerys Targaryen's dragon-outfitted forces, since doing so would have resulted in large-scale carnage.

However, if we look closely at actual uses of dragons, we find that they more closely resemble conventional air power, as we explain below.

**Dragons are used on the battlefield — not just for deterrence**

The idea behind nuclear deterrence is that nuclear weapons are so destructive that simply threatening to use them, implicitly or explicitly, prevents others from attacking you — so they never actually have to be used.

But that's not how things go with dragons.

Our team analyzed data on the political-military use of dragons in the "Game of Thrones" universe, collecting information on nearly 100 battles across the TV show and books. Dragons were used in 26 percent of these battles.

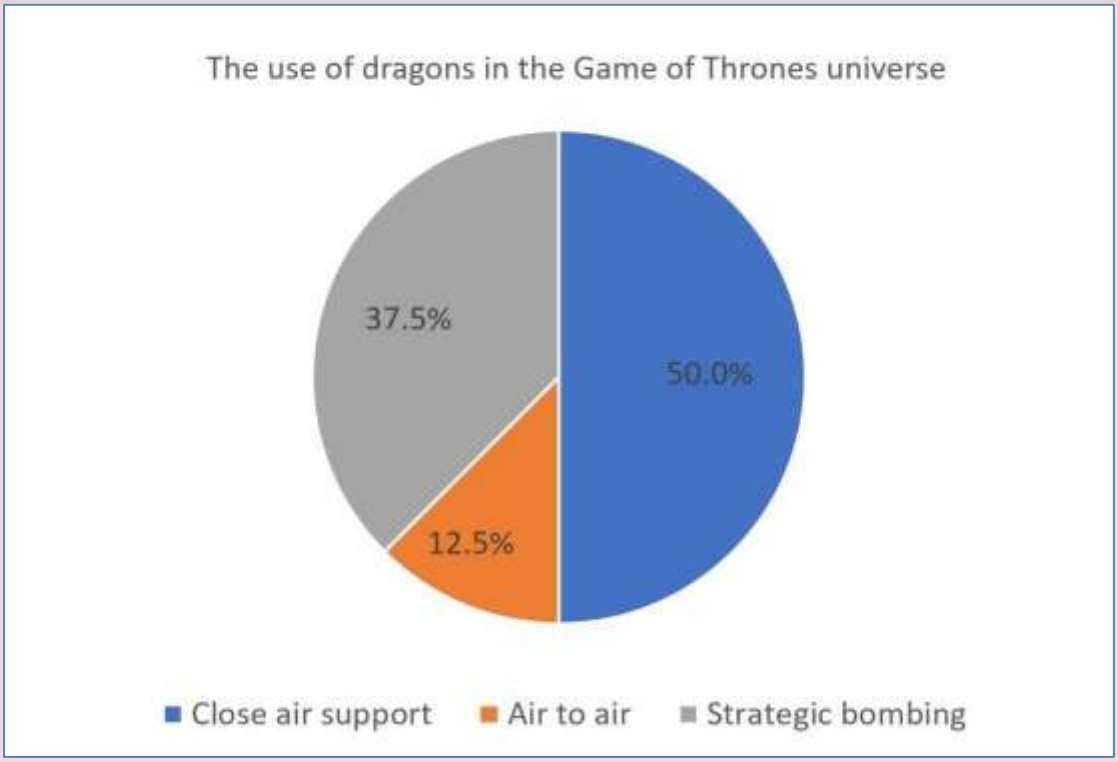
Those who had dragons used them in three main ways.

First, dragons were deployed to support troops on the battlefield — "close air support," in military parlance — half the time. For example, in the Battle of the Goldroad (Season 7, Episode 4), better known as the "Loot Train" battle, Daenerys rides Drogon to destroy the Lannister forces that sacked Highgarden. But they're not used alone; they're air support for Dothraki riders, Daenerys's mounted cavalry.

Second, dragons were used in strategic bombing campaigns against castles or cities to achieve some political goal nearly 38 percent of the time. For instance, as described in "The World of Fire & Ice," Aegon the Conqueror used the dragon Balerion to burn Harrenhal and kill his adversary King Harren during the Conquest.

Third, in about 13 percent of cases, dragons were used in air-to-air combat against opposing dragons — primarily in the Dance of the Dragons, a Westerosian civil war about 175 years before the events depicted in the TV show.

Nuclear weapons, by contrast, primarily serve as a deterrent. They have not been used in combat since the U.S. bombings of Hiroshima and Nagasaki in August 1945.




Dragon use in battles in the "Game of Thrones" universe. (Michael C. Horowitz and Matthew Fuhrmann /Michael C. Horowitz and Matthew Fuhrmann)

**Dragons are less destructive and more vulnerable than nuclear weapons**

Just one nuclear weapon causes massive devastation. The bomb the United States dropped on Hiroshima, known as "Little Boy," killed or injured an estimated 136,000 people. Conventional bombings can inflict lots of carnage, too — but not as swiftly. The U.S. bombing of Tokyo in March 1945, one of the most destructive conventional bombing raids ever, involved 325 bombers.

Dragons are more like conventional air power, requiring many passes to deliver destruction — much as an air force sends out many bombers on bombing runs. For example, in the Field of Fire battle that consolidated Aegon's Conquest, Aegon used the three Targaryen dragons to compensate for the numerical inferiority of his ground forces.

Dragons are also more vulnerable than nuclear weapons. There exists no defense against a nuclear weapon — only against the methods that deliver them, such as missiles, bombers or submarines. Dragons, however, like bombers, are vulnerable to anti-air attacks, such as Scorpion artillery pieces, which resemble enormous crossbows. A Dornish scorpion brought down the dragon Meraxes during the First Dornish War. And in Season 7 Episode 6, The Night King uses the most accurate javelin toss ever to kill the dragon Viserion.

**Dragons don't create mutually assured destruction**

Until very late in last season, Daenerys's forces had a decided edge against all other armies because she possessed the only three known living dragons. But the Night King has a dragon as well, which he acquired by killing and then raising Viserion from the dead. And as season 7 ended, Viserion's blue flames destroyed a portion of the Wall, changing the balance of power.

What does this mean for peace and stability in Westeros?

Many believe that nuclear weapons bring stability through mutually assured destruction (MAD) — the idea that since war between two nuclear-armed adversaries would destroy both, each side avoids picking a fight. According to this view, MAD explains why the Cold War between the United States and the Soviet Union did not turn hot.

However, MAD will not work in Westeros. Armies can limit the damage caused by a dragon with Scorpion bolts or another dragon, so mass destruction is hardly inevitable. And the Night

King seems bent on war regardless of how many casualties his undead army may suffer. Even if he were not, Cersei Lannister has made clear that she's prepared to fight with her mercenary army for continued power. At least one major war is coming.
What will it look like? In season 2 (A Clash of Kings in the books), Daenerys has a vision in the House of the Undying that shows a destroyed, snow-topped Iron Throne room in King's Landing. Many other visions have come to pass; this one may as well. But if it does, what burns the roof off the throne room? A dragon is most likely, though either Daenerys or the Night King could pilot the attack.
Whatever Season 8 has in store, remember that dragons, like any form of air power, cannot win a war alone. Simply having the most destructive weapon in the land doesn't guarantee political victory. That requires an army that can take and hold territory. Like everyone else watching, our question is: Whose will it be?

***Michael C. Horowitz*** *is professor of political science and the associate director of Perry World House at the University of Pennsylvania.*
***Matthew Fuhrmann*** *is professor of political science at Texas A&M University*
*The authors would like to thank Lauren Kahn, Ali Khambati and Alexander Rabin for their research assistance.*

## South Africa a Shining Example of Dismantling Nuclear Arsenal

Source: https://www.indepthnews.net/index.php/the-world/africa/2617-south-africa-a-shining-example-of-dismantling-nuclear-arsenal

As the nuclear weapons and fossil fuel divestment campaigns gather steam, their political impact could be as powerful as the divestment campaign against South Africa in the late 20th Century, which was a critical factor in moving the South African government to end apartheid in 1994, anticipates Thies Kätow, researcher for the World Future Council.
There are hardly any signs that such an expectation will be realized and the campaign under way would persuade heavily armed nuclear states to disarm. Yet South Africa remains a shining example of a country that went from developing its own nuclear arsenal to dismantling it and being an outspoken advocate against these weapons of mass destruction.
The Central Asian republic of Kazakhstan also dismantled and destroyed nuclear weapons systems and facilities – but these were inherited Soviet Union when it collapsed.
South Africa reaffirmed its commitment 25 years after scrapping its nuclear program when it took another vital step towards a nuclear-weapons-free-world by ratifying on February 25, 2019 the UN Treaty on the Prohibition of Nuclear Weapons (TPNW) at the UN Headquarters in New York.
South Africa had signed the TPNW on September 20, 2017

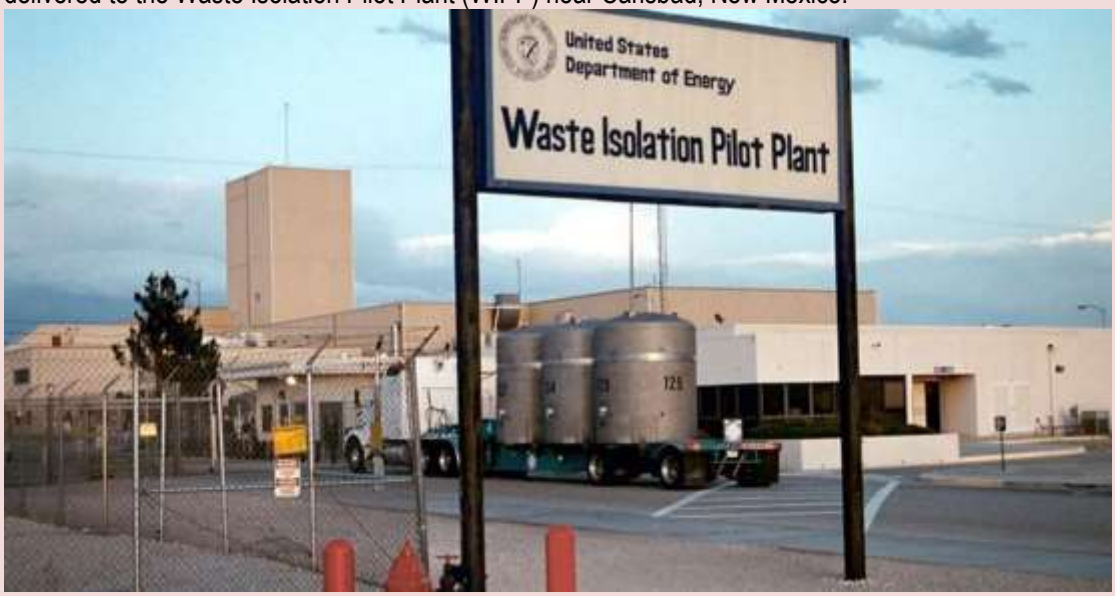
Uranium-rich apartheid South Africa was interested as early as 1948 in atomic energy, and the mining, trade and energy industry that could be built around it. The government bought its first reactor from the U.S. in 1957.
The apartheid government developed a three-stage deterrence strategy in 1978, fearing a direct invasion or an invasion of South African-controlled Namibia by Soviet-backed forces.
However, as the Nuclear Threat Initiative (NTI) points out, the departure of Cuban forces from Angola, Namibia's independence, and the dissolution of the Soviet Union enabled South Africa to abandon its nuclear weapons program in 1989. Isolated from the global economy, the government also recognized that South Africa would benefit more from giving up its nuclear weapons program than maintaining it.
Following the dismantlement of South Africa's nuclear weapons, the national 1993 Non-Proliferation of Weapons of Mass Destruction Act committed South Africa to abstain from developing nuclear weapons.
While officially the purpose of the nuclear explosion program did not change from peaceful to military purposes until 1977, U.S. intelligence reports show that South Africa formally began its nuclear weapons program in 1973.
Initially, heavy international pressure kept them from testing these weapons. But by 1982, South Africa had developed and built its first nuclear explosive device. By 1989, South Africa had 6 bombs, each containing 55kg of HEU (highly enriched uranium), capable of delivering an explosive equivalent of 19 kilotons of TNT.
In 1989, the government officially ended the nuclear program, and South Africa joined the Non-Proliferation Treaty (NPT) as a non-nuclear-weapon state in 1991. By 1994, the International Atomic Energy Agency (IAEA) confirmed that all of South Africa's nuclear weapons had been dismantled.
South Africa has been champion a world without nuclear weapons ever since. On April 11, 1996, the country joined other African nations to sign the Treaty of Pelindaba to create a Nuclear-Weapons-Free Zone on the African continent.
The African Commission on Nuclear Energy (AFCONE) – established for the purpose of ensuring States Parties' compliance with their undertakings in the Treaty – is based in Pretoria. On September 24, 1996 South Africa signed the Comprehensive Nuclear Test Ban Treaty (CTBT) and ratified it in 1999.
Besides, South Africa is member of the New Agenda Coalition (NAC) in support of a nuclear weapons free world. The origin of the NAC goes back to June 1998 when the foreign ministers of Brazil, Egypt, Ireland, Mexico, New Zealand, Slovenia, South Africa, and Sweden issued a statement calling for a new nuclear disarmament agenda. (Slovenia later withdrew from the NAC.)
The NAC called for the five nuclear weapon states – USA, Russia, Britain, France, China – and the three nuclear-capable states (India, Pakistan and North Korea) to make an unequivocal commitment to nuclear disarmament and to begin multilateral negotiations that would lead to the elimination of nuclear weapons through a Nuclear Weapons Convention.
Besides, as one of the most vocal state advocates of nuclear disarmament, South Africa supports proposals to create a new legally binding framework containing clear benchmarks and timelines to achieve and maintain a world free of nuclear weapons.
South Africa has continued to stand firmly behind the principle of nuclear disarmament, and became part of a core group of countries pushing the humanitarian initiative to end nuclear weapons since 2012. That initiative grew into a movement for a UN treaty banning nuclear weapons, which led to the adoption of the UN Treaty on the Prohibition of Nuclear Weapons on July 7, 2017.
South Africa was a leader in encouraging negotiations on a UN- proposed nuclear weapons ban treaty at the 71st session of the UN General Assembly.
Against this backdrop, it is not surprising that the 2017 Nobel Peace laureate International Campaign to Abolish Nuclear Weapons (ICAN) has welcomed South Africa's "continued leadership on nuclear disarmament and hopes its action will inspire other African nations to adhere to the Treaty".
ICAN recalls President Nelson Mandela's 1998 address to the UN General Assembly which illustrated the ways in which South Africa challenged the arguments of deterrence used by other nuclear-armed nations:
"We must ask the question, which might sound naive to those who have elaborated sophisticated arguments to justify their refusal to eliminate these terrible and terrifying weapons of mass destruction – why do they need them anyway!

"In reality, no rational answer can be advanced to explain in a satisfactory manner what, in the end, is the consequence of Cold War inertia and an attachment to the use of the threat of brute force, to assert the primacy of some States over others." [IDN-InDepthNews – 13 April 2019]

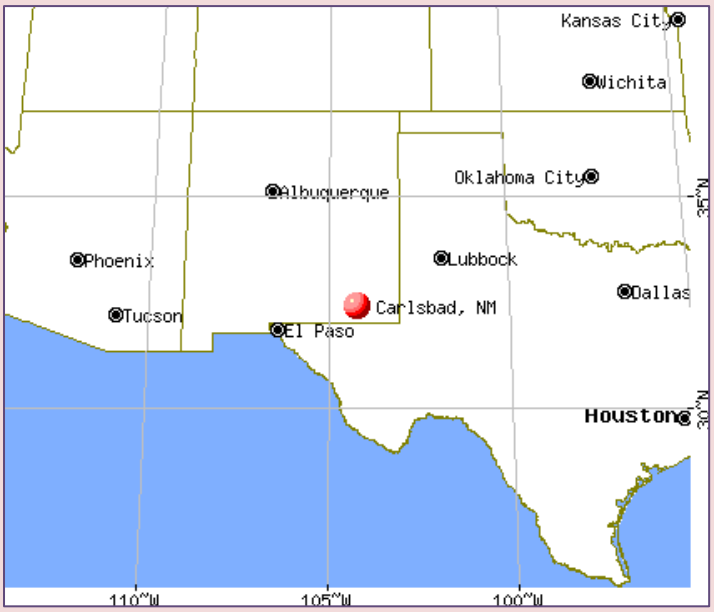
## Los Alamos nuclear waste successfully shipped to WIPP

Source: http://www.homelandsecuritynewswire.com/dr20190415-los-alamos-nuclear-waste-successfully-shipped-to-wipp

Apr 15 – The first shipment of Transuranic (TRU) waste from the newly reopened Radioactive Assay Nondestructive Testing (RANT) facility at Los Alamos National Laboratory has been successfully delivered to the Waste Isolation Pilot Plant (WIPP) near Carlsbad, New Mexico.




"The reopening of RANT and resumption of waste shipments to WIPP puts Los Alamos in a stronger position to fulfill its national security mission," said Laboratory Director Thom Mason. "As the Laboratory works to meet the Nation's future plutonium manufacturing and science goals a robust and continuous waste disposition program is more important than ever."




LANL says that Los Alamos is currently the largest producer of TRU waste in the nuclear security enterprise. As plutonium manufacturing increases so will the amount of TRU waste generated. Successful operations at the Laboratory and at WIPP will be crucial to meeting these goals.

The RANT facility serves as an indoor TRU waste loading capability for the Laboratory. TRU waste shipments to WIPP were last loaded out of RANT in May of 2014 after questions arose centered on the facility's ability to withstand a large earthquake event. In the spring of 2018 a new low Material At Risk (MAR) operational strategy was developed that insured the MAR stayed below a threshold where seismic would be a concern. That strategy was developed into a new Documented Safety Analysis, approved by the National Nuclear Security Administration and implemented by the Laboratory in December of 2018.

"Getting the RANT facility back in service and successfully moving TRU waste to WIPP will add to our operational and safety margins and provide a better level of efficiency as we continue to improve our waste operations," said Kelly Beierschmitt, Deputy Laboratory Director for Operations.

The facility demonstrated readiness in January and February of 2019 and received startup authorization

on February 28. The indoor loading capability provided by RANT increases the Laboratory's TRU waste shipping capacity to support de-inventory of the backlog of TRU waste at TA-55.

Prior to the re-opening of RANT shipments of TRU waste to WIPP were loaded in an outdoor area at TA-55, severely limiting operations due to weather and loading equipment factors.

This first shipment to WIPP departed from RANT on April 11, totaling 42 55-gallon drums of TRU waste, typically consisting of contaminated gloves, booties, cleaning materials, and general waste products.

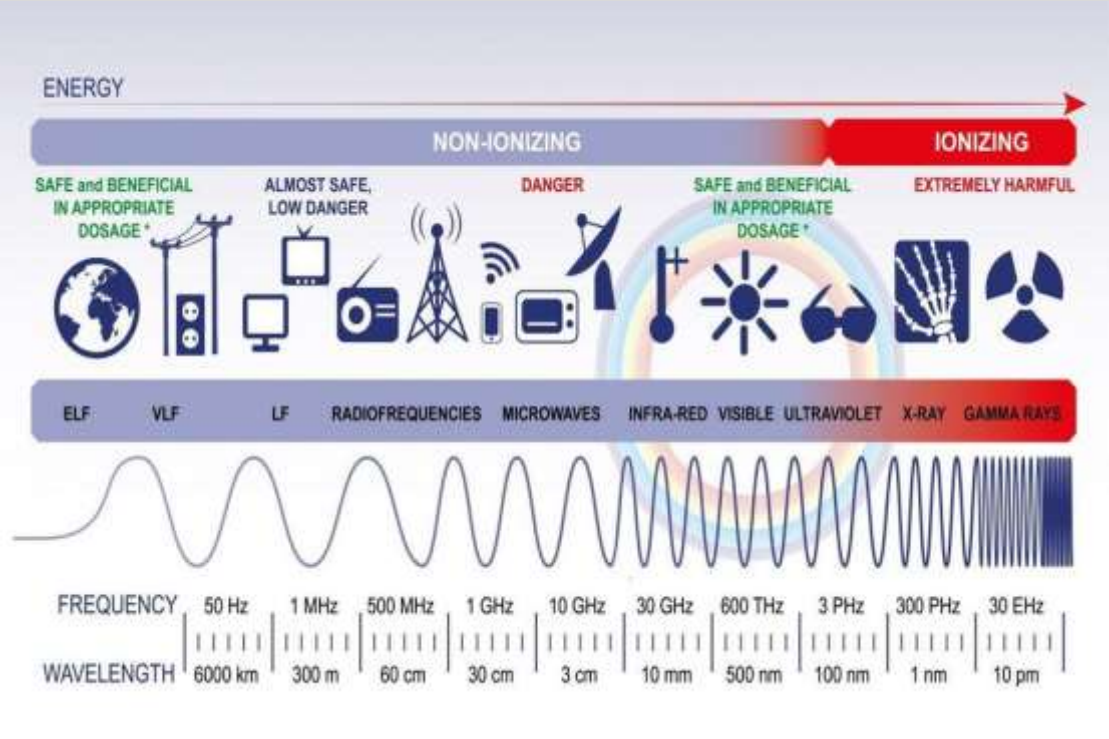
As the Nation's Plutonium Center of Excellence Los Alamos operates the most modern, fully operational, full capability plutonium science and manufacturing facility in the United States. Plutonium operations support a wide range of national security programs that involve stockpile stewardship, plutonium processing, nuclear materials stabilization, materials disposition, nuclear forensics, nuclear counter-terrorism, and nuclear energy.

## The Weaponization Of The Electromagnetic Spectrum

**By Jayshree Pandya**

Source: https://www.forbes.com/sites/cognitiveworld/2019/04/12/the-weaponization-of-the-electromagnetic-spectrum/

Apr 12 – The information age is evolving the very nature of warfare. Today, each nation increasingly depends on closely integrated, high-speed electronic systems across cyberspace, geospace, and space (CGS). But, it's a cause of great concern if an enemy can easily use a weapon like a small, inexpensive EMP device. An EMP weapon can deny any individual or entity across a nation the ability to use electromagnetic waves for their digital infrastructure and digital connectivity, e.g. radio, infrared, and radar. Moreover, a nuclear blast can also trigger an EMP effect, as can a solar storm. Individually and collectively, this emerging reality understandably changes the nature of warfare, the focus of the war, and the target of warfare, shaking up the very foundation of security.




Electronic warfare is on our doorstep, and no nation seems to be fully prepared. Since electronic warfare appears to already be on our doorstep, in order to meet the complex EMP warfare challenges that are seriously threatening the very progress and advances nations have made in CGS, it is essential to evaluate how prepared each nation is today in their defensive as well as offensive capabilities. *How are nations addressing the security challenges to their CGS?*

The weaponization of the electromagnetic spectrum is becoming a reality. Acknowledging this emerging reality, Risk Group initiated a much-needed discussion on Electromagnetic Warfare with Colonel Avraham Cohen, Head of National Security Cyber Research Group and the Co-Founder and Chief Technology Officer (CTO) of Sphere-SOC based in Israel on Risk Roundup.

**Changing Nature of Warfare**

Rapid advances in science and technology are creating asymmetries across nations: its government, industries, organizations, and academia (NGIOA) in many unforeseen ways. As nations move towards a highly digitalized society, there is increasing uncertainty on all fronts across CGS.

While the emerging technology is on its way to changing the way we communicate, collaborate, work, and socialize, it is also changing the way in which wars can be fought. This is primarily because today abriefcase-sized radio weapon could wreak havoc in our digitally connected world. The threat is genuine and growing. Electromagnetic (EM) attacks are not only theoretically possible, but they are also already happening. Many have been reported previously. A GPS failure was reported in South Korea in 2012, and it is believed that truck-based jamming systems were behind the attack. This is just one example. *So, what threats are nations facing today from the EM weapons? What threats are possible in the coming tomorrow? Is any nation prepared for electronic warfare today?*

**EM Warfare**

The increased need for information for all our electronics and the rapidly evolving digital systems, 4G/5G, makes many vulnerable to anyone who may wish to create problems. That means any enemy: hackers, criminals, vandals, or terrorists, can easily cause irreparable harm to anyone they want to. *That brings us to an important question: how resilient is each nation's infrastructure in cyberspace, geospace, and space to EM attacks?*

This is a rapidly growing concern because unlike many other means of attack, EM weapons can be used without much risk. For example, in geospace, any terrorist gang with firearms

and other weapons are noticeable and can be caught. In cyberspace, a cyber hacker may raise some alarms while attempting to slip through many firewalls. In space, any attempt to launch an attack requires extensive planning and preparation that is visible. However, for an EM attacker, it is challenging to notice any attack until electronics and computer systems begin to fail. Moreover, even when electronics or systems fail, the victims may still not know why they failed.

As seen today, the critical infrastructure across CGS is either controlled by the military, public or private entities. From defense systems to financial systems and communication systems to power systems, each system today is vulnerable to electromagnetic attacks. Not only is the personal digital infrastructure of any individual or a family at risk, but also the smart: meters, homes, enterprises, cars and so on are at risk as well. *That brings us to some important questions: what role does electromagnetic energy play in the digital infrastructure of a digital global age? What kind of EM pulses are more dangerous to digital infrastructure? Also, fundamentally, why is it that easy to destroy electronics?*

The digital revolution is transforming individuals and entities across NGIOA, and the military is no exception. As militaries acquire a host of new sensors and communications systems that allow their forces to establish information dominance in the fight against enemies quickly, the same capabilities can be seized by an electromagnetic weapon and exploited for the tactical advantage of the enemies. This is a complex security risk facing most nations today.

There is a growing concern that nations are vulnerable when it comes to secure communications links or access to GPS signals. *If that is true, in a potential electronic war, can any nation protect its electronics? Who is responsible for safeguarding a nation's electronics? The military? Can a nation's military protect an entire nation worth of electronics?*

**Electronics Vulnerability**

As we evaluate the complex security risks facing nations' electronics and digital infrastructure, the question arises as to why our electronics are vulnerable? Why have we not designed them to be resilient to EM attacks?

It seems that electronics are vulnerable because they were designed to handle naturally occurring electromagnetic radiation, but not harmful. This understandably makes not only military operations vulnerable, but also perhaps individuals and entities across NGIOA vulnerable. Moreover, unlike other means of attack, EM weapons can be used without much risk as they are almost undetectable. *So, the question is: is there no way to make electronics resilient?* Perhaps chips can be developed that are EM resistant!

*That brings us to an important point: whoever owns the electromagnetic spectrum will win the next war. Who owns the electromagnetic spectrum today?*

**Protecting Electronics from EMP Weapons**

What steps can be taken to guard against EM Weapons? While it is recommended to always put as much distance as possible between any electronics and the potential attacker, how do we know who the attackers are, where they come from, and how they look? How can we surround each electronic with a barrier that can resist the EM attack?

It is essential to understand and evaluate how the EM spectrum is being controlled today and what steps can be taken to ensure EM security. The current focus is on securing the critical infrastructure which is vital to everyone: individuals and entities across NGIOA. But it is not just critical infrastructure that is important, for individuals and entities across NGIOA also care about their private infrastructure as well. *That brings us to an important point: is there any practical way to limit the damage to electronic equipment? Is there any way to make electronics EMP resistant?*

**What Next?**

The electromagnetic spectrum is where the wars of tomorrow will be fought. Since the weaponization of the electromagnetic spectrum impacts our individual and collective security, each one of us has a role in ensuring the safety and security of the electromagnetic spectrum. Let us begin a discussion on how to secure the electromagnetic spectrum, what innovations are essential,

how to transform electronics to make them resilient to any EMP attacks, and how to secure the future of humanity in cyberspace, geospace, and space.

*Jayshree Pandya , is Founder of Risk Group, Host of Risk RoundupPodcast, Author of The Book, The Global Age & a Strategic Security Advisor.*


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EXPLOSIVE
NEWS

# Ridding Landscapes of Deadly Mines Could Have a Toxic Side Effect

Source: https://earther.gizmodo.com/ridding-landscapes-of-deadly-mines-could-have-a-toxic-s-1833607063

Undetonated mines and other ordinance collected from Kurdistan I Photo: Courtesy of Rahel Hamad

Mar 27 – Land mines are notorious for leaving a legacy of ongoing destruction from Southeast Asia to Africa, taking the lives and limbs of civilians decades after the wars and hostilities that brought them in the first place. As detonation is one of the main strategies for removal, clearing mines can be expensive and dangerous for people. It may also be harmful to the environment, according to recent research conducted in northern Iraq which is the first to indicate that mine clearing operations can leave high levels of heavy metals in the soil, potentially causing problems for ecosystems and humans in the area.

The Iran-Iraq War ended in a ceasefire in August 1988, but thousands of landmines remain in areas near the border. The Mines Advisory Group, a British organization focused on removing and destroying mines, began to clear the explosives in 1991 in areas of Kurdistan, either by detonating them where found or by taking mines collected from around the countryside and exploding them in a central location. Previous research by Rahel Hamad, a professor at the petroleum geosciences department at Soran University in Iraq, used satellite images to show that the explosions from demining operations have fragmented some forested areas in the Halgurd-Sakran National Park near Soran in northern Iraq, potentially contributing to a drop in biodiversity in the area. In their latest study, Hamad and his coauthors wanted to see whether the soil itself was affected by these operations. In 2016, they found areas used to explode mines in the national park with the help of the organizations that cleared them. "You can see the change in color around the explosion, especially the soils– they become darker because of the heavy metals," Hamad told Earther.

The researchers collected nine samples each from a roughly 20 square-meter area around two explosion sites and sent them to a laboratory in Canada to determine the level of heavy metals present in the soil, comparing the results to global standard soil measurements. They discovered extremely high levels of nickel and chromium, with the highest sample of nickel showing more than six times the global standard, as well as above average levels of manganese, arsenic and copper. They also discovered high levels of cobalt. All of these elements are generated from the detonation of mines.

The study was small-scale and exploratory, but offers some of the first concrete evidence that even the controlled detonation of mines

can create lingering problems. Hamad and his coauthors note that research on the soil between France and Belgium, which saw heavy use of mines and other sources of toxins during World War I, shows ground is still polluted even a century later. They said that over time, the whole area around the mines in Kurdistan could contain these pollutants.

This could have a negative impact on the flora growing in the soil, and any fauna eating these plants. Elevated levels of heavy metals could also potentially affect humans who use cleared areas cleared of mines to grow crops or graze sheep. "The largest significance of the study is to help the decision makers conserve the national park," Hamad said, adding that they could produce risk maps for areas contaminated during mine clearing operations.

Hamad said that the next step in this work is to check for soil contamination around more detonation areas and to study the concentration of heavy metals in other parts of the national park.

Ryan Casey, the chair of the chemistry department at Towson University in Maryland who studies soil contamination but who was not involved in the new research, said the authors "did a good job indicating that there is evidence of soil contamination from some of the metals they studied." He added that if the same levels of nickel and manganese discovered in Hamad's study were found in Maryland soil, a cleanup would likely be recommended.

But he says future research on this area should try to quantify the baseline levels of heavy metals in these soils in order to determine how the exploded mines have affected things, rather than measuring them against a global standard. Hamad said that he didn't take these samples because he doesn't trust the area to show normal levels due to eight years of fighting in the area during the war, when mines and other bombs exploded all over the place. But, the concentrations of heavy metals are higher in their small sample areas right around the actual explosion sites as opposed to on the outside of the square study areas.

Hamad emphasized that the biggest problem posed by mines is the immediate danger to life and limb. While in many of the villages in the area, he witnessed a number of children and adults missing legs or arms. He even witnessed kids chasing balls into mine fields with clear signs warning them away.

"The default assumption is that this is a long-term issue. These metals will be around at least on the order of decades."

Heiko Balzter, Director of the Centre for Landscape and Climate Research at the University of Leicester in England and a coauthor on Hamad's study, said in an email that clearing the mines is sometimes the only option. "Ideally one would collect unexploded land mines without detonating them, but this is sometimes not practical," he said.

Casey said areas where mines had exploded could remain contaminated for a long time, though just how long depends on the soil properties and local weather conditions. "The default assumption is that this is a long-term issue. These metals will be around at least on the order of decades," Casey said.

According to Balzter, the best way to avoid all these problems is to stop the use of mines in the first place.

"A ban on the production, sales and use of land mines is my highest priority recommendation to avoid building up an even bigger future legacy," he said.

## Improving canine detection of explosives

Source: http://www.homelandsecuritynewswire.com/dr20190401-improving-canine-detection-of-explosives

Apr 01 – The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has awarded $564,988 in funding to Auburn University for two research and development (R&D) projects designed to improve the effectiveness and efficiency of canines trained to detect explosives.

"Canines are the best, most versatile, mobile explosives detection tool we have supporting Homeland Security," said Don Roberts, S&T Detection Canine Program Manager. "S&T is making important investments in research to define the strengths and limits of detection canines. What we fund provides the community with the tools,

techniques, and knowledge to better understand, train, and use explosives detection canines and enables more effective and efficient operational performance."
S&T says that Auburn University has received two funded LRBAA awards:

- The *Whole Spectrum Explosive Odor Training* Project received $280,566 to develop a scientifically validated canine training program enabling canine teams to overcome adversaries' attempts to modify, filter, or reduce explosive odor signatures in improvised explosive devices (IEDs). S&T will also be conducting research to expand the understanding of how threat concealment affects a canine's ability to detect odor, and explore development of training aids that specifically mimic such conditions.
- The *Examination and Enhancement of Canine Evaluations* Project received $284,422.00 to examine the practical difference in performance measurement data integrity between single- and double-blind canine team evaluation methods, and will use the resulting data to develop tactics, techniques, and procedures to improve detection canine team performance.

Two contracts were awarded under Long-Range Broad Agency Announcement DHSST-LRBAA-14-02 EXD.08, Canine Explosive Detection Technologies topic area, which addressed several areas of detection canine R&D.

## Polymers help minimize fuel explosions and fires from accidents and terrorist acts

Source: http://www.homelandsecuritynewswire.com/dr20190403-polymers-help-minimize-fuel-explosions-and-fires-from-accidents-and-terrorist-acts

Apr 03 – When an act of terrorism or a vehicle or industrial accident ignites fuel, the resulting fire or explosion can be devastating. On Tuesday, scientists described how lengthy but microscopic chains of polymers could be added to fuel to significantly reduce the damage from these terrifying incidents without impacting performance.

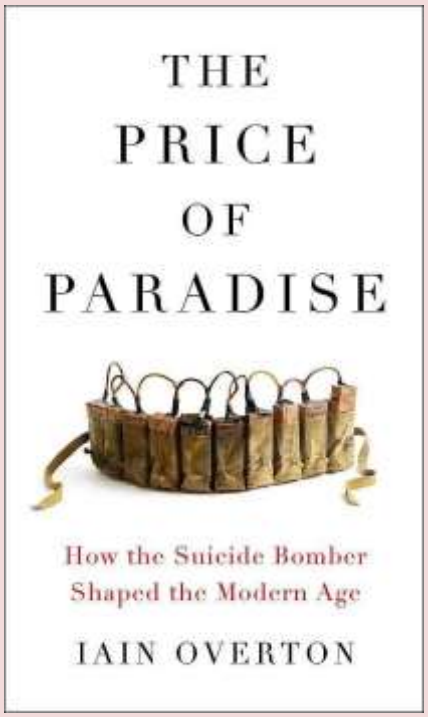
## Why suicide bombers became the go-to weapon for terrorists

Source: https://www.standard.co.uk/lifestyle/books/the-price-of-paradise-how-the-suicide-bomber-shaped-the-modern-age-by-iain-overton-review-a4109531.html

Apr 06 – The myth of the suicide bomber grips the Western imagination. The public thirst for stories about them is insatiable. But of all the suicide bombings in the past 30 years, it was the September 11 2001 attacks on the United States that made real the terror of this destructive weapon. In addition to the tragic human toll that the suicide bomber inflicts on civilians, the act of weaponising oneself in the service of ideology shatters a deeply-held universal belief regarding the sanctity of life and self-preservation. Thus viewed, the suicide bomber is the antithesis of modernity and rationality.
A widespread opinion is that religion provides inspiration and motivation for wannabe suicide bombers. Time and again it is argued that they are religious zealots who seek paradise at the cost of hell on earth, through death by self-immolation.
For example, nowadays many hold Islam accountable for the manifold increase in suicide bombings and their spread to European and US streets. Proponents of this hypothesis include both the perpetrators of suicide bombings and their detractors — both believe in a clash of civilisations. Others hold that extremist ideologies and ideologues twist Islamic doctrine to carry out evil deeds.
In his sweeping survey of suicide bombings — from the first documented modern suicide bomber, Ignaty Grinevitsky, a revolutionary who murdered Tsar Alexandar II in St Petersburg in 1881, to today's jihadists — veteran journalist and human rights activist Iain Overton sees a vision of utopia as a common thread.
Despite the different national, ideological and historical contexts of suicide bombers in countries as disparate as Russia, Japan, Iran, Lebanon, Sri Lanka, Palestine, Afghanistan, Iraq, Nigeria, Somalia, Syria, America, Europe and beyond, all are driven, we are told, by religious messianism and zealotry. A wish for paradise and an all-consuming religious sentiment unites nearly all of them, including secular revolutionaries, Marxists,

insurrectionists and jihadis. Overton's overarching and parsimonious argument erases core differences in motivation and ideologies between suicide bombers across time and space. Surely, the drivers behind their actions are more complex and multi-varied than a single cause?

A related argument, echoed in the book's subtitle, is that suicide bombers have shaped the modern world. "We live in the age of the suicide bomber," Overton writes. Do we really? And have they "become a defining feature of the modern era", as the author asserts? One must question if suicide bombings are as important as globalism, the Arab Spring uprisings, or the rise of far-Right populism worldwide.




In my view, Overton inflates the importance of the suicide-bomber phenomenon, and he invests it with strategic and even existential overtones. For example, his claim that "suicide bombers are the real weapons of mass destruction" overlooks the central function and targets of these weapons.

Suicide bombs are the tactical weapon of choice for radicals in asymmetrical conflicts — a weapon that extremists with limited resources employ against more powerful states and entities. As tools of political violence and terrorism, suicide bombers are symptoms of broken politics, broken institutions and broken lives.

All of that said, this well-researched and well-written book was conceived in the midst of the spiralling suicide attacks unleashed by Islamic State beginning in 2014. Overton writes that the trigger for his book came in late 2015, when suicide bombings were increasing in frequency on Western streets.

It is no wonder, then, that the tone is dire, warning that suicide bombings are on the rise and that they are a greater threat now than ever. But, in fact, there has been a dramatic decline in terrorist and suicide bombings worldwide in the past two years, with the biggest decrease occurring in the West, owing mainly to the weakening of Islamic State. Only 10 attacks occurred in Western countries in 2018 compared with 168 at IS's height in 2016-2017. If the trend holds, 2019 will likely witness even fewer deadly attacks.

Analysts should be cautious about generalising and allowing genuine fears to override facts and reason. Overton is right, of course, to curse the darkness. He cites raw data which shows that there have been over 3,500 recorded suicide attacks since 1881 (about 25 attacks per year over the past 138 years). Such numbers are dwarfed, however, when compared with other types of violence — for instance, gun violence in the US, which claims tens of thousands of lives each year.

Where Overton's book excels is in explaining the consequences of the US's (and Europe's) overreaction to suicide bombers, particularly after 9/11. America's global war on terror was costly in blood and treasure, as well as counterproductive. The US-led invasion and occupation of Iraq in 2003 devastated the country and likely is the precipitating event for many of the suicide bombings that occur to this day.

In November 2018 Brown University's Watson Institute for International and Public Affairs released the Costs of War study in which it was calculated that the US will have spent $5.9 trillion on activities related to the global war on terror from 2001 until October 2019.

Despite this staggering sum, not to mention that incalculable human cost, the number of jihadist fighters only multiplied in the same period from about 37,000 to 66,000 fighters in 2001 to about 100,000 to 230,000 in 2018 (according to a report by the Washington Center for Strategic and International Studies).

Overton also underscores the corrosive effects of the global counter-terrorism campaign on the rule of law and open society in Western democracies.

My criticisms of this book do not take away from its substance, clarity and richness. Overton has written an informative book on a timely topic that demands critical scrutiny.

***Fawaz Gerges*** *is professor of international relations at the London School of Economics and the author of ISIS: A History (Princeton University Press) among other books.*

## Explosion at Russia's Military Space Academy leaves four seriously hurt after 'bombs' spark evacuation

Source: https://www.thesun.co.uk/news/8773091/explosion-russia-military-space-academy/

Apr 02 – Four people including two bomb disposal experts and a teacher were hurt in an explosion that rocked a military space academy in St Petersburg today.
Local news sites said a homemade bomb destroyed a staircase at the prestigious Mozhaisky Academy - as cops said they were treating it attempted mass murder.

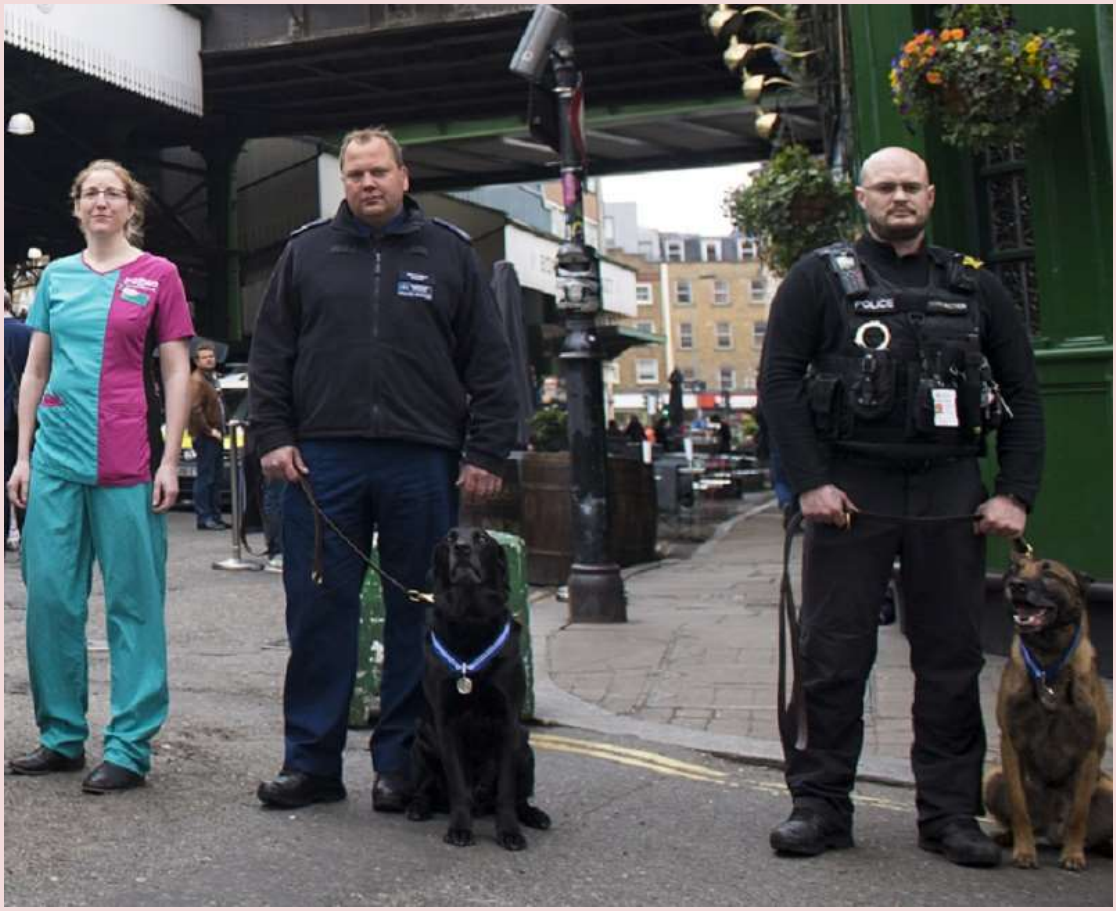
There were also unconfirmed reports of a second explosion from a TM-57 anti-tank mine which had been stored at the academy.
Cadets and instructors were evacuated from the building before the blast on the second floor, but around 15 people were trapped on the level above when the staircase collapsed, according to local TV channel 78 News.
Later the Fontanka news agency reported the blast was caused by a "selfmade" improvised explosive device equivalent to 200 grams of TNT.
Officers who found it called in the Academy's own mine-clearance group.
It detonated as sappers covered the suspicious device with body armour preparing for its disposal.
The wounded are said to include Colonel Rifat Zakirov, a bomb disposal expert who is reported to be in a coma after suffering head injuries.
Colonel Nikolay Kurday was also said to be in hospital where he was described as conscious.
And a teacher was hit by flying shrapnel, according to reports.
Officials from the FSB spy agency reportedly visited the scene along with police and emergency rescuers after the blast rocked Russia's second city just after lunch.
Russia's top investigative body said it has launched a criminal inquiry into conspiracy to murder.

## Hero dogs receive bravery awards: Canine OBEs for dogs who helped at scenes of terror attacks

Source: https://www.londonnewsonline.co.uk/hero-dogs-receive-bravery-awards-canine-obes-for-dogs-who-helped-at-scenes-of-terror-attacks/

Apr 02 – A police mutt probably wouldn't know what to do with a medal, unless you covered it in gravy or made it look like a tasty chihuahua.
He or she is much more likely to appreciate an extra few biscuits for dinner – and would probably love you forever.
That is probably what seven dogs from the Met and British Transport Police are tucking into this week.
Seven police dogs who supported the cops and paramedics during the London terror attacks at Westminster Bridge, London Bridge and Borough Market have been honoured for their heroic actions by vet charity PDSA.
They were awarded the PDSA Order of Merit – the animal equivalent of the OBE – at a ceremony on Tuesday.
The dogs have been chosen to represent the 19 dogs who served during the 2017 attacks. From the Met, they are Kai, Delta and Dave and from the BTP Bruno, Marci, Jax and Bobby.
PDSA vet, Rosamund Ford, said: "The actions of these incredible dogs – and their handlers – was vital in keeping the public safe and allowing the emergency services to carry out their work.

They performed their duties in a highly-charged and unfamiliar environment that no amount of training can fully prepare them for.



PDSA is honoured to recognise their devotion to duty and service to society."

In the moments following the Westminster Bridge attack, the BTP Explosive Search Dog Section and the Met Police Explosive Detection Dog Team were rushed to the scene to ensure public safety.

BTP Dogs Ollie, Oscar, Bruno and Scooby searched through the chaos for potential devices that could cause further harm on the bridge itself and around Parliament Square.
They were joined at the scene by Met Police Dogs Kai and Bruce and their handlers.
They searched the car that had crashed into the wall of the Palace of Westminster, as a precautionary measure in case it contained a bomb.
Once safe, Helicopter Emergency Medical Services landed in Parliament Square to help injured victims.
At London Bridge BTP General Purpose Dog Teams were called to the scene alongside firearms officers.
Police Dogs Jax, Marci, Johnny, Rocy, Tara and Bobby searched amid a volatile situation for more than 13 hours, virtually non-stop.
Police Dogs Tara, Rocy and Bobby worked tirelessly, never faltering in their duty.
Met Police Dogs Alfie, Dave, Poppy and Robson were also deployed to search the area. Together with the newly qualified Police Dog Kai, they searched a dozen buildings.
Police Dog Delta worked with his handler and a team of firearms officers to search over 30 buildings.
His skills, calibre and professionalism saved vital time.
At Borough Market, the Met Dog Teams joined armed officers to search for a suspect who was still unaccounted for, despite the unknown risk to themselves and their dogs.
Police Dogs Casper and Romeo searched the suspects' suicide vests for explosives.
Police Dog Casper and his handler later cleared a suspect vehicle under a nearby railway bridge which could have contained a bomb. He was able to show the vehicle was safe, allowing the vehicle to be searched.
The teams worked with the knowledge that potential further danger remained all around them, but put the safety of the public ahead of their own as they continued their searches.
PDSA director general, Jan McLoughlin, said: "The role played by all of the dogs was crucial. They are trained to search in a non-hostile environment.
Yet they worked in unimaginable conditions, remaining calm and responsive.
"Their devotion and service to society was incredible, especially under such distressing circumstances, and we will never forget those who lost their lives in these appalling attacks.
Recognising the actions of these devoted dogs with our prestigious PDSA Order of Merit will be an honour."
British Transport Police Inspector Paul Miles said: "I am immensely proud of our dogs and their handlers. It is an honour for them to receive such a prestigious award and they will continue to work day and night to keep London safe."

## Responding to a Suicide Bomber Incident

**By Robert Stephan**
Source: https://www.domesticpreparedness.com/preparedness/responding-to-a-suicide-bomber-incident/

August 2006 – As has been proved literally hundreds of times in Iraq, Israel, and elsewhere, the detonation of an explosive device by a suicide bomber can occur, without warning, anywhere in the world – including the United States. When, not if, such an attack takes place on American soil, the jurisdiction directly victimized will be expected to be fully prepared to deal with it. More specifically, the community's first responders – firefighters, police officers, and emergency medical technicians, primarily, who will in all likelihood be the first trained personnel on the scene – must be trained and ready to save lives, stabilize the incident scene, and minimize the short- and long-term impact of the suicide bombing in general.
Those who activate the explosive device will pick the date, time, place, and method of attack – and may decide to maximize the destructive effect by lacing their weapon with an extremely toxic chemical or radioactive material, making it a so-called "dirty bomb." Because of this possibility, responders who are approaching the scene should position themselves upwind and wear an acceptable level of personal protective equipment, including respiratory protection devices. Caution in obviously necessary – but so is speed. It is particularly important, for example, that the first

emergency responders on the scene enter the incident area as rapidly as possible to immediately remove any injured patients.
Thanks in large part to the efforts of U.S. and allied intelligence agencies, there have been no new terrorist attacks on U.S. soil since the bombing of the World Trade Center, and the Pentagon, on 11 September 2001. It is only natural, therefore, as time passes, that memories fade and the nation's first responders are lulled into a false sense of security and the belief that another 9/11 event either will not occur or, at worst, is very unlikely. That sense of complacency may well be the first responders' greatest enemy.

**Last Week, and Five Years Ago**

Several other incidents of self-annihilation by terrorists have in fact been attempted. The arrest last week It is only natural that memories fade and first responders are lulled into a false sense of security; that sense of complacency may well be the first responders' greatest enemy. of the terrorists plotting to carry out a dozen or more suicide bombings on U.S. passenger aircraft en route from London's Heathrow Airport to the United States was a helpful reminder that as far back as December 2001 Richard Reid, a British citizen, had planned to detonate a shoe bomb containing plastic explosives while over the Atlantic Ocean on a commercial flight from Paris to Miami.
First responders who are trained in managing mass-casualty incidents, and in patient triage, may believe that they are now properly prepared – much more so, certainly, than in September 2001. But U.S. decision makers, and the American people, are entitled to ask if the nation's first responders are, in fact, truly prepared for the grotesque mutilation, carnage, dismemberment, and repulsive odors emanating from the explosion site that will be facing those who are treating the victims of a suicide-bomb attack.
The successful attack, by American citizens, on the Murrah Building in Oklahoma City, was not a suicide attack per se – but it proved that there are few if any public buildings or critical-infrastructure facilities within the United States that are 100 percent safe from terrorist attacks in general. Suicide attacks, by definition, are more difficult to guard against than attacks in which the terrorists themselves hope to survive. And it is obviously more difficult to protect any community from several attacks occurring more or less at the same time. In short, well-planned and well-implemented multiple attacks by suicide bombers similar to the attacks against the public transportation systems in London, Madrid, and Mumbai could occur in the United States as well.

**Immediately If Not Sooner**

Gary Briese, executive director of the International Association of Fire Chiefs – and, not incidentally, one of the nation's earliest prognosticators of the probability of terrorist attacks within the United States itself – subscribes to what is called the "20-minute rule" for the care and evacuation of patients. The approach suggested by Briese, and many other experts, emphasizes that the victims be removed from the bomb site, and the incident scene, as quickly as possible – i.e., within 20 minutes or less – and be transported to the closest available trauma center. To meet that ambitious goal, though, hazmat responders must rapidly enter the explosion site to verify the presence (or, preferably, absence) of possible WMD (weapons of mass destruction) materials, a difficult task that requires the use of specialized detectors. If such materials are present, decontamination of the site will probably be necessary.
For operational purposes, perhaps the most important question that will be asked, if and when a suicide bomb explodes in a crowded venue, is what the first incident commander arriving on the scene should decide about victim rescue. If he or she decides - because of the potential presence of a secondary device – not to proceed immediately into the debris field to rescue and remove injured victims, the question is still valid: At what point in time will such a decision be made and carried out? The time for preplanning responders' incident activities, and for developing operational guidelines, has to be prior to an incident, not after another suicide bombing takes place.
Following are some suggested action guidelines for first responders arriving at the scene of a suicide bombing or similar incident:

- Approach and position themselves upwind, 300 feet or more from the edge of the debris field;

- Isolate the area and deny entry by those who are not first responders – and by first responders who are not wearing the personal protective equipment they need;
- Search the incident area as rapidly, as safely, and as thoroughly as possible for secondary suicide bombs and/or other explosive devices;
- Immediately – i.e., in 20 minutes or less – remove injured victims and transport them to an appropriate medical facility; and
- Extinguish any uncontrolled fires in the area

*The following reference works are highly recommended for those seeking additional information on this important subject: Suicide Bombings: The New Chaos (International Association of Fire Chiefs, 2005); The Cult of the Suicide Bomber (Robert Baer, June 2006); and Radiological Standard Operating Guidelines for First Responders (Metropolitan Washington Government Council of Governments, July 2006).*

***Battalion Chief Robert Stephan**, a member of the Montgomery County (Md.) Fire and Rescue Service for 34 years, has been the leader of the county's Hazardous Incident Response Team since its creation in 1981. He is also a member, and a former chairman (for 14 years), of the HazMat Subcommittee of the Metro Washington Council of Governments for the National Capitol Region. He is cross-trained as a 15-year National Registry Paramedic, a member of the Washington, D.C., National Medical Response Team, and an instructor for the National Center of Biomedical Research and Training. He holds an Associate Degree in Fire Science from Montgomery College and is a National Fire Academy Executive Fire Officer Graduate.*

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

# C²BRNE DIARY

# CYBER NEWS

# Two gov notices point to vulnerabilities in devices for heart problems

Source: https://techxplore.com/news/2019-03-gov-vulnerabilities-devices-heart-problems.html

Mar 23 – The U.S. Department of Homeland Security (DHS) and the U.S. Food and Drug

Administration (FDA) issued communications that cybersecurity vulnerabilities were found in some Medtronic devices. Hundreds of Medtronic heart devices are vulnerable to cybersecurity incidents, according to two US federal government notices.

The vulnerability also affected patients' home bedside monitors that read data from the devices and in-office programming computers used by doctors, said *Star Tribune*.

Ana Mulero, *Regulatory Focus*: The FDA issued an FDA safety communication; DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory to flag cybersecurity vulnerabilities. These were detected in Medtronic's Conexus telemetry protocol. "The wireless technology is used to enable communication between the medical device manufacturer's implantable cardiac devices, clinic programmers and home monitors."

Implanted defibrillators are for treating heart problems. They are placed beneath the skin. They deliver electric shocks if an irregular heartbeat is detected, noted *TechSpot.*

Two vulnerability types were mentioned regarding (1) formal authentication or authorization protections, and (2) data encryption. Mulero said, "Improper access was assigned a critical (9.3) score and data transmission has a medium (6.5) vulnerability score."

According to Mulero, "Both FDA and ICS-CERT reported that an attacker or unauthorized individual could exploit the detected cybersecurity vulnerabilities to access one of the affected products in proximity, impact device functionality and/or intercept sensitive patient data within the telemetry communication."

The official website of the Department of Homeland Security posted on Thursday Medical Advisory (ICSMA-19-080-01), Medtronic Conexus Radio Frequency Telemetry Protocol. "The result of successful exploitation of these vulnerabilities may include the ability to read and write any valid memory location on the affected implanted device and therefore impact the intended function of the device."

A list of specific products and versions of Medtronic devices that use the Conexus telemetry protocol that are affected can be found in the medical advisory posting of Thursday, March 21. (A protocol is used to connect monitors wirelessly to an implanted device, said *TechSpot*.)

Homeland described vulnerabilities in different models of Medtronic implantable defibrillators, said *Star Tribune*.

*TechCrunch* and *TechSpot* discussed some technical details of what sparked the warning. Those devices having wireless or radio-based technology pose the benefit of allowing patients to monitor their conditions and their doctors to adjust settings without having to carry out an invasive surgery. Medtronic's proprietary radio communications protocol, known as Conexus was not encrypted and there was no authentication process.

Attackers, with radio-intercepting hardware, and within a certain range, could modify data on an affected defibrillator, changing the implant settings.

Hackers would need to be close to users—around 20 feet, noted Rob Thubron in *TechSpot*.

Medtronic in its security bulletin on Thursday informed that "Fully exploiting these vulnerabilities requires comprehensive and specialized knowledge of medical devices, wireless telemetry and electrophysiology."

The *Star Tribune* article carried quotes from Dr. Robert Kowal, chief medical officer for Medtronic's cardiac rhythm and heart failure products. He said that "a hacker would have to be within

20 feet or so of the patient, would need detailed knowledge of the device's inner workings, and have possession of specialized technology to pull off the hack."

What should patients do, then? Medtronic recommended that patients and physicians continue to use these devices as prescribed and intended. "The benefits of remote monitoring outweigh the practical risk that these vulnerabilities could be exploited."

Discussing mitigation, Medtronic said in its bulletin that it was "developing updates to mitigate these vulnerabilities" and will be informing patients and physicians when available subject to regulatory approvals. The medical advisory appearing on the Department of Homeland Security website said that "Medtronic has applied additional controls for monitoring and responding to improper use of the Conexus telemetry protocol by the affected implanted cardiac devices. Additional mitigations are being developed and will be deployed through future updates, assuming regulatory approval."

Thubron in *TechSpot* added that the company was monitoring its network "for anyone trying to exploit the flaws." He said that "the defibs will shut down wireless transmission upon receiving any unusual requests. The company is working on a fix for the vulnerabilities, which should arrive later this year."

Medtronic, meanwhile , stated that "To date, neither a cyberattack nor patient harm has been observed or associated with these vulnerabilities."

In the bigger picture, "Medical device makers have bolstered efforts to mitigate product security vulnerabilities in recent years following a flurry of warnings from security researchers who have identified bugs in devices like the Medtronic implant programmers," said Reuters.

# Why the next terror manifesto could be even harder to track

**By Megan Squire**

Source: http://www.homelandsecuritynewswire.com/dr20190326-why-the-next-terror-manifesto-could-be-even-harder-to-track

Mar 26 – Just before his shooting spree at two Christchurch, New Zealand mosques, the alleged mass murderer posted a hate-filled manifesto on several file-sharing sites, and emailed the document to at least 30 people, including New Zealand's prime minister. He also posted on several social media sites links to the manifesto and instructions on how to find his Facebook profile to watch an upcoming video. The video turned out to be a 17-minute Facebook livestream of preparing for and carrying out the first attack on March 15. In his posts, the accused killer urged people to make copies of the manifesto and the video, and share them around the internet.

On March 23, the New Zealand government banned possession and sharing of the manifesto, and shortly thereafter arrested at least two people for having shared the video. By then, the original manifesto document and video file had long since been removed from the platforms where they were first posted. Yet plenty of people appear to have taken the shooter's advice, making copies and spreading them widely.

As part of my ongoing research into extremism on social media – particularly anti-Muslim sentiment – I was interested in how other right-wing extremists would use the manifesto. Would they know that companies would seek to identify it on their sites and delete it? How would they try to evade that detection, and how would they share the files around the web? I wanted to see if computer science techniques could help me track the documents as they spread. What I learned suggests it may become even harder to fight hate online in the future.

**To catch a file**

To find as many different versions of the manifesto as possible, I chose an unusual key phrase, called a "hapax legomenon" in computational linguistics: a set of words that would only be found in the manifesto and nowhere else. For example, Google-searching the phrase "Schtitt uses an unamplified bullhorn" reveals that this phrase is used only in David Foster Wallace's novel "Infinite Jest" and nowhere else online (until now).

A few minutes of Google-searching for a hapax from the manifesto (which I'm intentionally not revealing) found copies of the document in Microsoft Word and Adobe PDF formats on dozens of file-sharing services, including DocDroid, DocumentCloud, Scribd, Mega and Dropbox. The file had been uploaded to blogs hosted on Wordpress and attached to message boards like Kiwi Farms. I also found numerous broken links to files that had been uploaded and quickly deleted, like the original versions that the author had uploaded to Mediafire and Zippyshare.

To determine whether all the files were the same, I used a common file-identification technique, generating a checksum, or cryptographic hash, for each manifesto document. A hash is a mathematical description of a file. If two files are identical, their hashes will match. If they are different, they will produce different hashes. After reviewing the file hashes, it became clear that there were only a few main versions of the manifesto, and most of the rest of the files circulating around were copies of them.

A hash can only reveal that the files are different, not how or why they are different. Within the different versions of the manifesto files, I found very few instances where entirely new content was added. I did find a few versions that had color graphics and new cover art added, but the text content itself was left largely unchanged. Most of the differences between the originals could be chalked up to the different fonts and paper sizes set as defaults on the computer of whoever created the copies. Some of the versions also had slightly different line spacing, perhaps introduced as the file was converted from Word to PDF.

The video file was another story. At least one person who watched the Facebook video made a copy of it, and that original video was subsequently compressed, edited, restreamed and reformatted until at least 800 different versions were circulating.

Any change to a file – even a small one like adding a single letter to the manifesto or one extra second of video – will result in an entirely different file hash. All those changes made my analysis of the spread of these artifacts difficult – and also complicated social media companies' efforts to rid the internet of them.

Facebook and YouTube used some form of hash-matching to block most of the video upload attempts. But with all those changes – and the resulting entirely new hashes – 300,000 copies of the video escaped hash-based detection at Facebook. Google also lamented the difficulty of detecting tiny text changes in such a lengthy manifesto.

**More tech, more problems**

Despite the internet companies' claims that these problems will disappear as artificial intelligence matures, a collection of "alt-tech" companies are working to ensure that hate-fueled artifacts like the manifesto and video can spread unbidden.

For example, Rob Monster, CEO of a company called Epik, has created a suite of software services that support a broad collection of hate sites. Epik provides domain services for Gab, an online platform favored by violent extremists like the accused Pittsburgh synagogue shooter, and the company recently acquired BitMitigate, which offers protection against online attacks to neo-Nazi site The Daily Stormer.

Just 24 hours after the mosque attacks, Monster explained on Gab that he shared the manifesto and video file onto IPFS, or the "Interplanetary File System," a decentralized peer-to-peer file sharing network. Files on IPFS are split into many pieces, each distributed among many participants on the network, making the removal of a file nearly impossible. IPFS had previously been a niche technology, relatively unknown even among extremists. Now, calling IPFS a "crazy clever technology" that makes files "effectively uncensorable," Monster reassured Gab users that he was also developing software to make IPFS "easy for anyone … with no technical skills required."

**A shift in tactics**

As in-person hate groups were sued into obscurity in the 1980s, extremism went underground. But with the advent of the commercial internet, hate groups quickly moved online, and eventually onto social media. The New Zealand attacker was part of a far-right social media "meme" culture, where angry men (and some women) justify their grievances with violent, hateful rhetoric.

Widespread adoption of artificial intelligence on platforms and decentralized tools like IPFS will mean that the online hate landscape will change once again. Combating online extremism in the future may be less about "meme wars" and user-banning, or "de-platforming," and could instead look like the attack-and-defend, cat-and-mouse technical one-upsmanship that has defined the cybersecurity industry since the 1980s.

No matter what technical challenges come up, one fact never changes: The world will always need better, smart people working to counter hate than there are promoting it.

*__Megan Squire__ is Professor of Computer Science, Elon University.*

# Hackers can dupe radiologists, AI software

Source: http://www.homelandsecuritynewswire.com/dr20190403-hackers-can-dupe-radiologists-ai-software

Apr 03 – Hackers can access a patient's 3-D medical scans to add or remove malignant lung cancer, and deceive both radiologists and artificial intelligence algorithms used to aid diagnosis, according to a new study published by Ben-Gurion University of the Negev cybersecurity researchers. Click here for video of the attack.

A 3-D CT (computerized tomography) scan combines a series of X-Ray images taken from different angles around the body and uses computer processing to create cross-sectional images (slices) of the bones, blood vessels and soft tissues. CT scan images provide more detailed information than standard X-Rays, and are used to diagnose cancer, heart disease, infectious diseases, and more. An MRI (magnetic resonance imaging) scan is similar, but uses powerful magnetic fields to diagnose bone, joint, ligament, and cartilage conditions.

Malicious attackers can tamper with the scans to deliberately cause a misdiagnosis for insurance fraud, ransomware, cyberterrorism, or even murder. Attackers can even automate the entire process in a malware which can infect the hospital's network.

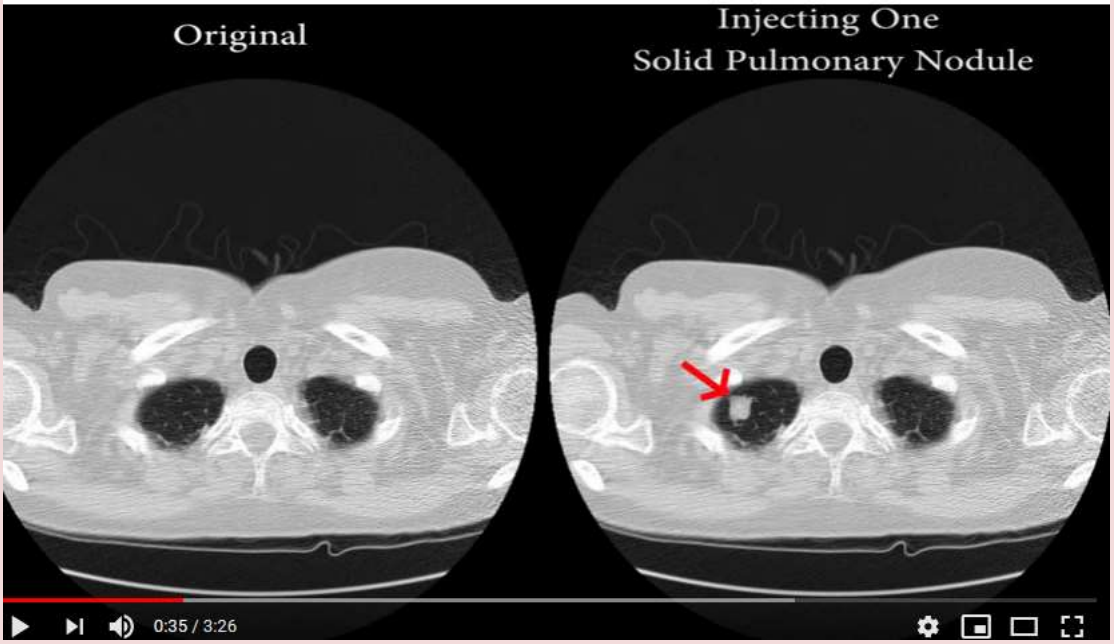
"Our research shows how an attacker can realistically add or remove medical conditions from CT and MRI scans," says Dr. Yisroel Mirsky, lead researcher in the BGU Department of Software and Information Systems Engineering (SISE), project manager and cybersecurity researcher at BGU's National Cyber Security Research Center. "In particular, we show how easily an attacker can access a hospital's network, and then inject or remove lung cancers from a patient's CT scan."

The attacker has full control over the number, size and locations of the cancers while preserving the same anatomy from the original, full resolution 3-D image. This is a significant threat since 3-D medical scans are considered to provide more definitive evidence than preliminary 2-D X-Rays.

To demonstrate the feasibility of the attack, with permission, the researchers broke into the network of an actual hospital and intercepted every scan taken by a CT scanner.

"The scans were not encrypted because the internal network is usually not connected to the internet. However, determined intruders can still gain access via the hospital's Wi-Fi or physical access to the infrastructure," Dr. Mirsky says. "However, these networks are now being connected to the internet as well, which enables attackers to perform remote attacks."

To inject and remove medical conditions, the researchers used a deep learning neural network called a generative adversarial network (GAN). GANs have been used in the past to generate realistic imagery,




such as portraits of non-existent people. The researchers showed how a 3-D conditional GAN can be used to efficiently manipulate high resolution 3-D medical imagery. The architecture (CT-GAN) uses two of these GANs: one trained to inject cancer and the other trained to remove cancer.

The BGU researchers verified the attack effectiveness by training CT-GAN to inject/remove lung cancer using free medical imagery off the internet. They hired three radiologists to diagnose a mix of 70 tampered and 30 authentic CT scans.

When the scans of healthy patients were injected with cancer, the radiologists misdiagnosed 99 percent of them as being malign. When the algorithm removed cancers from actual cancer patients, the radiologists misdiagnosed 94 percent of the patients as being healthy. After informing the radiologists of the attack, they still could not differentiate between the tampered and authentic images, misdiagnosing 60 percent of those with injections, and 87 percent of those with removals.

“In addition to the radiologists, we also showed how CT-GAN is an effective adversarial machine learning attack,” Dr. Mirsky says. “Consequently, the state-of-the-art artificial intelligence lung cancer screening tools, used by some radiologists, are also vulnerable to this attack.”

The researchers proposed some immediate countermeasures which can mitigate most of the threat. One solution is to enable encryption between the hosts in the hospital’s radiology network. In addition, some hospitals can enable digital signatures so that their scanners sign each scan with a secure mark of authenticity. If this approach is followed, then administrators should ensure that proper signatures are being used and that the end devices are correctly verifying these signatures.

“Another method for testing the integrity of the images is to perform digital watermarking (DW), the process of adding a hidden signal into the image such that tampering corrupts the signal and thus indicates a loss of integrity,” Dr. Mirsky says. “Unfortunately, the vast majority of medical devices and products currently do not implement DW techniques.”

## Turning incident scenes into virtual 3D models

Source: http://www.homelandsecuritynewswire.com/dr20190403-turning-incident-scenes-into-virtual-3d-models

Apr 03 – When officers arrive at a crime or crash scene, they have to spend a lot of time looking for evidence, processing it, taking photos of it, and documenting.

To help make this process more efficient, the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) has teamed up with the Israeli Police to invest in a new tool. The tool, called 3D-Hawk, can turn a crash or crime scene into an interactive 3D model within minutes, based on high-definition (HD) video footage. This helps the investigation move from an incident scene to the police station for in-depth analysis, so normal activities can resume. Roads could be cleared sooner, evidence documented more quickly, and investigators could have an exact replica of the scene to build a case and verify witness testimony.

**Introducing 3D-Hawk**

3D-Hawk, an innovative technology, creates 3D models by using standard HD video as a sole source of data. The models recreate, in detail, crash and crime scenes, thus enabling investigators to do their work at any time, at any place, and on

any device.

S&T says that work on the 3D-Hawk started in June 2015 after the Israeli police raised the need of such technology during a meeting with S&T. As part of a bilateral agreement with the government of Israel, S&T engaged in joint research and development efforts that are advantageous to both parties.

"Israel is one of our strongest allies, and they have quite a bit of experience in many of the same first responder challenges and issues we deal with in our country," said Milt Nenneman, S&T First Responder Program Manager, who oversees the 3D-Hawk project.

A product of the Israeli company B-Design3D, the tool consists of an HD video camera, a dedicated Site Survey Set for shooting from above, a short handle for up-close shots, a smart phone for showing what the camera is capturing, and a laptop with software for turning video into 3D models.

Armed with a mouse, investigators can do a number of things with the interactive model. One is moving around the virtual scene. If they want to see in detail a specific location, they can click on it. Another feature of the model is measuring distances and heights by calculating the line of sight to verify witness testimonies.

**Field assessment with Fairfax County Police**

The uniqueness of 3D-Hawk is that it is made mostly for the police and other first responders such as firefighters and bomb squads.

In May 2018, the Fairfax County Police Department (Virginia) was able to try this new tool during an Operational Field Assessment with S&T and its Israeli partners. The 3D-Hawk was tested on three types of mock scenes – a car crash, an outdoor crime scene involving a car bomb explosion, and an indoor homicide.

"First responders with no prior access to the tool were able to record a scene in approximately five minutes. The full rendering of the environment can take up to 30

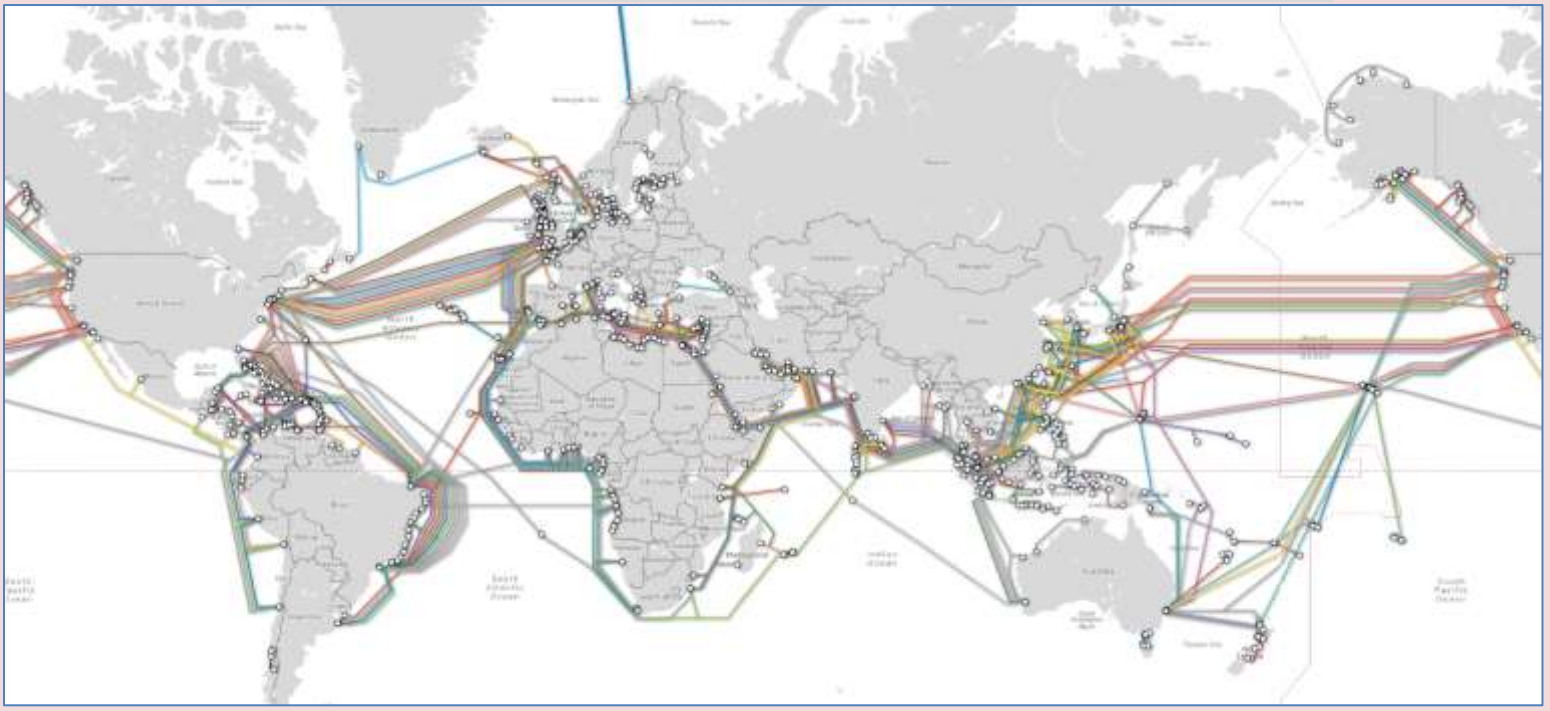
minutes," said Nenneman. "This is significantly less time than the capabilities that currently exist for first responders."
The fake homicide scene depicted a victim sitting on a sofa, his head tilted back, a gun and a suicide note in front of him. The Israeli company asked a Fairfax County Police detective to go around the room with the video camera and shoot the whole room, including its walls, the table beside the victim, and finally, the pistol. Next, the detective turned the videos into multiple 3D models, which he then combined using the 3D-Hawk software.
"You want to show how each layer of the 3D model is a layer in a story that a crime scene investigation officer needs to tell himself, his commander, and the court," said Gil Koubi, Vice President of Marketing for B-Design3D. "The idea is to empower police forces with the power of 3D."
Both the Israeli police and Fairfax Police have incorporated the 3D-Hawk technology into their work and have created thousands of models since the assessment in May.
"I am very impressed with the equipment and the training that we received," said Second Lieutenant Richard Buisch, Fairfax County Police Crime Scene Section. "The 3D-Hawk is much more effective and efficient, and much easier to use than other 3D scanners we have dealt with."
He said the technology can be used successfully to further document crime scenes and reconstruct crash scenes, instead of just taking photos.
After the assessment of the tool, the lieutenant and his detectives provided feedback to S&T and its Israeli partners regarding upgrades involving indoor scenes, ballistic evidence, projector viewpoints and bloodstain patterns.
"If S&T came to me to test more technologies, I would agree 100 percent," said Buisch. "I think my team and my detectives really benefited from it, and I could see us moving forward and possibly trying other devices that can help us in in the field to close criminal cases."
As part of the bilateral agreement, S&T provided three prototypes to be used on a rotational basis by state and local law enforcement agencies; and the government of Israel provided three systems to several of its police units. The Fairfax County Police continue to operationally pilot the 3D-Hawk they used in testing, as are the Ohio Highway Patrol and the Federal Law Enforcement Training Centers.

**In the future**
The Israeli company B-Design3D continues to improve its product based on the feedback it received so that the police can do their jobs better and faster.
"Because of the ease and the relatively brief time it takes to collect an accurate representation of the environment, it is believed that this tool can be used much more frequently than other tools, expanding the use of 3D modeling and law enforcement evidence," said Nenneman.

## China's Next Naval Target Is the Internet's Underwater Cables

By **James Stavridis**
Source: https://www.bloomberg.com/opinion/articles/2019-04-09/china-spying-the-internet-s-underwater-cables-are-next

Apr 09 – As the West considers the threat posed by China's naval ambitions, there is a natural tendency to place overarching attention on the South China Sea. This is understandable: Consolidating it would provide Beijing with a huge windfall of oil and natural gas, and a potential chokehold over up to 40 percent of the world's shipping.
But this is only the most obvious manifestation of Chinese maritime strategy. Another key element, one that's far harder to discern, is Beijing's increasing influence in constructing and repairing the undersea cables that move virtually all the information on the internet. To understand the totality of China's "Great Game" at sea, you have to look down to the ocean floor.
While people tend think of satellites and cell towers as the heart of the internet, the most vital component is the 380 submerged cables that carry more than 95 percent of all data and voice traffic between the continents. They were built largely by the U.S. and its allies, ensuring that (from a Western perspective, at least) they were "cleanly" installed without built-in espionage capability available to our opponents. U.S. internet giants including



Google, Facebook and Amazon are leasing or buying vast stretches of cables from the mostly private consortia of telecom operators that constructed them.

But now the Chinese conglomerate Huawei Technologies, the leading firm working to deliver 5G telephony networks globally, has gone to sea. Under its Huawei Marine Networks component, it is

constructing or improving nearly 100 submarine cables around the world. Last year it completed a cable stretching nearly 4,000 miles from Brazil to Cameroon. (The cable is partly owned by China Unicom, a state-controlled telecom operator.) Rivals claim that Chinese firms are able to lowball the bidding because they receive subsidies from Beijing.

Just as the experts are justifiably concerned about the inclusion of espionage "back doors" in Huawei's 5G technology, Western intelligence professionals oppose the company's engagement in the undersea version, which provides a much bigger bang for the buck because so much data rides on so few cables.

Naturally, Huawei denies any manipulation of the cable sets it is constructing, even though the U.S. and other nations say it is obligated by Chinese law to hand over network data to the government. The U.S. last year restricted federal agencies using from using its 5G equipment; Huawei responded with a lawsuit in federal court. Washington is pressuring its allies to follow its lead — the American ambassador to Germany warned that allowing Chinese companies into its 5G project would mean reduced security cooperation from the U.S. — but this is an uphill battle. Most nations and companies feel that better cell phone service is worth the security risks.

A similar dynamic is playing out underwater. How can the U.S. address the security of undersea cables? There is no way to stop Huawei from building them, or to keep private owners from contracting with Chinese firms on modernizing them, based purely on suspicions. Rather, the U.S. must use its cyber- and intelligence-gathering capability to gather hard evidence of back doors and other security risks. This will be challenging — the Chinese firms are technologically sophisticated and entwined with a virtual police state.

And back doors aren't the only problem: Press reports indicate that U.S. and Chinese (and Russian) submarines may have the ability to "tap" the cables externally. (The U.S. government keeps such information tightly under wraps.) And the thousand or so ground-based landing stations will be spying targets as well.

Once Washington has real evidence of risks that it can share with allies, it can put the security of the Huawei underwater cable operations on the international agenda with the same vigor it has applied in addressing the 5G concerns. This evidence would be the backbone of a strong strategic communications effort to persuade friendly governments and Western companies that working with Chinese won't pay off in the long term. To some extent this is already happening — last year Australia banned Huawei from involvement in a cable it is subsidizing that will connect it to the Solomon Islands.

The U.S. could also flex its technological muscles. Opportunities range from developing less costly alternatives in cooperation with the private sector that can pose price competition to the Chinese; innovating on means to test and protect the information on the cables Huawei Marine does eventually lay; and working to improve end-to-end encryption in all internet-based communications, which would make the task of compromising the security of the information on the cables much more difficult.

As U.S. Admiral Jamie Foggo, a career submariner, told me: "Underwater cables are part of our critical infrastructure and essential to the global economy. The U.S. must protect the integrity and security of them as surely as we provide international freedom of the high seas." So while we certainly need to consider the challenges China poses on the surface of the South China Sea, we also need to look down to the murky depths of the bottom of the sea.

***James Stavridis** is a Bloomberg Opinion columnist. He is a retired U.S. Navy admiral and former supreme allied commander of NATO, and dean emeritus of the Fletcher School of Law and Diplomacy at Tufts University. He is also an operating executive consultant at the Carlyle Group and chairs the board of counselors at McLarty Associates.*

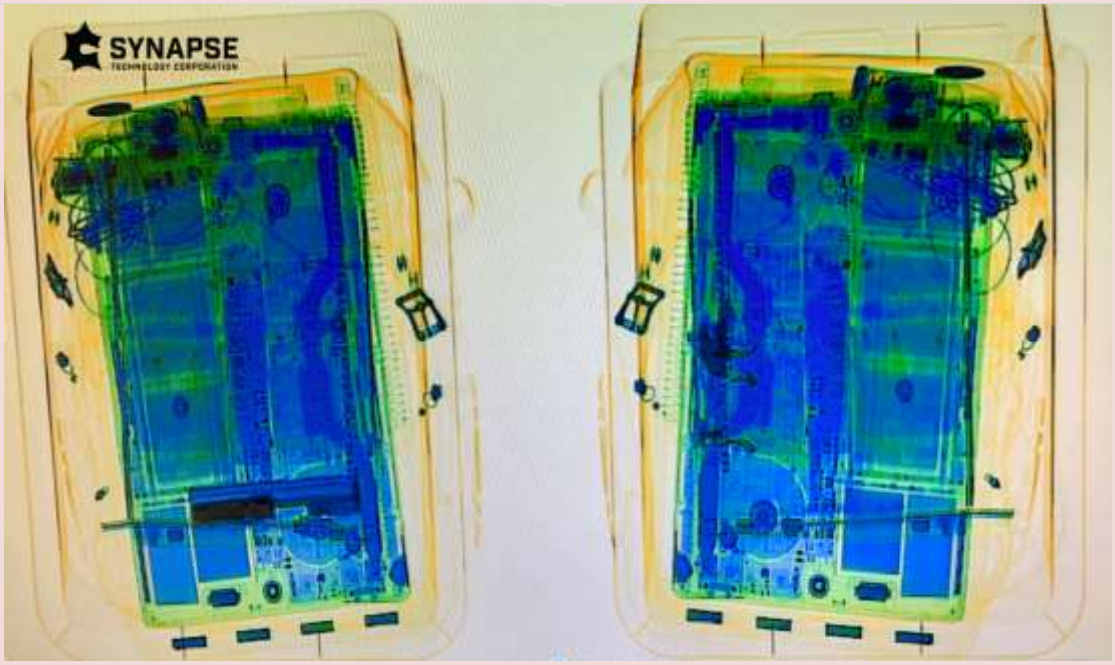
## AI Tech to Revolutionize Baggage Screening

Source: https://i-hls.com/archives/90186

Apr 03 – AI will speed passengers and visitors through checkpoints, lower operating costs, and dramatically improve security. A new Artificial Intelligence (AI) software platform released recently will replace human screening teams in airports. A first of its kind threat detection system for security X-ray machines, this AI software technology can automatically detect weapons, knives and other threats at airports, concert venues, schools and secure facilities.

The Syntech ONE 200 Series developed by Synapse Technology was already ordered by the Osaka Airport for multiple passenger lanes, the first airport to deploy true live AI technologies for baggage screening.

Instead of relying solely on human screeners to identify threats, the system augments and automates the detection of multiple dangerous weapons and items using state of the art artificial intelligence and computer vision.




The technology has already been widely deployed, having processed over 6,000,000 passenger bags at security checkpoints around the world. The US Department of Homeland Security (DHS) also recently granted the company a SAFETY Act award for its technology platform.
The 200 Series represents the first broadly-available plug-and-play system that is compatible with new and existing X-ray security system, according to benzinga.com. Customers do not have to endure costly replacements of their current x-ray technology to garner the performance benefits of this new technology. The system is designed to increase the probability of detection of threats while speeding up throughput at security checkpoints. It leverages big data techniques to provide frequent enhancements, including additional machine capability and additional item detection.

## Hackers could cause disastrous total facilities wipe-out

Source: https://www.itweb.co.za/content/GxwQD71AGA67lPVo

Apr 10 – Many people do not truly comprehend the extent to which computers control the modern world. Everything from traffic lights at intersections, to power plants have automated systems, and for good reason.
These programs allow for a level of efficiency and effectiveness that humans simply cannot provide.
However, this convenience comes at a cost, says **Veronica Schmitt**, lead forensic analyst at DFIR Labs, who will speak at ITWeb Security Summit 2019, to be held from 27 to 31 May at the Sandton Convention Centre.

Her talk is titled: "Total wipe-out: What could happen if cyber criminals successfully attacked a country's critical infrastructure systems."
According to Schmitt, there has not been a system designed that is completely impenetrable, and this is particularly true of the programs guiding the world's critical infrastructure. "Facilities such as power stations are a major attack vector for hackers with the expertise necessary to break into them, and loss of control over them could be disastrous."
Cyber-crime vs cyber warfare
Schmitt says a clear distinction needs to be made between cyber-crime and cyber warfare. Cyber-crime refers to offences which are committed with criminal motives, often with the goal of financial gain for attackers, which intentionally harm the reputation of the victim or cause physical or mental harm or financial loss.

Cyber warfare refers to the politically motivated attacks that can destroy data or cause physical harm to a country's critical infrastructure. An example of this would be the cyber attacks which took place against Estonia, Georgia, and the Ukraine.
The consequences of cyber warfare can be dire. "The worst-case scenario when critical infrastructure is targeted could be the loss of human life. In addition, when a country's critical infrastructure is taken down, the country will fall into chaos."
She believes prevention is not an option as, inevitably, a country at some point in time will be hacked. "The main question is whether they will be able to detect the compromise early on in the attack. The focus should be on hardening the infrastructure to such a degree that a country is no longer an easy or soft target."
Secondary to this would be a disaster recovery management plan that a country needs to have in place to survive total darkness or wipe out of its critical infrastructure. "A contingency plan is needed to survive this as much as one would need to survive a flood. The concerning part is that I don't think the majority of smaller countries have considered cyber warfare as a notable threat which should be planned for, often dismissing the likelihood of them being a target."
Delegates attending Schmitt's talk will learn about the systems which are critical to a country, how they work and can be affected by malware or compromises. She will also outline previous attacks which have taken down critical infrastructure. "The perfect storm in a teacup," she concludes.

## Biologically inspired network protection software

Source: http://www.homelandsecuritynewswire.com/dr20190415-biologically-inspired-network-protection-software

Apr 15 – Engineers at the University of South Florida have developed a new type of cybersecurity software that mimics the human immune system.
It's a concept that's beginning to be explored more and more by researchers in a variety of fields: What does the human body do well and how can we adapt those mechanisms to improve technology or engineering systems?
Researchers in the USF Department of Electrical Engineering looked to the human immune system as a model for intrusion detection in wireless sensor networks. The concepts apply equally well to high-value financial or military mission critical networks that may or may not be wireless. The research was published in Procedia Computer Science and has demonstrated extremely promising results in testing.
"It's very logical to develop these software systems based on human systems," said Salvatore Morgera, PhD, a USF professor of electrical engineering and the project's principal investigator. "Our immune system does a very good job at protecting us – so we wanted to take those mechanisms and adapt them for cybersecurity."
In its simplest form, the human immune system protects the body from pathogens, like germs, viruses and other potentially harmful foreign bodies. If we become infected, our immune system is able to identify and attack the threat in an attempt to keep the body healthy. This idea is exactly what Morgera and his research team hoped to accomplish with their biologically-inspired software. When a network is at risk of being attacked, the software can identify and eliminate the threat. It's essentially an immune system for a digital network.
USF says that to develop the software, Morgera, along with USF doctoral students Vishwa Alaparthy and Amar Amouri, broke the immune system down into three layers. The first layer is external protection; how our bodies prevent pathogens from getting inside. In their software, this layer of protection is encryption – a common cybersecurity tool used to keep unauthorized users out of networks. Most network security methods depend almost exclusively on encryption, and while modern encryption techniques are extremely sophisticated, they are not always successful at preventing intrusion.
To combat this risk, researchers looked to the bodies second layer of protection; non-specific resistance. This non-specific immune response acts as a "catch-all", immediately responding to any foreign-body with a variety of non-specific immune cells. In their software, Morgera and his team developed a similar non-specific response that quickly recognizes

any intrusion and quarantines the threat for further examination. Just like in the human body, this response acts as a first line of defense when threats enter the system.

The third layer that researchers looked at is the immune system's specific resistance to pathogens. This subsystem of the overall immune system is composed of highly specialized cells that respond to specific pathogens. This response also builds immunological memory, leading to an enhanced response after the initial encounter. Just like in our bodies, the USF-developed software learns from each attack and maintains millions of intrusion-fighting templates it can sort through to fight individual threat attempts. As Morgera states, "The need to sort through millions of intrusion-fighting templates can be a computationally complex undertaking." Another researcher, Patrick Lie Chin Cheong, and Morgera have developed a highly efficient 'big data' approach to the sorting that only takes fractions of a second and can be easily implemented on power-limited sensor networks using small microprocessors.

When used in combination, these three mechanisms not only work to keep our bodies healthy but have been shown to be extremely successful in maintaining secure, high value digital networks.

Morgera and his team originally began this research as a potential new tool to secure wireless sensor networks deployed by the military. They have worked in collaboration with U.S. Special Operations Command (SOCOM) to test the software and have seen very promising results. Now, researchers plan to continue to improve the software and make it available for a variety of applications. It's work that may change the future of cybersecurity around the world.

# Qatar ranked third in the region on global cybersecurity index

Source: https://www.qatarliving.com/forum/news/posts/qatar-ranked-third-region-global-cybersecurity-index

Apr 15 – In yet another achievement for Qatar, the country has been ranked third best in the region for cyber security on the Global Cybersecurity Index (GCI) 2018.

Qatar's *initiatives to maintain cyber security* have resulted in the country's enhanced world ranking where it advanced eight positions on the global landscape, moving up to the 17th place in 2018 from the 25th in 2017, reported *Gulf Times*.

| High | | |
|---|---|---|
| United Kingdom | Qatar | New Zealand |
| United States of America | Georgia | Switzerland |
| France | Finland | Ireland |
| Lithuania | Turkey | Israel |
| Estonia | Denmark | Kazakhstan |
| Singapore | Germany | Indonesia |
| Spain | Egypt | Portugal |
| Malaysia | Croatia | Monaco |
| Norway | Italy | Kenya |
| Canada | Russian Federation | Latvia |
| Australia | China | Slovakia |
| Luxembourg | Austria | Bulgaria |
| Netherlands | Poland | India |
| Saudi Arabia | Belgium | Slovenia |
| Japan | Hungary | Rwanda |
| Mauritius | Sweden | Viet Nam |
| Republic of Korea | The former Yugoslav Republic of Macedonia | Uruguay |
| Oman | Thailand | |

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access, according to *Digital Guardian*. Cyber security is highly important for governmental, military, corporate, financial, and medical organizations that collect and process unprecedented amounts of data including sensitive information, for which unauthorized access or exposure could lead to harmful consequences.

The GCI 2018, which assesses the level of cybersecurity in as many as 175 countries across the world, is released by the *United Nation's International Telecommunication Union (ITU)*, according to *Qatar Tribune*.

Based on the ITU's Global Cybersecurity Agenda (GCA), the third version - GCI 2018 - still oversees the level of commitment in five areas: legal measures, technical measures, organizational measures, capacity building, and co-operation.

Qatar has been placed among the top three countries in the Arab region in the GCI 2018, according to *The Peninsula*.

"Qatar ranks third with a strong legal framework and a robust organizational structure with a National Cybersecurity Strategy (NCS) that has a key focus on securing critical information infrastructure and a National Cybersecurity Committee responsible to implement and drive that Strategy. Their eCrime law integrates a large arsenal of procedural measures," GCI noted.

According to the GCI 2018, the Top 10 most committed countries globally are: UK, which ranked first; the US, which placed second; and France, third. Positions from four to 10 were taken by Lithuania, Estonia, Singapore, Spain, Malaysia, Norway, Canada, and Australia, respectively.

Previously, Qatar was also declared to be the *leader in the Middle East for introducing youth to the Internet and cyber security*, according to a survey commissioned by Raytheon Company and the US National Cyber Security Alliance.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

# DRONE NEWS

# A few reasons why cops haven't immediately shot down London Gatwick airport drone menace

**Risk of causing even more embuggerance is high, we repeat: high**

Source: https://www.theregister.co.uk/2018/12/20/gatwick_drone_non_shootdown_reasons/

December 2018 – As the Gatwick drones chaos rolls on, with the airport now set to reopen at 8pm UK time at the earliest*, many people have been asking a simple question-n: why the hell can't the authorities just shoot down the offending drones?

Like all simple questions, the answer is complex. Counter-drones tech is a new field and not quite as easy as you might imagine.

## 1. Shoot the bastard down!

The most obvious solution is to shoot down the drones using a rifle or a shotgun. Here the problem is simple: a rifle bullet fired upwards travels a very long way if it doesn't hit its target, or passes through it. If you're using a .308"/7.62mm rifle pointed upwards at 70 degrees, the dangerous zone in front of it where the bullet could land is up to 2.5 miles or four kilometers long.

Current police issue rifles tend to fire .223"/5.56mm rounds, which can still travel up to 8,000ft (1.5 miles, 2.4km) high if fired at 70 degrees.

Are the police going to evacuate a 2.5-mile strip of West Sussex so they can go all Dirty Harry on the drones? Of course not.

What about a shotgun? This is far more likely than using a rifle. The danger zone for a shotgun firing the usual shot pellets is about 390 ft, or 120 meters, long, according to Blighty's Ministry of Defence. Unfortunately, there's no guarantee that once shot, the drones will land on the spot. A partial hit could send the drones flying off to crash on someone's house (the town of Crawley is next to Gatwick), or leave bits of the drones lying around on the airfield – ready to be sucked into a jet engine. Far from ideal.

It also depends where the drones are flying. If it is not flying directly over the airfield, you would need the landowner's permission to start shooting at it – as well as the permission of every other landowner that both the bullet/shotgun pellets might pass over on their way to the drone, and for good measure the permission of whoever might be the lucky recipient of the spent bullets or shot as they fall to earth. A faff, but not impossible.

Judging by police reports that the drones are "of an industrial specification", it could be that we're dealing with something like a DJI Matrice or an Aeryon Skyranger – larger than your average kid's toy (or a DJI Phantom, for that matter). Shotgun pellets lose energy rapidly: if the drones are flying at a few hundred feet above the ground, it might be the case that it's outside effective shotgun range.

## 2. Jam its signals!

The next thing you could do is jam the command signals controlling the drones. Is that doable?

Doable? Yes. Practical? Not really. Fraught with danger? Oh yes.

It's also illegal.

No, really. Assuming the local police even have access to spectrum analysis equipment that allows them to find what frequency is being used to control the drone, they need legal permission to start broadcasting jamming signals.

That said, maybe they do have spectrum analyser kit?

Either way, the permission the plod need to jam the drones is something they simply don't have right now, as far as we're aware. You need to have authority under the Wireless Telegraphy Act to start broadcasting any kind of signal – even one intended to bring down a fleet of naughty drones.

*(Edit: Our attention has been drawn to S93 (1)(b) of the Police Act, which allows an authorising officer to green-light wireless interference if a serious crime is taking place. Whether or not flying drones over airports is a serious crime – think fraud, violence, or something that would put you away for three or more years – is perhaps a sticking point.)*

But let's forget the law for a bit and think about it. Even if the drones were being flown live, as opposed to following programmed waypoints, simply jamming the control signals introduces a real

problem: where will the drones go? What will it do?
Most modern drones have return-to-base functions that kick in if they lose their control signal. Some do not. And if one of these drones doesn't do that, there's no telling what it might do: it might carry on flying in a straight line until it crashes. Or it could veer off towards all those very expensive airliners parked at the gates. It might even drop out of the sky and onto someone's roof, or greenhouse, or head.
It's just too unpredictable. And as we said, they may be flying on autopilot anyway to avoid control-signal jamming.

**3. Get a trained bird to grab it!**
Too expensive and complicated, according to the flying Dutchmen who actually tried this idea a couple of years ago.

**4. Fly a helicopter next to it and shoot it down! Or throw a net at it!**
Refer to the first point about shooting. Also, what if the drones' operator feels like adding a helicopter kill to their list of "bad things I have achieved today"? All they'd have to do is fly it into the rotor blades – or into the glass canopy protecting the pilots. If the drones are quadcopters, they can manoeuvre in three dimensions, rather than having to fly in a straight line like a normal aeroplane.
Phil Tarry, director of Halo Drones, told *El Reg*: "Other technologies proposed include dropping nets on them. Nets might not be able to go high enough. First you've got to catch them but it seems they're having problems tracking them."

**5. Cut off the GPS so it lands!**
Tarry continued: "I did the training for a system that was to be used during the London Olympics. Everything using GPS within a large area stops. It swamps the receiver. Difficulty with that being, if it's not using GPS, then that won't have any effect. It'll cause significant disruption to GPS, though."
Do you want to be the one who signs off on the use of something that potentially screws over nearby GPS receivers in phones, tablets, and satnavs, and aboard dozens of airliners? No, thought not. Aeroplanes do not rely solely on GPS, and have other navigational systems, but do you want to take that chance given the paperwork involved and potential added travel chaos and looming compensation claims? Do you want to find out the hard way that some planes need GPS to initialise takeoff procedures? Again, thought not.
Tarry also speculated that the drones' operator could in fact be a number of people, based on the drones (plural) appearing and disappearing at intervals during the day, in spite of 280 police on the ground searching for whoever caused this disaster.
"It surely can't be an off-the-shelf DJI system," he said. "Either they've hacked it or it's a kit-built drone."
DJI drones are supplied with geofencing tech baked into their firmware to keep them out of restricted airspace, though, as previously reported, the drones themselves are relatively easy to hack to remove the restrictions. And the drones could be setup to not rely on GPS, thus jamming that may be fruitless.
So there you have it. You can't shoot it down, you may not be able to jam the controls, and disabling GPS may be pointless or non-trivial. At the time of writing, Sussex Police had contacted the British Army for help downing the drones with unspecified "specialised military tech", so perhaps they might shoot them down after all. ®
* This is very likely going to be pushed back soon. Airfield Non-Available times have been repeatedly rolled back by air traffic control throughout the day.

**Updated to add at midnight UTC**
Gatwick airfield is still closed. "Passengers due to fly from Gatwick should check the status of their flight with their airline and not travel to the airport if their flight is not confirmed," the airport spokespeople said in a statement.
"We have called in additional staff right across the airport, many from Christmas leave, and are working tirelessly with police and security partners to halt this drone flying and thank passengers for their continued patience."
While this remains a police-led operation, the military are on hand for support, we're told. Firearms to take down the pesky quadcopters haven't been ruled out after other lines of attack have failed. It is believed the drone, or drones, have been modified to evade the authorities.
Detective Chief Superintendent Jason Tingley, of Sussex Police, said there have been more than 50 sightings of drones over the airport

since 9pm last night, adding: "We have to work on the assumption that this is a professionally prepared drone with the intent of causing the disruption."

## How We Used Drones to Digitize the Biggest U.S. Battleship Ever Made

Source: https://adsknews.autodesk.com/stories/drones-digitize-uss-iowa

## Gatwick Drone Attack 'May Have Been Inside Job'

Source: https://www.silicon.co.uk/workspace/gatwick-drone-attack-may-have-been-inside-job-244117

Apr 15 – Gatwick officials say the attacker had knowledge of airport procedures and may have monitored its communications networks

Police say the drone attack that disrupted flights at Gatwick Airport for 33 hours last December may have been carried out by an insider at the airport.

Sussex Police said the possibility that an insider was involved was "credible", while Gatwick's chief operating officer said the attacker appeared to have knowledge of airport procedures.

"It was clear that the drone operators had a link into what was going on at the airport," said Chris Woodroofe, Gatwick's chief operating officer, who oversaw the facility's response to the incident.

He said the attacker could apparently see what was happening on the runway, or was eavesdropping on the airport's radio or internet communications.

**Detection and response**

The drone used was "specifically selected" as one that could not be seen by the DJI Aeroscope drone-detection equipment Gatwick was testing at the time, Woodroofe told the BBC's Panorama programme, in his first report since the incident.

Sussex Police said it expects its inquiry to take "some months" to complete.

Woodroofe said he did not believe the airport had overreacted by halting flights whilst the drone repeatedly reappeared.

"There is absolutely nothing that I would do differently when I look back at the incident, because ultimately, my number one priority has to be to maintain the safety of our passengers, and that's what we did," he said.

"It was terrible that 140,000 people's journeys were disrupted – but everyone was safe."

Gatwick said it spent £5 million on drone detection equipment following the incident, which Panorama said included two sets of Anti-UAV Defence System (AUDS) gear, one of the systems deployed by the military during the attack.

Woodroofe said he was confident the airport was now better prepared to fend off drone incursions.

"We would know the drone was arriving on site and we'd know where that drone had come from, where it was going to and we'd have a much better chance of catching the perpetrator," he said.

## Parrot's latest drone targets professionals with a thermal camera

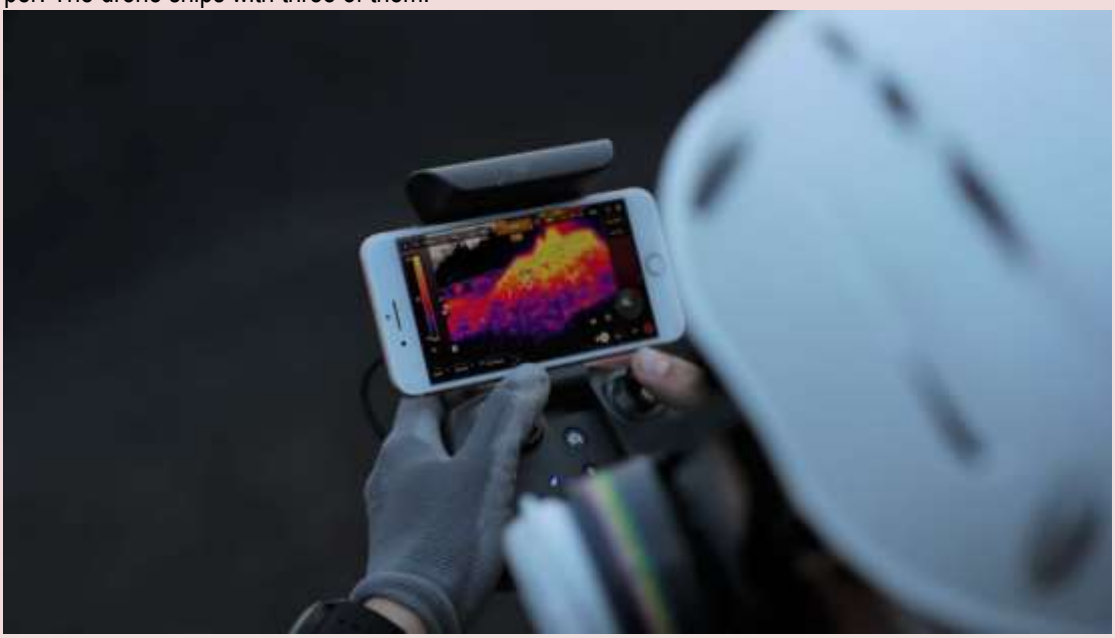
Source: https://techcrunch.com/2019/04/15/parrots-latest-drone-targets-professionals-with-a-thermal-camera/

Apr 15 – The last several years have seen an interesting pivot for Parrot, from Bluetooth headset/speakers to drones. The company's ANAFI line is probably one of the best-positioned products to go head to head with DJI's successful Mavic line, but the company's looking to take things a bit further by moving beyond hobbyists/consumers.

The system's primary differential from other products in the line is the inclusion of the titular thermal camera designed by Flir. The ANAFI Thermal is capable of capturing live images that layer thermal and high-res images.

With this technology, the French company is hoping to open up the drone offering to a wide range of fields that can use the technology for things like surveillance and inspection. The list of potential use cases includes firefighters, solar panel inspections and building industry/construction workers, who can monitor things like insulation and thermal leakages in buildings.


The system also includes a 4K HDR camera with 21-megapixel sensor and 3x digital zoom, mounted on a gimbal that's capable of tilting 90 degrees up and down. That last bit should also prove helpful for things like building inspections. The batteries, meanwhile, are slightly better than recent models, at 26 minutes per. The drone ships with three of them.



The ANAFI Thermal arrives next month, priced at $1,900.

## These are the seven new drone industry trends

Source: https://www.geospatialworld.net/blogs/these-are-the-seven-new-drone-industry-trends/

Apr 12 – Telecom will be a major beneficiary of the drone industry and there will be rapid growth in the counter drone technology, according to PWC.

Among other things, it was also noted that drones and photogrammetry are becoming standard tools in mining while UAV urban mobility pilots are taking wings, especially across Europe.

These were the revelations by Michael Mazur, Consulting Partner and head of PwC Drone Powered Solutions. Azur was delivering one of the keynote addresses at the Commercial UAV Expo Europe, in Amsterdam.

**Telecom will benefit immensely from drone industry**

Mazur said that while analysts predict that revenue for the telecom industry will drop by 5% per year for the foreseeable future, drones may offer the companies a new revenue stream. That's because Unmanned Traffic Management (UTM) systems will require consistent communication between drones and air traffic or other UTM services. The huge amounts of data generated by drone missions would have to be communicated in one way or the other, and telecom companies will reap the benefits.

**Energy grid operators are scaling up autonomous detection of failure modes**

Grid operators are increasingly using drones to keep the grid up and running, moving from a reactive maintenance model to a preventive maintenance model. Using LiDAR and photogrammetry, grid operators can create digital models of the grid; using AI-powered analysis tools, they are able to monitor vegetation growth, identify failure modes and create preventative maintenance plans.

**Drones and photogrammetry are becoming standard tools in mining**

"The time to do an open mine survey has moved from two weeks to two days using drones," pointed out Mazur. In an industry, where difficult terrain is common, drones make sense for many applications. Mining regulations require that mines be monitored even after they are no longer working, so making the entire process as cost-effective as possible is critical to profitability. Stockpile measurement through photogrammetry is another drone mission being accepted as standard in the industry, he added.

**UAV urban mobility pilots are spreading across Europe**

"In the EU, traffic congestion in urban areas is currently estimated to cost 100 billion pounds per year," said Mazur. In Europe's crowded cities, many urban planning experts see expanding traffic up — using drones as part of an integrated and multimodal transportation system — as the only option to improving the situation.

**UTM models are being refined and rolled out across Europe**

UTM is a critical step in the growth of the drone industry and its not too far in the future. UTM models are currently being implemented across Europe, having an impact on the global drone community.

**Rapid growth in counter drone technology**

The growth of rogue drones causing problems in sensitive areas is for real. "Counter drone technology is growing faster than DJI revenue," Mazur said on a lighter note. With some highly publicized drone incidents like the Gatwick Airport fiasco, regulators are showing interest in the development and implementation of counter drone technologies.

**BVLOS will become standard in Europe**

"The country of Malta had just announced a complete survey of all the roads in the country over the last 2 months with no accidents," said Mazur. Mazur believes that drone flight beyond visual line of sight (BVLOS) will become standard in Europe. BVLOS flight opens commercial drone operations like large scale infrastructure inspections, remote operations and drone delivery.

## Unique Kite Drone to be Mounted on Emergency Vehicles

Source: https://i-hls.com/archives/90667

Apr 18 – A new technology integrates an autonomous tethered "kite" drone in emergency vehicles to help provide firefighters with situational awareness. In fact, this is a completely new product category which allows first responders to quickly gain aerial situational awareness.

The development is the result of a collaboration between the startup Fotokite and Pierce Manufacturing, a supplier of firetrucks.

Equipped with two cameras — one low-light visual, one thermal — the Pierce Situational Awareness System by Fotokite (SIGMA) is a tethered six-rotor c-drone in a cradle which can be mounted into any fire vehicle, including non-Pierce vehicles.


The two cameras provide simultaneous thermal and regular video streams. The custom integrated camera payload is actively stabilized in 3 axes to ensure maximum situational awareness and operational flexibility throughout deployment, according to the company website.

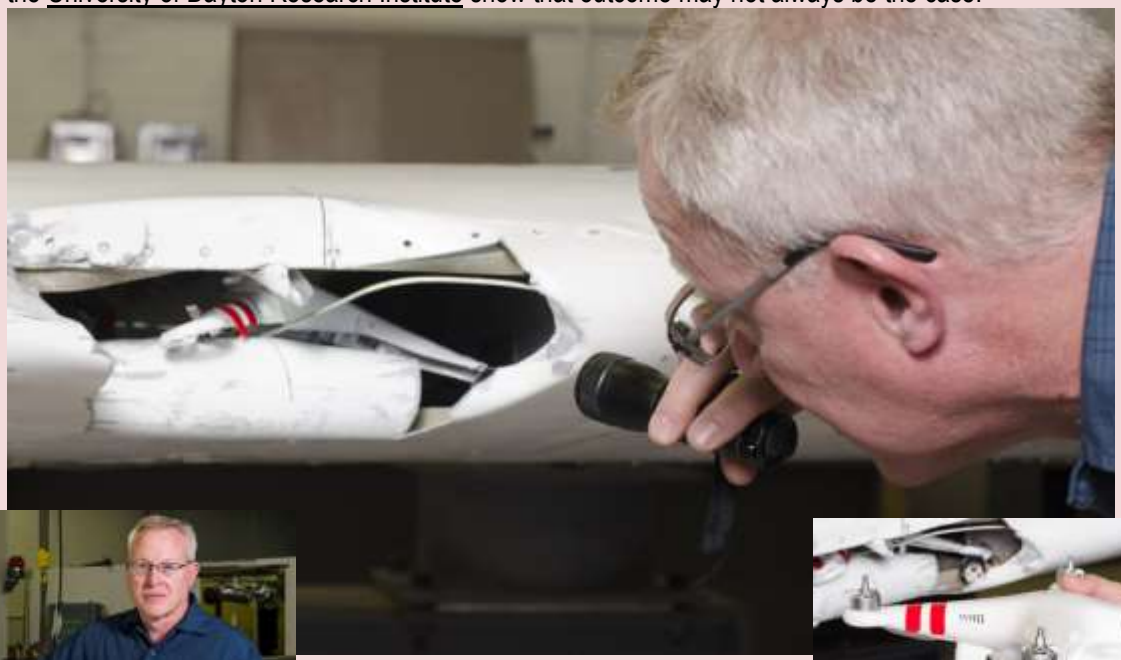
For vehicles without room to mount the standard sliding drawer configuration, a Pelican case standalone version is available; all it needs is a power connection to the host vehicle. No pilot or license is necessary; a Fotokite software application, Fotokite LIVE, allows any firefighter to launch or retrieve the drone with a touch of a tablet or computer screen button with a slider for the desired altitude up to 150 ft (46m), the Federal Aviation Administration (FAA) ceiling for tethered drones ("Public Actively Tethered UAS") which just came into effect last week.

Connectivity to the software is through WiFi or Ethernet for wireless-denied environments. The thin but extremely strong tether provides power and secure data/video link to the drone, which has a solid carbon fiber frame and can continue controlled flight with only five rotors operating.
The tether allows 24+ hours of flight; it is never necessary to change batteries as there aren't any (except for backup power for both the ground station cradle and the drone).
Christopher McCall, CEO of Fotokite, said that the Pierce Situational Awareness System is available today for fire departments and emergency responders across North America. It can be installed in any emergency vehicle. It is pilotless and requires no licenses, waivers, or training to use in the US.
The system consists of the Ground Station and the Kite. A tablet computer runs Fotokite LIVE and receives the thermal and low light video streams, giving teams actionable information throughout their mission.

## When planes and drones collide

Source: https://udayton.edu/momentum/stories/udri-drone-test.php

When a large military helicopter collided midair with a small quadcopter in 2017, the helicopter sustained only minor damage and returned safely home; the drone was destroyed. But tests performed at the University of Dayton Research Institute show that outcome may not always be the case.



In a test designed to mimic a midair collision at 238 miles per hour, researchers in UDRI's Impact Physics group launched a 2.1-pound DJI Phantom 2 quadcopter at the wing of a Mooney M20 aircraft. The drone did not shatter on impact. Rather, it tore open the leading edge of the wing as it bore into the structure, damaging its main spar.
"While the quadcopter broke apart, its energy and mass hung together to create significant damage to the wing," said Kevin Poormon, group leader for impact physics at UDRI.
As the number of hobby drones in the air dramatically increases, so does the risk of a catastrophic event, Poormon said. "We've performed bird-strike testing for 40 years, and we've seen the kind of damage birds can do. Drones are similar in weight to some birds, and so we've watched with growing concern as reports of near collisions have increased, and even more so after the collision last year between an Army Black Hawk helicopter and a hobby drone that the operator flew beyond his line of sight."

Although the helicopter returned home with only minor damage to a rotor, Poormon said it is only a matter of time before a drone strike causes more significant damage to a manned aircraft. To educate the community, Poormon presented test results and video of the drone shot at the fourth annual Unmanned Systems Academic Summit.

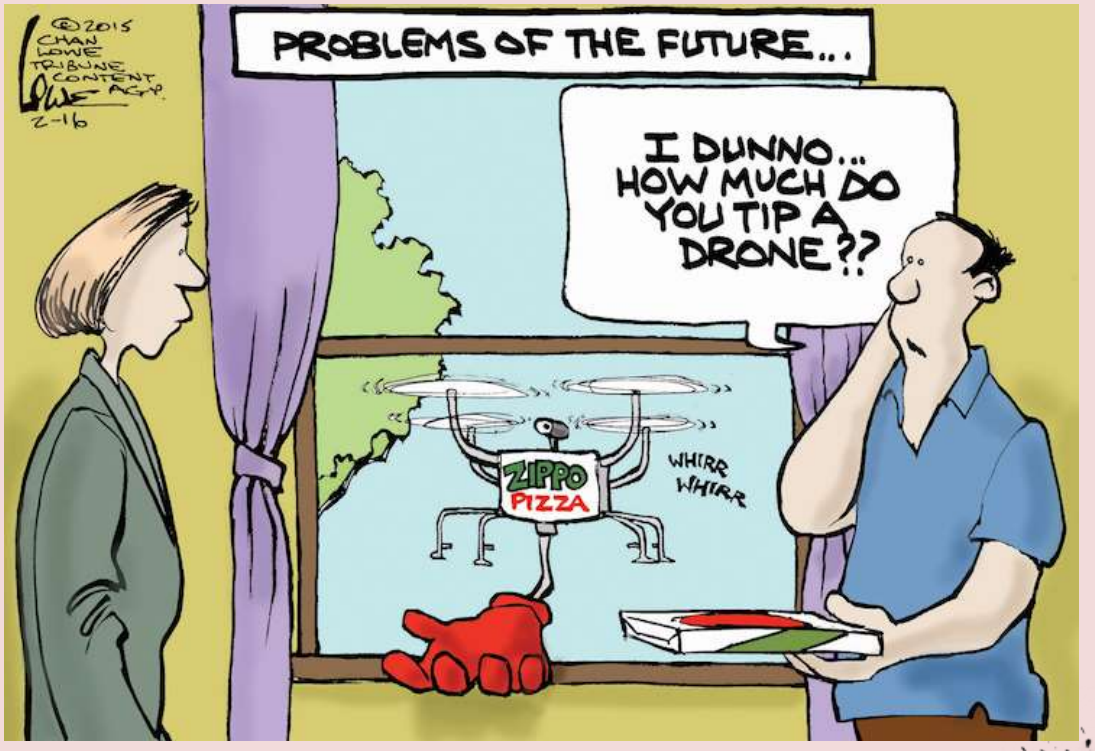
"We wanted to help the aviation community and the drone industry understand the dangers that even recreational drones can pose to manned aircraft before a significant event occurs. But there is little to no data about the type of damage UAVs can do, and the information that is available has come only from modeling and simulations," said Poormon. "We knew the only way to really study and understand the problem was to create an actual collision."

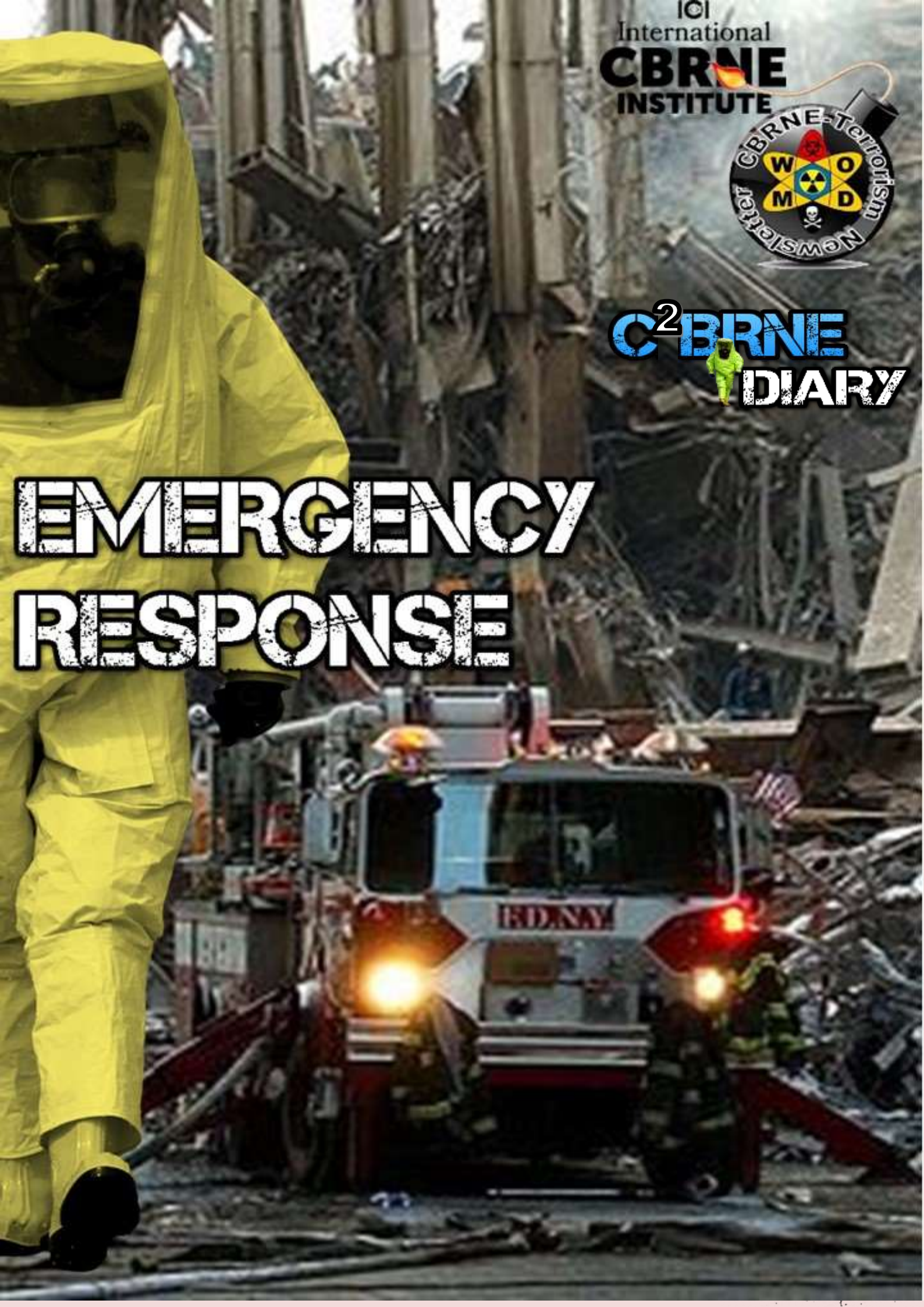
Poormon and his team collaborated with the Sinclair College National UAS Training and Certification Center, whose experts provided guidance on unmanned aerial systems. "We're fortunate to be in close proximity to Sinclair's nationally renowned UAS Center," Poormon said. "We're experts on bird strikes, but Sinclair's team provided valuable insight on how these systems are being used and helped us determine the best models for testing."

After calibration work to ensure they could control the speed, orientation and trajectory of a drone, researchers fired a successful shot at the Mooney wing. The researchers then fired a similarly weighted gel "bird" into a different part of the wing to compare results. "The bird did more apparent damage to the leading edge of the wing, but the Phantom penetrated deeper into the wing and damaged the main spar, which the bird did not do."

Poormon said additional tests using similar and larger drones on other aerospace structures, such as windscreens and engines, would provide critical information about how catastrophic a collision would be. He and his team are hoping even this first test result will help bring awareness to the manned and unmanned aviation communities about the importance of regulations related to safe drone operating.

In addition to the FAA regulations already in place for drone operators, Poormon noted other factors that could help enhance safety, such as building drones to be more frangible — meaning they'll shatter more easily on impact — or keeping them under a certain weight limit.




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

# The True Test of a Successful Crisis Response: Public Trust

**By W. Craig Fugate**

Source: https://www.domesticpreparedness.com/resilience/the-true-test-of-a-successful-crisis-response-public-trust/

June 2017 – No organization, or government, can solve every problem. There will always be a crisis that will require an emergency response. And fundamental to the success of that response will be the public's reaction. Emergency managers can react and can mobilize, but they will not be successful unless they do so in such a way as to ensure the public trust. This was apparent in 2005 with Hurricane Katrina, which was a crisis of government.

Emergency managers must approach every crisis considering the following: "How are we ensuring the public maintains its confidence in us?" "Are we maintaining the public trust?" The answers to these questions will be the true test of success.

Be Prepared, Be Credible & Communicate


First and foremost, to help maintain public trust, emergency managers must be prepared to provide a credible, timely response to a crisis. They must be prepared to meet basic needs through responders and perform to the best of their abilities. The path to achieving this is clear, with resources and trainings available to ensure managers can deliver.

But another, equally critical aspect that many emergency managers do not consider or are not comfortable performing is communicating with the public – being honest and transparent to the public, as quickly and as completely as possible. There is this mindset that says, "Don't tell the public. They'll panic." That is not good advice. Transparency is needed to earn and maintain trust. If senior government officials say one thing, and responders say something different, then distrust is created. And, if people find out they have been misled or purposefully misinformed, that is really bad.

Building public trust is achieved by knowing what to tell the public. First, be clear on the objectives. Let the public know what emergency managers are looking for and what they are looking to do. Then, tell them in real time what is being done; keep communicating throughout and keep these lines open. And, let them know what is expected of them too. Be concise so everyone understands.

Next, let people know if there will be challenges. Do not say everything is going to be okay when it is not. Do not say there will not be problems, when there will definitely be problems. Be realistic. People must have a realistic understanding of the situation. If something will take days to resolve, tell them it will take days.

**A Successful Case of Achieving Public Trust**

The Tylenol tragedy of 1982 is a textbook example of how to successfully maintain public trust. Bottles of Tylenol were laced with cyanide, which resulted in several deaths. Johnson & Johnson, the company that makes Tylenol, did not wait for answers: "Was it local?" "Did it come from a lone plant?" They did not know, and they did not care at that point; they pulled ALL their products off the shelf. That was their step one – they provided a credible response.

Johnson & Johnson also told their customers what they were doing: They told their customers they would not put products back on the shelves until they were sure they were safe. They communicated throughout the process. They distributed warnings to hospitals and distributors and advertised across national media, warning people not to take any of their products that contained acetaminophen once they determined that these were the capsules that had been affected. The company was clear and concise; they told people what to expect, and they did not "sugar coat" anything.

They also added a critical third piece: they put public safety ahead of their own bottom line. The company did not wait for information or try to minimize the effect on their supply chain. They just pulled all the products. Their reputation was more valuable than anything and, as a direct result, they successfully protected that reputation.

**Disasters – Inherently Chaotic**

Emergency management is what happens when the traditional organizational chart is no longer capable of managing the crisis. As such, emergency managers must provide a successful response and they must maintain the public's trust. If the public's trust is lost, it is not possible to get that time or that credibility back.

***W. Craig Fugate*** *is currently senior advisor to the chief executive officer at The Cadmus Group Inc. Previously, he served as the Administrator of the U.S. Federal Emergency Management Agency (FEMA) from May 2008 to January 2017. Prior to his tenure at FEMA, he served as the state of Florida's emergency management director from 2001 through 2009. In 2016, he received the National Emergency Management Association (NEMA) Lacy E. Suiter Award for lifetime achievements and contributions in the field of emergency management.*

# Core Principles of Threat Management Units

**By Michael Breslin**

Source: https://www.domesticpreparedness.com/resilience/core-principles-of-threat-management-units/

Apr 10 – Homeland security is a complex and ever-evolving challenge whose mitigation necessitates the actions and collaboration of personnel across all branches of government and the private sector. This enhanced complexity presents law enforcement, homeland safety, and security professionals with a myriad of challenges due to an environment overflowing with existential and hybrid threats, technological innovation, interconnectivity, and limited resources.

The risks faced by the public are real and the dangers posed by those intent to do harm seem to occur on a daily basis. The United States is an open society with hard-fought liberties. These freedoms combined with geopolitical and domestic conditions provide a ripe environment for those lone individuals and bad actors intent on causing harm to disrupt this way of life.

The report, *Mass Attacks in Public Spaces – 2017*, published by the United States Secret Service's National Threat Assessment Center (NTAC) provides valuable information about mass attacks in the United States. The report examines attacks, from January 2017 through December 2017, where three or more were injured in public spaces. During this timeframe, 28 such attacks occurred and resulted in the loss of 147 lives and injury to nearly 700 others.

Threat Management Units

In the absence of enough threat management units (TMUs) and the ongoing debate over homeland safety funding and public safety initiatives, the NTAC report was disseminated to the Department of Homeland Security (DHS) Office of State and Local Law Enforcement, Fusion Centers, DHS Protective Security Advisors, International Association of the Chiefs of

Police, and the Major County Sheriff's Association. It provided insights into the targets, locations, and methods of attack. The backgrounds and behaviors of the perpetrators – including history of criminal activity, concerning behaviors, communications, mental health symptoms, stressors, and other factors – were explored and presented by the NTAC report.

Public sector organizations of all types share commonalities in their respective operational missions (e.g., investigative, protective, emergency preparedness, health and safety capabilities). These organizations share in the collective challenges presented by diminishing financial, personnel, and subject matter expertise resources.

Due to these circumstances, the establishment and enhancement of existing TMUs is a vital component required to successfully identify risk factors, create an environment that reduces or prevents acts of violence, and mitigate the threats of violence posed to the public. Law enforcement and public safety professionals serve a critical role in the threat management process. The immediate and effective response to all threats against the public and facilities is essential to the successful execution of this grand mission requirement.

TMUs should deliver a comprehensive, coordinated, and multifaceted investigative approach and response to all threat-based intelligence. An effective and wide-ranging threat management process organized through a TMU results in a timely, comprehensive, and factual based recommendation, assessment, and evaluation of the risk of violence toward the public, facilities, or events.

The threat environment has evolved despite numerous successes of public safety professionals in the identification and mitigation of foiled attempts to disrupt and cause harm. Bad actors and lone individuals prepare daily to hone their tradecraft on new ways to inflict maximal damage and instill fear among the populace. Lone offenders, homegrown violent extremists, international terrorist groups, and transnational criminals pose asymmetrical threats. The internet serves as an available platform for accessing and sharing these severe ideologies, propaganda, and threatening language, which can inspire acts of violence.

Given the number, types, and ways that threats expand, various elements contribute to a successful TMU program. Partnerships and training are two of the most pressing elements that must be continuously reinforced.

Partnerships are crucial because of information sharing, leveraging resources, and best practices. Partnerships create the dependable, trusted relationships needed during a time of crisis. Training reinforces what works and reduces gaps in response actions. Partners have to train with and without each other before a crisis in order to be ready.

Lessons Learned From the Secret Service

Following are some of the lessons learned gathered by the author, a former Secret Service agent, who was tasked with solving complex problems in protecting Americans. The lessons were learned during the preparation required in securing high-profile elected officials and managing protective intelligence units and investigations.

Partnerships combined with training are the heart and foundation of a TMU. The revolving nature of ubiquitous threats demand the development by law enforcement, public, and safety professionals of new nontraditional countermeasures. These countermeasures must be both proactive and comprehensive, utilizing the full complement of their investigative and protective capability and fully exploiting global, national, state, and local resources.

*Community partnering.* All threat intelligence activity – including investigative, protective, social media monitoring, tracking, and trend analysis of suspicious reports and activity – yields more positive results with a renewed focus on community partnering. Paramount in this tool kit is the need for increased outreach and liaison with internal and external partners. Agency leadership should ensure this initiative is conducted in collaboration, coordination, and integration across their organizations. It should also be done in partnerships within the law enforcement, mental health, and education communities with the public and private sectors in the specific communities they serve as well as in a broader geographical context. With this approach, the TMU establishes a holistic approach to the community.

*Community intelligence.* The concept of community intelligence as an informational gathering process involving key public and private stakeholders for receipt and dissemination of relevant ground-level information is a tool that should be exploited. Below are some

examples of agencies where the professional experience, knowledge, skills, and abilities of their workforce should be fully leveraged and geared toward a singularity of focus. The identification, mitigation, and management of threats toward those whose safety they are charged with safeguarding are very important in the process. With so many places to gather information, the following list is a start:

- State Fusion Centers
- FBI – Joint Terrorism Task Force
- DHS – Office of Intelligence & Analysis
- U.S. Attorney's and State Attorney's Office Liaison
- Mental and Community Health Centers
- University and Community College Police
- School Boards & Associations
- Airport Intelligence Liaison
- Homeless Shelters and Community-Based Organizations

*Suspicious activity.* Each community partner defines "suspicious activity" differently. It is helpful to define and know how every partner defines this term. In the case of building a TMU for the Secret Service, suspicious activity is defined as observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Community partnerships can be sustained through information sharing of all types of suspicious activity with all law enforcement, public safety, and private sector stakeholders. The benefits include a more fully engaged interagency collaborative. Guidelines to follow are outlined in the Nationwide Suspicious Activity Reporting Initiative led by the National Criminal Intelligence Resource Center. A good checklist to read is "10 Ways to Integrate Suspicious Activity Reporting Into Your Agency's Operations."

*Individual and shared responsibilities.* Law enforcement, public safety and security, government, and private sector agencies have a key role to play in safeguarding the public. However, the role of individuals and their importance in playing an active part in this joint effort cannot be undervalued. The collective goal is the development and enhancement of a TMU with a seamless threat identification and mitigation plan to create a safe and secure environment.

*Free resources.* The complete leveraging of existing partnerships and capacity by law enforcement and public safety professionals may be accomplished at a minimal cost to the agency. These professionals should build on their trusted partnerships with government and private industry to gain expertise in the realm of threat identification and mitigation. The professional development and immersion of its supervisors and employees in the principles of threat intelligence, investigative principles, and risk management will, in time, permeate the culture and daily practices of the workforce. Law enforcement is increasingly using threat intelligence as a tool for threat mitigation in areas such as school and workplace violence. As such, numerous complimentary resources available – such as associations, newsletters, and alerts – should be tapped.

Multifaceted Training

A robust training program needs to be established in conjunction with a comprehensive outreach program to enhance the skill set and strength of existing partnerships. The establishment of a proactive training methodology is necessary for the conception, development, and execution of public safety planning. The emphasis on training should be addressed by leadership and subsequently reinforced to all civilian, law enforcement, and private sector partners. A multifaceted training program should be developed, consisting of numerous tabletop and dynamic exercises in support of the threat management process.

The tabletop exercises should introduce a range of scenarios that could affect the protected people, facility, or venue. Scenarios should be all encompassing and meant to facilitate responses from law enforcement, fire, medical, emergency management, and legal professionals. The purpose of the training is to ensure a continuity of operations concerning the command and control function, particularly during a multipronged response platform.

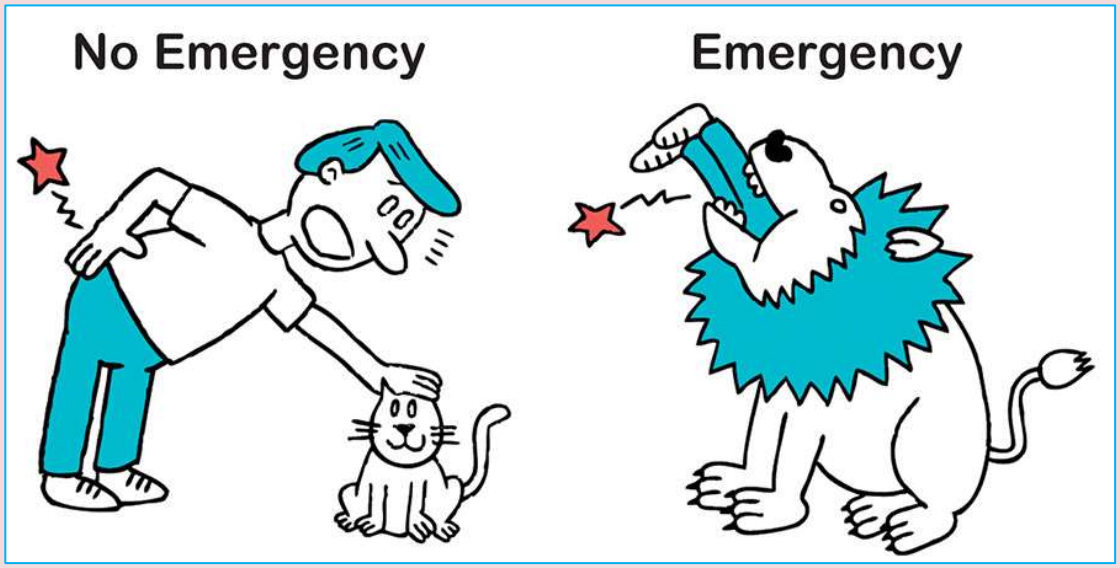
A successful training methodology is one that prepares stakeholders for the unforeseen event, despite deficiencies in resources, personnel availability, and time. Professional trainers and those with subject matter expertise can adeptly infuse their professional experience, knowledge, and abilities to complement the skills of a veteran workforce across multiple organizations.

A professional training program would help foster a collaborative learning environment to address challenges facing the public safety community.

Training programs focused on mental health, work-life balance, stress and violence indicators, social media monitoring, trend analysis, outreach, and suspicious activity are an integral part of an effective TMU. "The use of TMUs remain the most viable and effective method for recognizing and disrupting planned attacks of targeted violence" (Behavioral Threat Assessment Center, Department of Justice, October 2013).

These lessons learned recommendations incorporate the best practices of information gathering for the expansion of partnerships and training, resulting in improved results and better functioning TMUs. The goal is to expand the reach and effectiveness of law enforcement and public safety agencies' coverage, capacity, and capability. Implementing these best practices would increase mission effectiveness and improve aptitude to outline and communicate trends in potential violence-related activity, specific threat reporting in the impacted zone, threats to critical infrastructure, and overall situational awareness of intelligence matters with explicit impact on the specific organization.

***Michael Breslin*** *is the strategic client relations director for LexisNexis Risk Solutions, government. As strategic client relations director for federal law enforcement, he plays a critical role in further driving the expansion of executive relationships and innovative solutions designed to meet the evolving needs of law enforcement agencies. He has more than 20 years of federal law enforcement experience working with the United States Secret Service and the Department of Homeland Security. Before joining LexisNexis Risk Solutions, he served as deputy assistant director for the Office of Investigations for the Secret Service, where he oversaw the planning and coordination. Throughout his career, he has initiated and managed transnational cyber and financial crime investigations of network intrusions and the theft and safeguarding of data and information from corporate, financial, and government institutions. He helped develop security solutions that protected U.S. and foreign dignitaries and facilities including the U.S. president, vice president, and visiting heads of state. As the special agent in charge of the Criminal Investigative Division of the Secret Service, he led a staff of 153 administrative, professional, technical, and special agents working on counterfeiting, financial, electronic, and cyber crimes. He holds a bachelor of arts from St. John's University, Queens, New York. He also holds a master of science degree in national security strategy and a graduate certificate in business transformation and decision making from the Industrial College of the Armed Forces, as well as a master of public administration from John Jay College of Criminal Justice.*




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

# Stern warning: Climate expert emphasizes the fierce urgency of now

**By Peter Dizikes**

Source: http://www.homelandsecuritynewswire.com/dr20190411-stern-warning-climate-expert-emphasizes-the-fierce-urgency-of-now

Apr 11 – Prominent economist and policymaker Lord Nicholas Stern delivered a strong warning about the dangers of climate change in a talk at MIT on Tuesday, calling the near future "defining" and urging a rapid overhaul of the economy to reach net zero carbon emissions. "The next 20 years will be absolutely defining," Stern told the audience, saying they "will shape what kind of future people your age will have." "Don't underestimate the size of the challenge," Stern added, while giving the MIT Undergraduate Economics Association's annual public lecture.

To consider the climate trouble we are already in, Stern noted, consider that the concentration of carbon dioxide in the atmosphere is now over 400 parts per million, a level the Earth has not experienced for about 3 million years, long before people were around. (The modern human lineage is estimated to be about 200,000 years old.)

Impression of Florida after rise of sea height // Source: jpl.nasa.gov

Back then, sea levels were about 30 to 60 feet higher than they are now, Stern said. The recent rise in carbon dioxide concentrations has created rapidly increasing temperatures that could raise the ocean back to those pre-human levels — which would profoundly alter our civilization's geography.

"It would be Oxford-by-the-Sea," Stern said, referring to the English university seat that lies about 50 miles inland at present. "Bangladesh would be completely underwater." Moreover, Stern noted, "Southern Europe would probably look like the Sahara Desert."

And with a 2-degree Celsius rise in average temperatures, Stern pointed out, the proportion of people on Earth exposed to extreme heat would jump from 14 percent to 37 percent.

"This is the kind of heat that can kill, in a big way," Stern warned.

**"Net zero is fundamental"**

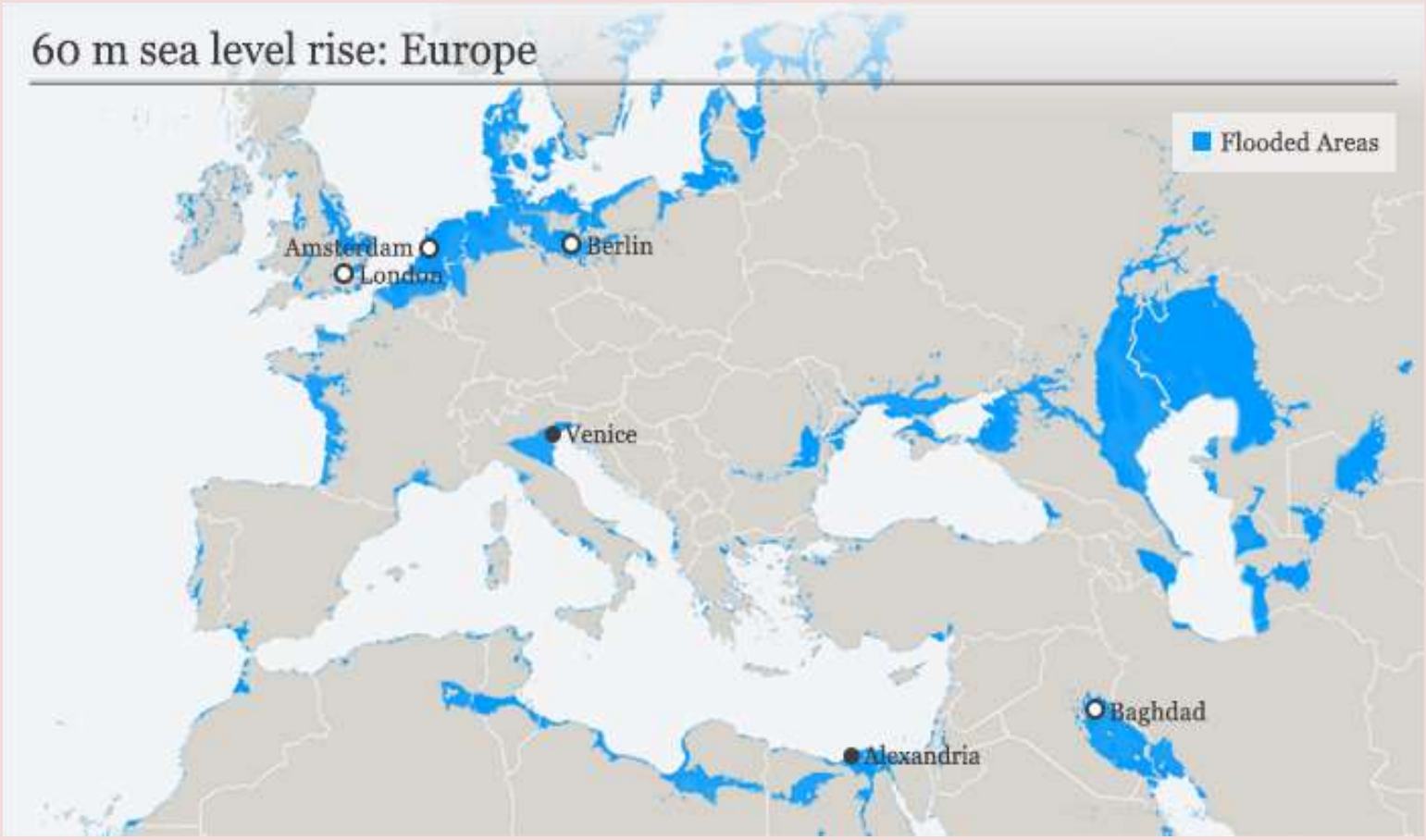
As dire as those scenarios seem, Stern also expressed some optimism, saying that policymakers are now much more likely to believe that we can combine continued economic growth with zero-emissions technology — a change from common views expressed at, say, the 2009 global climate summit in Copenhagen.

"What we've seen I think in the last five years or so is a change of understanding of the policy toward climate change," Stern said, "from 'How much growth do we have to give up to be more responsible and sustainable?' to 'How can we find a form of growth that's different and sustainable?'"

However, he warned, a world with a net of zero carbon dioxide emissions within a few decades will be absolutely necessary for society to maintain its current form.

"The net zero is fundamental," Stern said. "That's not some strange economist's aspiration. The net zero is the science. If you want to stabilize temperatures, you're going to have to stabilize concentrations. Stabilizing concentrations means net zero."

Stern's lecture, "Unlocking the Inclusive Growth Story of the 21st century: The Drive to the Zero-Carbon Economy," was delivered to an audience of over 100 people in MIT's Room 2-190, a lecture hall.
As part of his remarks, Stern contended that the overhaul of energy production and consumption could have leveling economic benefits globally. Indeed, a successful transformation of energy use would almost by definition have a broad impact, he said, since about 70 percent of energy involves infrastructure and 70 percent of growth in coming decades may be located in the developing world.
Multiplying those factors, Stern said, "Half of the story is infrastructure in developing countries and emerging markets."
Among many specific urban climate measures, Stern suggested that, for instance, "if cities banned internal-combustion engine cars [from] coming into the [city] centers by some date, say, 2025, that would radically change the kinds of cars that come to market." And he touted the ability of policymakers to effect change, citing the massive global switch to more efficient LED light bulbs as one case where lawmaking has created massive improvements in energy efficiency.




**It's not enough to talk**
Stern is an accomplished economist who has studied development and growth extensively, and shifted his focus to include climate economics over the last two decades. He is professor of economics and government and chair of the Grantham Research Institute on Climate Change and the Environment at the London School of Economics.
Stern may be best-known in public for his work as a minister in Britain's Treasury Department, where he spearheaded a major report on climate and economics, released in 2006. In 2007, Stern was made a life peer in Britain in 2007, and sits in the House of Lords — as a nonpartisan member, he reminded the audience on Tuesday. Stern was chief economist of the World Bank from 2000 to 2003, and president of the British Academy from 2013 to 2017.

As Stern remarked at the beginning of his talk, he also spent a year at MIT in the early 1970s, working with MIT economist Robert M. Solow. Stern said the Institute has "been my U.S. home" through the years. At one-point, Stern asked audience members to raise their hands if they were economists; a significant percentage of people in the room did so.

"Those of you who are not economists," Stern quipped, "it was your decision, and you have to live with it."

Stern was introduced at the event by Paul Joskow, the Elizabeth and James Killian Professor of Economics, Emeritus, at MIT, and a faculty member at the Institute for over 45 years. Joskow also led off the question-and-answer session after Stern's talk with a query about rural land use and its impact on climate. Stern responded that, although he had emphasized urban policy in his talk, rural policies such as reforestation should play a significant role in capturing excess carbon dioxide.

Stern fielded a wide variety of queries, including one about the economics profession from an audience member who asked: "As an economist working on an issue that affects the world in a relatively short time frame, is it enough, is it persuasive enough, to be doing research … and doing presentations like this?"

"No," Stern responded instantly. "That's why I spend a lot of time doing other things." In recent years, Stern has worked with high-level government officials on climate policy matters in China, India, France, and for the U.N., among other projects.

As advice for economics students concerned about climate, Stern suggested: "Invest in your own skill."

And he left no doubt about his own view on the importance of the climate challenge.

"We have the biggest problem facing humankind," Stern said.

***Peter Dizikes** is the social sciences, business, and humanities writer at the MIT News Office.*

# Climate change: Our greatest national security threat?

**By Mark Nevitt**

Source: http://www.homelandsecuritynewswire.com/dr20190418-climate-change-our-greatest-national-security-threat

Apr 18 – The climate century is here: the earth is warming, humans are to blame, and we must take immediate action *now* to prepare for climate change's massively disruptive consequences. Both the congressionally-mandated 2018 National Climate Assessment (NCA) and United Nations Intergovernmental Panel on Climate Change reports make clear that the window to take collective action to reduce worldwide greenhouse gas emissions is shrinking. And advances in the field of climate attribution science demonstrate that climate change plays a major role in the frequency and intensity of extreme weather events.

Mark Nevitt writesin *Just Security* that No longer can climate change be categorized solely as an environmental issue—it is a grave threatto national security. "Indeed, it may be *the* threat. While there are many national security challenges facing the nation and the world, climate change is an aptly described "super wicked" problem that exacerbates and accelerates already existing threats. It is also manifestly unjust. In a cruel irony, the poorest nations of the world that contributed the least to global warming will bear the brunt of climate change's impacts. What we, as a society, choose to do (or not do) now will define the health and welfare of future generations. Their fate is increasingly shaped by climate change's dramatic, erratic, and catastrophic national security effects."

In his article, Nevitt explains the current predicament and offers three reasons to hope that we may yet be able to address climate security.

He writers:

> We must think bigger and bolder about the national security threats posed by climate change. Beyond what we can read in the best peer-reviewed climate scientific reports, we can see firsthand climate change's massively destabilizing effects. Consider the damage to national security infrastructure at military bases this last hurricane season, costing taxpayers billions and harming military readiness.
>
> Consider, too, climate change's outsized impact in the Arctic region, opening up new maritime trade routes, oil and gas extraction, and the looming potential for a heavily militarized Arctic region. And what happens in the Arctic does not stay in

the Arctic: permafrost and methane emissions significantly harm the environment while causing significant sea level rise throughout the world. Ice-free Arctic summers are coming soon.

How fast is the ice melting in the Arctic? If we are honest, we don't truly know. Past estimates of warming and ice loss in the Arctic have been widely underestimated. Indeed, the United Nations Environmental Program (UNEP) reported that the Arctic has 3-5 degrees Celsius of warming locked in, *irrespective* of future greenhouse gas mitigation effort. Make no mistake: we need to be prepared for a physically transformed Artic region in our lifetime, however fast the ice melts.

**White House climate inaction fueled by denialism**

Yet the current Administration has stepped backwards in the face of its own government's best peer-reviewed science, the collective wisdom of the international scientific community, and the already-evident physical destruction wrought by climate change. Unfortunately, the United States is increasingly an international climate-outlier: it has already announced its intent to withdraw from the near universally-ratified Paris Climate Agreement (that the last administration played a leading role in negotiating) and has failed to advance a meaningful domestic climate agenda. Indeed, it has effectively stepped away from the world's climate leadership stage and has removed all mention of climate change from both the National Security Strategy and National Defense Strategy.

It wasn't always this way. In 1991, then-President Bush assessed that climate change "respects no international boundaries" and contributes to political conflict in his 1991 National Security Strategy. Climate change has been consistently mentioned in national security policy guidance since then. Recently, the White House took the remarkable step of proposing the creation of a closed-door task force to determine the validity of the National Climate Assessment's national security discussion.

Nevitt notes that outside the executive branch — if you look closely enough — the climate landscape is shifting.

If our political will can align with our scientific understanding, then a solution to the "super-wicked" climate security problem may just be possible. Consider the following three areas that provide hope in our fight against climate change.

***The intelligence community and military strike back***

The intelligence and national security communities have begun to speak up louder and actively engage with the world's most authoritative climate science reports in their own threat assessments. Earlier this year, the Office of the Director of National Intelligence (ODNI) issued a new, clear-eyed threat assessment report that highlighted climate change's destabilizing effects. It stated that the "negative effects of environmental degradation and climate change will impact human security challenges, threaten public health, and lead to historic levels of human displacement." Specifically, the ODNI report noted:

> global environmental and ecological degradation, as well as climate change, are likely to fuel competition for resources, economic distress, and social discontent through 2019 and beyond. Climate hazards such as extreme weather, higher temperatures, droughts, floods, wildfires, storms, sea level rise, soil degradation, and acidifying oceans are intensifying, threatening infrastructure, health, and water and food security.

The intelligence community—composed of sober-minded, non-partisan professionals—brings enormous credibility and perspective when weighing the complex security threats facing the nation.

Further, congressional hearings on climate security continue to occur at a steady pace. Just last week, General David L. Goldfein, Air Force chief of staff, cited the conflict in Syria as an example of how climate change's impact is already destabilizing some nations. His remarks came two days after the commanders of U.S. European Command and U.S. Transportation Command voiced similar views before Congress. The military has the

responsibility to prepare for future threats, however defined—this includes climate change.

***Congress awakens***

Congress, too, has slowly awoken from its climate slumber, including provisions in the yearly National Defense Authorization Act (NDAA) that address climate adaptation efforts within DoD. It recently required that DoD report on military installations especially vulnerable to climate change. While the details of the DoD report fell short of expectations, it signaled congressional willingness to actively engage on this issue. Congress also addressed climate adaptation efforts, recently placing restrictions on military construction in the riskiest floodplain areas.

Earlier this week, John Kerry and Chuck Hagel (former Senators and Secretaries of State and Defense, respectively) testified in front of the House Oversight Committee on the national security implications of climate change. We should look for more action in the climate security space as Congress holds hearings on climate change's national security impacts and looks to include provisions in the annual DoD budget bill.

Finally, the Green New Deal – though it may not be on a fast track to becoming law – does not shy away from climate change's security implications, explicitly stating that climate change:

> constitutes a direct threat to the national security of the United States …by impacting the economic, environmental, and social stability of countries and communities around the world and by acting as a threat multiplier.

While Congress has yet to pass comprehensive legislation that would require the United States to meet the emission reduction goals the last administration set in joining the Paris Agreement — and the Obama-era Clean Power Plan was halted by the Supreme Court — the groundwork may be in the process of being laid for such action in the national security arena.

***Innovative legal solutions to combat climate change***

As a general matter, most of our domestic law environmental statutes *suspend* environmental protections for reasons of national security. For example, the Clean Air Act—the major environmental statute governing EPA regulation of carbon dioxide and other Greenhouse Gas (GHG) emissions—authorizes the President to suspend regulation of stationary sources (such as coal-fired power plants) if it is in the "paramount interest of the United States" to do so.

But what if climate change is the underlying emergency and we needed greater authorities to decrease GHG emissions?

While there is no "break glass in case of climate emergency" statute, Congress has delegated broad powers to the President possesses in the 1976 National Emergencies Act. In the aftermath of President Trump's emergency declaration to build a border wall, commentators have begun to speculate that future Presidents could use similar legal authorities to declare climate change a national emergency. The term "emergency" is undefined in law. Moreover, there should be little debate that as a scientific matter, climate change does present an extraordinary threat to the security of the United States. There are certain authorities that could potentially be actuated pursuant to a "climate emergency" declaration, from reducing oil drilling to restricting car emissions to investing in climate adaptation measures. While I do not argue for this approach at this time, we must begin to think innovatively about all the legal authorities available.

Internationally, the United Nations Security Council (UNSC) has shown a renewed willingness to discuss climate change's multifaceted impacts on peace and security. Under Article 39 of the UN Charter, the UNSC has special authorities to "determine the existence of any threat to the peace, [or] breach of the peace." While the UNSC has not (yet) formally declared

climate change a threat to international peace and security — thereby actuating legal authorities under Chapter VI and VII — scholars have begun to assess the implications of doing so.

David Wallace-Wells, in his recent book the Uninhabitable Earth, foreshadows a world where tens of millions of climate refugees flee drought, food insecurity, and extreme weather. Yet these "climate refugees" lack legal protections, including under the 1951 Refugee Convention. How should international law account for and safeguard future refugees fleeing from the disruptive effects of climate change? And if you are a citizen of a small island developing state that may not be habitable due to climate change, what is a more pressing issue facing you? The Security Council may yet need to step in to resolve some of these vexing questions.

Nevitt concludes:

Let me be clear: we need domestic climate legislation, re-entry into the Paris Climate Agreement, and massive governmental investment in renewable energy technology before we actuate these innovative climate legal solutions. However, there is some good news: we have made enormous strides in clean energy technology in recent years and climate denialism and inaction policy have helped energize the electorate. The technology is there; but the political will among our current leaders is not.

And in a twist of fate, the United States cannot formally withdraw from the Paris Climate Agreement until November 4, 2020—one day after the next Presidential election. Whether climate change is on the ballot as a core issue in 2020 still remains to be seen. But the electoral landscape, too, may be changing. Governor Inslee of Washington is seeking the Democratic nomination based upon a climate change platform and Mayor Pete Buttigeig spoke at length about the climate security challenge in his announcement for his Presidential bid on Sunday, explicitly stating "let's pick our heads up to face what might be the great security issue of our time, climate change and disruption."

As I have argued before, climate change cannot be wished away and we are already paying a "do nothing" climate tax on our economy and environment. Indeed, if "we are the first generation to feel the effect of climate change and the last generation that can do something about it" we must meet the climate century head on. It's time to *get moving* on climate action. If not now, when?

*Read the article: Mark Nevitt, "Climate change: Our greatest national security threat?" Just Security (17 April 2019).*

## Climate's Troubling Unknown Unknowns

**By William B. Gail**

Source: https://www.nytimes.com/2019/04/21/opinion/climate-change-greenhouse-gas-emissions.html

Apr 21 – Donald Rumsfeld famously popularized the term "unknown unknowns" in a 2002 news briefing when describing the challenges of linking Iraq to weapons of mass destruction. Troublingly, climate change may also be strewn with such unknowns, and they pose daunting tests for how we face the future. One is choosing among policy alternatives. Should we minimize tomorrow's risks now by reducing greenhouse gas emissions, or save money today and spend it on adapting to the effects of planetary warming once threats emerge more fully, like rising seas or prolonged droughts? The policy debate increasingly tilts toward adaptation.

But we can't adapt to perils from unknown unknowns. In such cases, adaptation will largely fail; only mitigation will be effective.

The National Climate Assessment released last fall provided an updated scientific summary of the "knowns." The simple version was this: Earth is warming, humans are largely responsible, ecosystems are changing in response, and the impact on societies will be large. The report also characterized the known unknowns, as Mr. Rumsfeld might put it — those things we know at a fundamental level but about which we seek greater certainty. They

include how much Earth will eventually warm, how rapidly oceans will rise, where and when weather extremes and water shortages might occur, and whether potential tipping points (like the collapse of Antarctic ice sheets) will, in fact, occur.

Unsurprisingly, the report carefully limited speculation about unknown unknowns: the many initially small environmental shifts that are potential consequences of the changing climate. What will actually emerge is largely unknowable because of the highly unpredictable nonlinear response to the warming of Earth's complex and adaptive physical and ecological systems.

Yet credible speculation on climate's unknown unknowns is sorely needed by policymakers. Future generations will be affected by today's policy decisions, whether the underlying science is complete or not. The basics are simple: The more we warm our planet, the more likely it is that deeply surprising environmental changes will ensue.

Most of these smaller environmental changes should be manageable, readily addressed through adaptation. Inevitably, however, a rare few will most likely evolve and expand until they threaten our security, health or economy. We lack the ability to predict which are which. This is the curse of unknown unknowns. Nevertheless, things we can credibly imagine should accentuate our concern for what we are unable to imagine.

Perhaps a routinely ice-free Arctic summer, altering polar ocean life in subtle ways, sets off an unpredictable cascade of complex changes throughout the global ocean ecosystem, devastating fisheries. Maybe agricultural pests adapt to climate change stresses by evolving novel and frequently changing abilities to destroy crops, leaving farmers struggling to keep pace and feed populations. One unsettling risk is that mutant diseases — like Zika and Ebola today and the 1918 flu epidemic that killed 50 million people — could emerge more often because of altered evolutionary competition in a changing climate, each a greater medical challenge than the last.

Environmental changes occur regularly; climate change significantly accelerates the process. Should warming progress too far, society risks being overwhelmed by the growing rate at which disruptive events could occur. Each new threat is likely to emerge and proliferate differently, undermining adaptation's effectiveness.

Some threats might be so startling and strange that our imaginations would struggle to comprehend them even after they arise. Timely response efforts would be frustrated by poor knowledge about what is occurring and how to contain the threat.

Though climate change has yet to produce clearly attributed examples, Zika hints at this dispiriting future. Within a few short years, it transformed from an ignorable rare disease into a medical terror. Nobody saw it coming. Its long-term societal consequences run deep, with

childbearing upended for people threatened by the mosquito that carries the virus. Though probably not a direct result of climate change, Zika starkly illustrates the type of inconceivable surprises, and their demoralizing consequences, that threaten to emerge with ever greater frequency should we fail to slow global warming.

Three millenniums ago, Homer foreshadowed our dilemma. He wrote of Odysseus returning by ship across the Aegean Sea, headed homeward to Greece after his great victory over Troy. Odysseus anticipated an arduous sea journey, but was unprepared for what followed: an interminable voyage punctuated by unimaginably difficult experiences one after another, from Sirens to the Cyclops.

Our decisions in the next few years will determine whether our climate journey follows a similar course. Perhaps current policy discussions will navigate society through the journey's recognized risks. If warming progresses rapidly, however, the known concerns — increasing temperatures, sea level rise, a melting Arctic — will not be the whole story. Nature's unforeseeable surprises, some unimaginable to us today, could become pivotal to our fate.

Without an aggressive policy commitment to mitigation by rapidly reducing our carbon emissions, our grandchildren could be destined to live in a world with nature's unknown unknowns around each year's turn.

***William B. Gail*** *is a co-founder of the Global Weather Corporation, a past president of the American Meteorological Society and the author of "Climate Conundrums: What the Climate Debate Reveals About Us."*