9\20

HZS

CBRNE DIARY

Dedicated to Global First Responders

September 2020

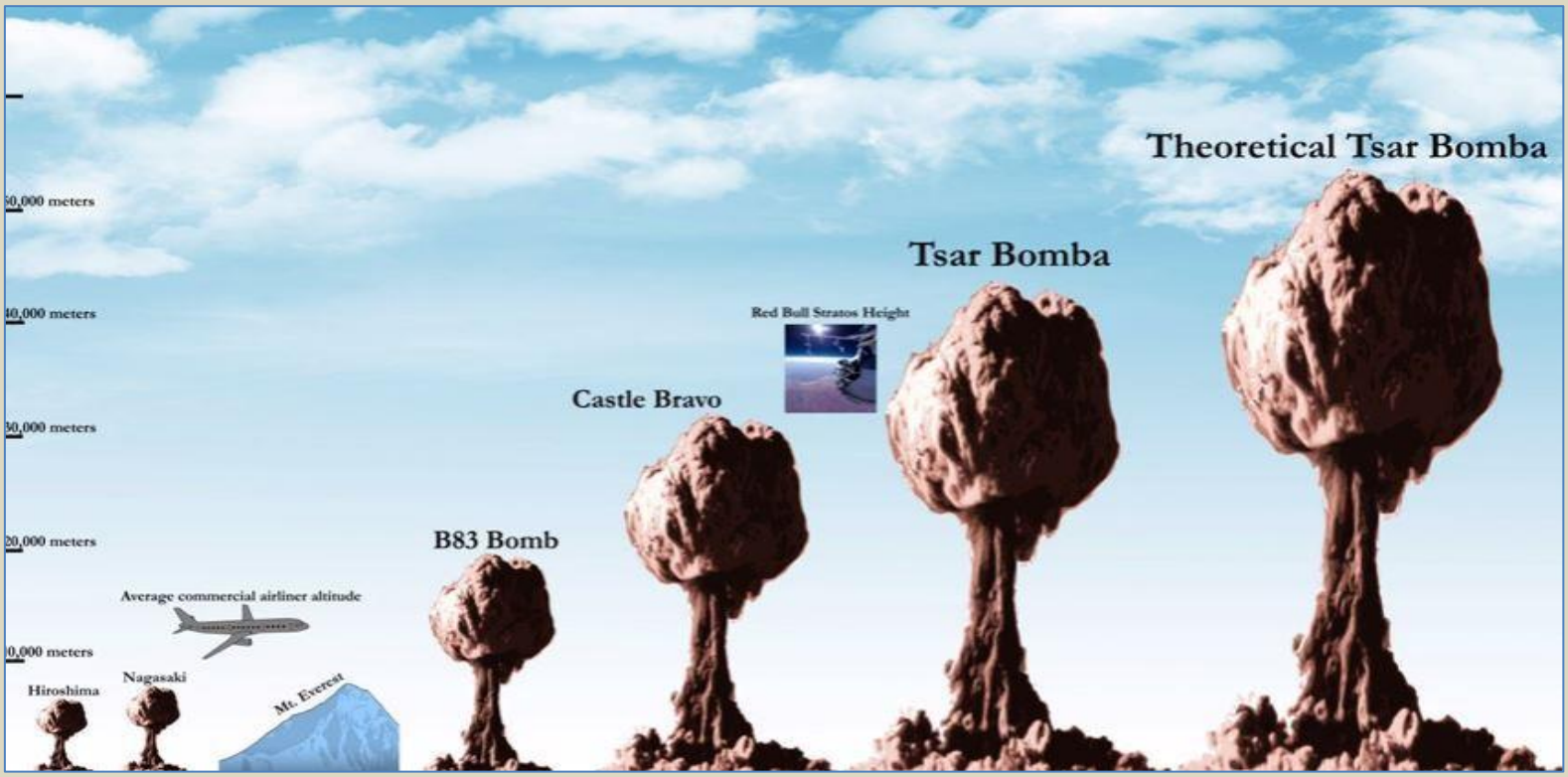
تذكر بيروت!

A HOTZONE SOLUTIONS GROUP PUBLICATION


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

Rosatom releases previously classified documentary video of Tsar Bomba nuke test

Source: https://thebarentsobserver.com/en/security/2020/08/rosatom-releases-previously-classified-documentary-video-50-mt-novaya-zemlya-test



Aug 22 – Photos and short video clips have previously been available, but this unseen 40-minutes declassified footage of the Soviet Union's monster nuclear bomb give a whole new insight into what happened on Novaya Zemlya on October 30, 1961. **The documentary film was released and posted on August 20 on the YouTube channel of Rosatom State Atomic Energy Corporation in connection with the celebration of 75 years of nuclear industry.**

The film, edited in classic Soviet-style propaganda, shows all preparation procedures. First the transportation of the giant bomb by rail to the Olenya airbase near Olenegorsk on the Kola Peninsula. The Tu-95 aircraft take-off and flight across the Barents Sea to the detonation site near the Matochkin Strait at Novaya Zemlya. Then the release of the bomb attached to a parachute to slow the fall so the plane could get in safer distance from the blast. Videos from several directions and distances show the apocalypse looking detonation and following mushroom cloud.

The bomb, officially named RDS-220 and later nick-named Tsar Bomba, was the largest nuclear weapon ever constructed. With a yield of 50 megatons (50 million tons), equal to around 3,800 Hiroshima bombs, the weapon was set off over Novaya Zemlya on October 30, 1961.

It was Soviet Premier Nikita Khrushchev who in July 1961 ordered the development of the doomsday-size bomb at a time amid rising political tensions between the Soviet Union and the United States. Khrushchev wanted a 100-megaton weapon and to achieve such size, the engineers added a third stage on the thermonuclear warhead. Normal hydrogen bombs comprise two stages. Understanding the extreme radiation releases, the engineers, and among them Andrei Sakharov, decided to reduce the actual yield of 100 megatons to around half.

The film shows how the modified Tu-95 bomber plane was coated with a special white reflective paint to protect it from the heat caused by thermal radiation from the explosion. Measurement equipment was attached all over and a second plane flew besides, filming and monitoring radiation samples.

To slow the drift down after release, the bomb was deployed to a giant parachute, itself weighing nearly a ton.

The bomb was detonated 4,000 meters above the ground. As seen in the film, the fireball flash lasted far longer than seen on any other nuclear weapon test videos. The flash dome itself reached 20 km, while the ring of absolute destruction had a radius of 35 kilometers

After 40 seconds, the dome of the fire reached 30 km and thereafter developed into a mushroom cloud which soared to a height of 60-65 kilometers with a diameter of 90 km. In the military town Severny, center for the nuclear weapons test around the Matochkin Strait, most buildings were destroyed. The town was 55 kilometers from ground zero.

At 11:32 am on October 30, 1961, the Tsar Bomba exited Andrei Durnovtsev's plane at a height of 6.5 miles and slowly parachuted towards Mityushikha Bay test range in Novaya Zemlya (giving the drop plane just 188 seconds to escape). At 2.5 miles high, Big Ivan went boom! A few seconds after the explosion, the diameter of the dust column was about 10 km. Screenshot from the film

Although being detonated four kilometers above the ground, the seismic shock wave equivalent to an earthquake of over 5.0 on the Richter scale was measured around the world.

The Tu-95 plane carrying the bomb was far away at the time of detonation. However, the explosion's shock wave caused the aircraft to instantly lose 1,000 meters of altitude, but it later landed safely.

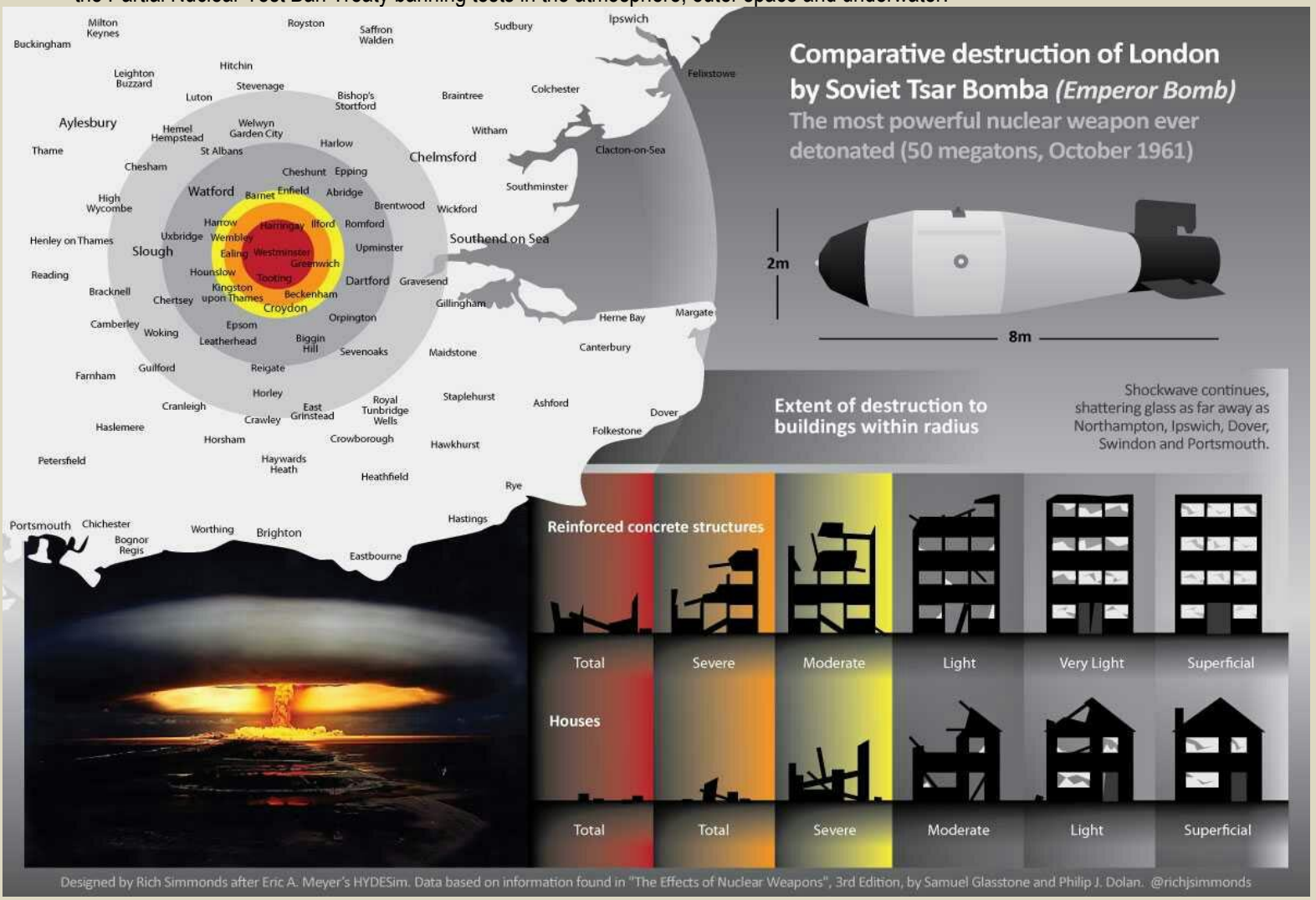
In Norway, military border guards on the Jarfjord Mountain near Kirkenes could see the flash. In the film, it is said the light from the flash could be seen at a distance of 1,000 kilometers.

Radiation fallout was measured all over Scandinavia, and international condemnation followed.

Domestic protests were also voiced inside the USSR, among them from Andrei Sakharov who began speaking out against nuclear weapons. In his book, Memoirs, Sakharov wrote in detail against the Soviet leadership's policies. In 1975, Sakharov was awarded the Nobel Peace Prize, but Moscow denied him permission to go to Oslo for the ceremony.

After the Tsar Bomba and other thermonuclear tests on Novaya Zemlya and by the United States in the Pacific, the two superpowers realized the craziness of conducting atmospheric tests with huge radioactive fallouts. In 1963, the United States and the Soviet Union signed

the Partial Nuclear Test Ban Treaty banning tests in the atmosphere, outer space and underwater.



Consequently, nuclear weapons tests were conducted underground. The last two such tests took place at Novaya Zemlya on October 24, 1990.
In 1996, the UN adopted the Comprehensive Nuclear Test Ban Treaty, prohibiting any nuclear weapon test explosion or any other nuclear explosions.

▶▶ **The video:** https://www.youtube.com/watch?v=nbC7BxXtOlo&feature=emb_logo

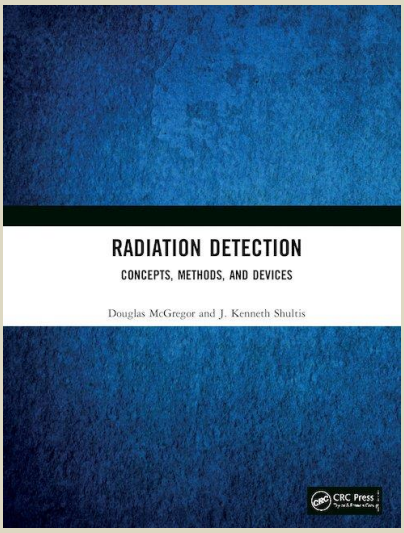
Radiation Detection

Concepts, Methods, and Devices

By Douglas McGregor and J. Kenneth Shultis (*authors*)
September 7, 2020 by CRC Press
Source: https://www.routledge.com/Radiation-Detection-Concepts-Methods-and-Devices/McGregor-Shultis/p/book/9781439819395

Radiation Detection: Concepts, Methods, and Devices provides a modern overview of radiation detection devices and radiation measurement methods. The book topics have been selected on the basis of the authors' many years of experience designing radiation detectors and teaching radiation detection and measurement in a classroom environment.
This book is designed to give the reader more than a glimpse at radiation detection devices and a few packaged equations. Rather it seeks to provide an understanding that allows the reader to choose the appropriate detection technology for a particular application, to design

detectors, and to competently perform radiation measurements. The authors describe assumptions used to derive frequently encountered equations used in radiation detection and measurement, thereby providing insight when and when not to apply the many approaches used in different aspects of radiation detection. Detailed in many of the chapters are specific aspects of radiation detectors, including comprehensive reviews of the historical development and current state of each topic. Such a review necessarily entails citations to many of the important discoveries, providing a resource to find quickly additional and more detailed information.



This book generally has five main themes:

- Physics and Electrostatics needed to Design Radiation Detectors
- Properties and Design of Common Radiation Detectors
- Description and Modeling of the Different Types of Radiation Detectors
- Radiation Measurements and Subsequent Analysis
- Introductory Electronics Used for Radiation Detectors

Topics covered include atomic and nuclear physics, radiation interactions, sources of radiation, and background radiation. Detector operation is addressed with chapters on radiation counting statistics, radiation source and detector effects, electrostatics for signal generation, solid-state and semiconductor physics, background radiations, and radiation counting and spectroscopy. Detectors for gamma-rays, charged-particles, and neutrons are detailed in chapters on gas-filled, scintillator, semiconductor, thermoluminescence and optically stimulated luminescence, photographic film, and a variety of other detection devices.

Table of Contents

Douglas S. McGregor *is a University Distinguished Professor in Kansas State University (KSU) and holds the Boyd D. Brainard Chair in Mechanical and Nuclear Engineering. Professor McGregor serves as director of the Semiconductor Materials and Radiological Technologies Laboratory at KSU, a 9500 sq ft laboratory dedicated to radiation detector research. He has published over 200 research articles and reports, is co-inventor on over 20 radiation detector patents, and his research group has received five R&D-100 Awards for radiation detector innovations. Prof. McGregor is also the recipient of various other honors, including the KSU College of Engineering (CoE) Frankenhoff Outstanding Research Award (2006) and the CoE Engineering Distinguished Researcher Award (2016).*

J. Kenneth Shultis *joined the Nuclear Engineering faculty at Kansas State University in 1969 and where he presently holds the Black and Veatch Distinguished Professorship and is the Ike and Letty Conerstone teaching scholar.Besides being coauthor of this book he has coauthored the books Fundamentals of Nuclear Science and Engineering, Radiation Shielding, Radiological Assessment, Principles of Radiation Shielding, and Exploring Monte Carlo Methods.He is a Fellow of the American Nuclear Society (ANS), and has received many awards for his teaching and research, including the infrequently awarded ANS Rockwell Lifetime Achievement Award for his contributions over 50 years to the practice of radiation shielding.*

U.K. Nuclear Power: The Next Huawei?

By Jo Harper

Source: http://www.homelandsecuritynewswire.com/dr20200825-u-k-nuclear-power-the-next-huawei

Aug 25 – London's relations with China — hailed as entering a "golden era" only four years ago — have deteriorated badly over Hong Kong, hitting a nadir when the U.K. finally bowed to U.S. pressure to ditch Huawei's involvement in its new-generation internet (5G) rollout.

In late 2019, the US published a list of companies linked to the Chinese military, and after Huawei came the China General Nuclear Power Group (CGN). The state-owned Chinese firm has invested 3.8 billion pounds (€4.1 billion, $4.3 billion) in Britain to date, mainly in the Hinkley Point nuclear plant under construction in Somerset, southwest England, and the Sizewell plant in eastern England. It is also seeking UK regulatory approval to build its own nuclear reactor at Bradwell in Essex, east of London.

China warned the U.K. it would face "consequences if it chooses to be a hostile partner" after London announced its Huawei's decision. Liu Xiaoming, the Chinese ambassador to the U.K., reportedly said China could cut its backing for U.K. nuclear plants altogether.

Years of Chinese Involvement in U.K. Nuclear Industry

CGN's involvement in the U.K. nuclear industry began in 2016 when a deal was signed with French state-owned utility Electricite de France (EdF) to collaborate on three reactors totaling 8.7 gigawatts (GW) of power generation, starting with Hinkley Point. The agreement spoke of CGN's "progressive entry" into the UK's "resurgent" nuclear ambitions.

The UK currently has 15 operational nuclear reactors at seven locations. At its height in 1997, 26 percent of the country's power was generated from nuclear, but this has slipped since to 19 percent.

In the Sizewell and Hinkley projects, CGN is providing cash, holding 66 percent stakes, but with Bradwell it wants to build the reactor itself, using its own technology, and it wants to operate it. Observers say Bradwell is the prize CGN is really seeking: the first Chinese-built nuclear plant outside China.

In May, EdF outlined its plans to start work on Sizewell by the end of next year. The project would create 25,000 jobs, it said.

But EdF's continued involvement could be thrown into doubt if no other investor came forward to replace CGN. This is especially troubling given the project is also expected to result in cost overrun. Hinkley Point now costs about 3 billion pounds more than the 20 billion pounds originally planned. Sizewell is also slated to cost 20 billion pounds.

"Several projects were planned but only Hinkley Point will likely go ahead," Jonathan Marshall, Energy and Climate Intelligence Unit (ECIU), told DW. "Bradwell would be a Chinese project, but is now unlikely for political reasons."

Bradwell looks surplus to requirements for the reasons the National Infrastructure Assessment (NIC), a government advisory body, outlined in its most recent long-term assessment: "Given the balance of cost and risk, a renewables-based system looks a safer bet at present than constructing multiple new nuclear power plants," it read.

Financing of Nuclear Plans Unclear

"Sizewell is not dependent on CGN investment," a spokesman from the the Department for Business, Energy and Industrial Strategy (BEIS) said.

But not many agree. "Equity funding for nuclear power stations is very difficult for private actors," Rob Gross, director of the UK Energy Research Centre, told DW. The government's offer in 2018 to Hitachi to take a third of the equity at the Wylfa nuclear project wasn't enough to keep the company interested, for example.

As Paul Dorfman of University College London's energy institute and founder of the Nuclear Consulting Group told environmental news platform electrictyinfo.org, it was hard to see who else might invest in Sizewell if the Chinese pull out. "The market won't touch nuclear with a barge pole. You only see nuclear being built in command-and-control economies, like China and Russia, and a few outliers," he said.

One option would be for the government to take either a majority or minority stake in Sizewell. Another option is a Regulated Asset Base (RAB) model, where consumers are charged a fixed price to cover infrastructure costs. But this would hike energy prices in the long term and make it politically hard to justify. Others suggest developing smaller, modular reactors.

U.K. Energy Strategy Shifting?

The fate of nuclear power in Britain —to date seen as a low-carbon way of supplementing renewables — will be decided later this year when the government publishes its plans. The 2011 National Policy Statement (NPS) identified eight sites suitable for new nuclear reactors by the end of 2025, but a new NPS later this year could change that.

"With all but one of the nuclear fleet set to retire by 2030, and uncertainty over the scale of the new build program, it is likely that more electricity from renewable sources will be needed," Jonathan Marshall, head of analysis at the Energy and Climate Intelligence Unit, told DW.

"It is impossible to say what the UK government will decide on nuclear power later this year since the decision will be political," Gross said. But there is one thing to bear in mind, he adds, namely that the companies building nuclear power stations are completely separate from the company that controls the national grid and that power generation is privately owned.

"It's hard to imagine a threat to security of supply from Chinese investors," he says.

***Jo Harper** is a freelance journalist based in Warsaw.*

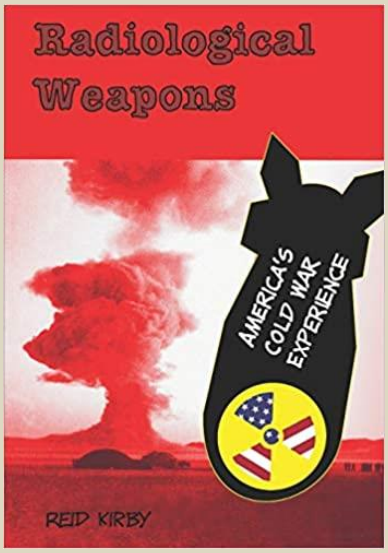
Radiological Weapons: America's Cold War Experience

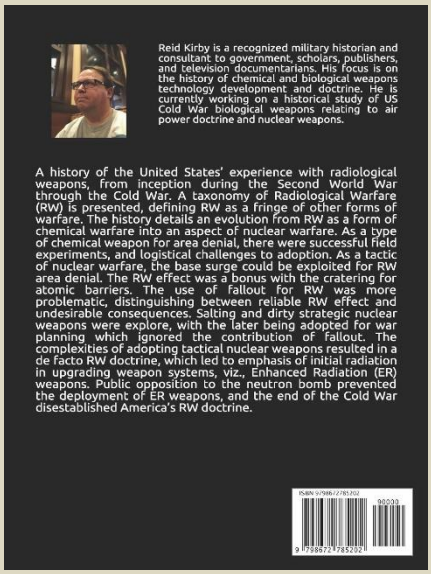
By Reid Kirby (Author)

Paperback – August 6, 2020

Source: https://www.amazon.com/Radiological-Weapons-Americas-Cold-Experience/dp/B08F8C93GT

A history of the United States' experience with radiological weapons, from inception during the Second World War through the Cold War. A taxonomy of Radiological Warfare (RW) is presented, defining RW as a fringe of other forms of warfare. The history details an evolution from RW as a form of chemical warfare into an aspect of nuclear warfare. As a type of chemical weapon for area denial, there were successful field experiments, and logistical challenges to adoption. As a tactic of nuclear warfare, the base surge could be exploited for RW area denial. The RW effect was a bonus with the cratering for atomic barriers. The use of fallout for RW was more problematic, distinguishing between reliable RW effect and undesirable consequences. Salting and dirty strategic nuclear weapons were explored, with the later being adopted for war planning which ignored the contribution of fallout. The complexities of adopting tactical nuclear weapons resulted in a de facto RW doctrine, which led to emphasis of initial radiation in upgrading weapon systems, viz., Enhanced Radiation (ER) weapons. Public opposition to the neutron bomb prevented the deployment of ER weapons, and the end of the Cold War disestablished the America's RW doctrine.



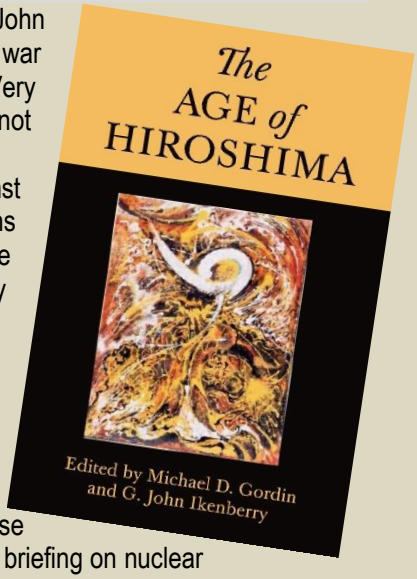


The New Nuclear Threat

By Jessica T. Mathews

Source: https://www.nybooks.com/articles/2020/08/20/new-nuclear-threat/

July 22 – Seventy-five years ago, at 8:16 on the clear morning of August 6, the world changed forever. A blast equivalent to more than 12,000 tons of TNT, unimaginably larger than that of any previous weapon, blew apart the Japanese city of Hiroshima, igniting a massive firestorm. Within minutes, between 70,000 and 80,000 died and as many were injured. Hospitals were destroyed or badly damaged, and more than 90 percent of the city's doctors and nurses were killed or wounded. By the end of the year, thousands more had died from burns and radiation poisoning—a total of 40 percent of the city's population.



The mushroom cloud became a universal symbol of horror. As Michael D. Gordin and G. John Ikenberry, the editors of ***The Age of Hiroshima***, describe, entirely new ways of thinking about war and peace had to be invented, together with a new understanding of global interconnectedness. "Very few aspects of life," geopolitical, technological, or cultural, they write, "have been left untouched," not just among the superpowers but worldwide.

In part because of effective deterrence, fear of their destructiveness, and a growing taboo against their use, and in part because of dumb luck, nearly a century has passed without nuclear weapons being used again in conflict. The US and the Soviet Union survived the cold war, living on a knife edge of fear that drove each to accumulate more than 30,000 nuclear weapons, enough to destroy all life on the planet many times over. In retrospect, as documents are declassified and participants speak and write about their experiences, and as brilliantly chronicled by Fred Kaplan in *The Bomb*, the competition emerges, on the US side at least, as a largely mindless cycle of more and larger weapons aimed at ever more targets, and more and more targets deemed to require ever more weapons, the whole enterprise impervious to the efforts of administration after administration to define saner policies.

Kaplan tells the story of how, two weeks into the Kennedy administration, Secretary of Defense Robert McNamara traveled to Strategic Air Command (SAC) headquarters in Omaha for his first briefing on nuclear war's holy text, the Single Integrated Operational Plan (SIOP). One of its thousands of targets, he learned, was an air defense radar station in Albania. The bomb slated to destroy it was—by then only a few years into the arms race—roughly three hundred times larger than the bomb that destroyed Hiroshima. "Mr. Secretary," said the commanding general, "I hope you don't have any friends or relations in Albania, because we're going to have to wipe it out." Albania, a tiny country, was Communist but politically independent of Moscow.

Decades later, the same thinking—if that's what it should be called—still prevailed. A Carter administration effort to reduce the consequences of nuclear war added "leadership" targets to the list of those to be hit in the belief that it would effectively deter Soviet leaders. The SIOP was accordingly revised to include not only government ministries but the homes and vacation dachas of every government minister, not just in Moscow but in every oblast across Russia. The use of megaton bombs to kill individuals meant, of course, that many hundreds of thousands of other people would also be killed.

The cold war ended peacefully, and the deployed nuclear arsenals of the US and Russia have been reduced by nearly 90 percent, but we are not safer today—quite the reverse. After decades of building just enough weapons to deter attack, China is now aggressively modernizing and enlarging its small nuclear arsenal. Russia and the US are modernizing theirs as well with entire menus of new weapons. Activities in space are enlarging the global battlefield. Advances in missile technology and conventional weapons "entangle" scenarios of nuclear and nonnuclear war, making outcomes highly unpredictable. The risk of cyberattacks on command and control systems adds another layer of uncertainty, as does research on artificial intelligence that increases the prospect of accidents and the unintentional use of nuclear weapons. Arms control agreements that significantly limited the US–Soviet arms race are being discarded one by one. And from Russian efforts to destabilize America through social media attacks on its democracy, to Chinese bellicosity in the South China Sea and clampdown on Hong Kong, to erratic lunges in US foreign policy, there is deep and growing distrust among the great powers.

Yet the public isn't scared. Indeed, people are unaware that a second nuclear arms race has begun—one that could be more dangerous than the first. Decades of fearing a nuclear war that didn't happen may have induced an unwarranted complacency that this threat belongs to the past. A million people gathered in New York's Central Park in 1982 to call for an end to the arms race in the largest political demonstration in US history. Today the prospect of nuclear disaster is barely noticed.

In the US, the nuclear age has been a fruitless, decades-long search for answers to three linked questions. The most basic is: What is our goal in a nuclear war? The military has a definite answer: "to prevail." Civilian leaders' answers have varied widely. President Eisenhower favored nuclear weapons because they were less expensive than conventional forces, yet he nevertheless told the Joint Chiefs that our aim in a general nuclear war should be not "to lose any worse than we have to." Defense Secretary Harold Brown, reaching for a formula to satisfy President Carter, described the goal as ending a war "on acceptable terms that are as favorable as practical," leaving "acceptable" and "practical" undefined. Ronald Reagan wrote in his memoir that he thought that those who claimed nuclear war was "winnable" were "crazy," apparently forgetting that he had signed a nuclear policy document that stated the US "must prevail."

What winning might look like is what makes this seemingly simple question so hard to answer. In the early 1960s, SAC was asked how many Russians, Chinese, and Eastern Europeans would die from its all-out attack plan. The answer was a nearly inconceivable 275 million, just from the bombs' blasts. (Heat, fire, smoke, and radiation would kill tens of millions more, but the numbers would vary depending on wind and weather, so SAC did not count

them.) Presidents and their advisers found it difficult if not impossible to imagine the conditions under which they would launch such a holocaust. Only in the basement at SAC headquarters—where targeters sat, day after day, assigning weapons to targets in a policy-free environment—did it make sense. "Look," yelled the SAC commander General Thomas Power at a nagging policy analyst from Washington who was arguing for a war plan with fewer casualties, "at the end of the war, if there are two Americans and one Russian, we win!"

The second question concerns deterrence: What weapons and force structure are needed to deter an enemy or enemies from attacking us? Unfortunately, there are no metrics to measure what makes a deterrent credible. Answers are entirely in the eye of the beholder, and arguments can almost always be contrived to justify the need for more weapons. What can be said with certainty, however, is that the threshold the US judges necessary to deter the enemy is always set immensely higher than what has actually deterred the US. In *The Button*, former defense secretary William J. Perry writes that at the time of the Cuban missile crisis the US had about five thousand warheads to the Soviets' three hundred, but "even with this seventeen-to-one numerical superiority, the Kennedy administration did not believe it had the capability to launch a successful first strike." Notwithstanding the enormous gap between the two arsenals (which has never again been anywhere near as large), Washington was deterred by the risk of a Soviet counterstrike.

The third question, closely tied to what it takes to create deterrence, asks what happens if deterrence fails. Can nuclear weapons then be useful instruments for fighting, as opposed to preventing, a war? Understandably, presidents demand all kinds of flexibility—weapons and war plans suited to a general war and to regional aggressions in different settings of greater or lesser geopolitical importance. The problem is that weapons and plans tailored to every situation, especially smaller weapons and plans for limited nuclear war, may be understood by the enemy (and by domestic opponents) as preparations for going to war. "The logic," writes Kaplan,

involved convincing adversaries that you really would use the bomb in response to aggression; part of that involved convincing yourself that you would use it, which required building certain types of missiles, and devising certain plans, that would enable you to use them—and, before you knew it, a strategy to deter nuclear war became synonymous with a strategy to fight nuclear war.

Many plans for limited nuclear war have been created on paper, but they immediately raise yet another critical question: Can there really be such a thing? To assert that the answer is yes, one has to believe that intentions can be clearly signaled ("I'm attacking you but with much less firepower than I might have used"), accurately interpreted by the other side, and responded to not in rage or fear but with calm reasonableness ("I'm retaliating but much more lightly than I might have"). There are all kinds of technical reasons to doubt that this is more than a fantasy. For example, at one point an American analyst discovered that Russian air defense systems could pinpoint no more than two hundred incoming missiles before they merged into a blob on the radar screen. Yet at that time the SIOP's smallest limited attack option called for launching one thousand missiles, which would therefore be indistinguishable to the Russians from an all-out attack.

The more powerful reasons to doubt that there could be a limited nuclear war, to my mind, are those that emerge from any study of history, a knowledge of how humans act under pressure, or experience in government. In his "speculative novel" *The 2020 Commission Report on the North Korean Nuclear Attacks Against the United States* (2018), the nuclear analyst Jeffrey Lewis convincingly traces the path to an unintended war. The book's lessons are much broader than the particulars of the Korean setting. Lewis uses variations on actual events to trace a series of miscalculations, mistakes, coincidences, domestic pressures, and misreadings of others' intentions, beginning with the mistaken shooting down of a commercial South Korean plane by North Korea and ending in a nuclear war involving both Koreas, Japan, and the US. Each step toward disaster is plausible. After a limited South Korean missile response to the downing of its plane, to which Seoul chooses not to alert its American ally in advance, North Korean leader Kim Jong-un finds that he can't use his

phone. The phone system is simply overloaded, but in the aftermath, one of his aides tells the commissioners investigating how the war had happened that the North Koreans had concluded something quite different: "We assumed it was an American cyber-attack. Wouldn't you?"

The recent real-world version of the recurring debates about limited war and the weapons needed to fight one is the Trump administration's decision to deploy low-yield warheads on American Trident submarines. The move was prompted by Russia's fielding of new low-yield tactical warheads aimed at Europe. Did this mean that Moscow had detected some gap in our deterrent that such a weapon could exploit? Didn't Washington have to respond in kind, asked proponents of the new warheads? Opponents argued that Russia had turned to tactical nukes because it feared American advances in long-range conventional weapons. The disadvantage was on their side, not ours. Moreover, the Russians would be unable to quickly distinguish one of these low-yield warheads fired by a submarine from the many megaton strategic warheads these ships carry, and hence unable to immediately distinguish a limited from an all-out attack. Nevertheless, proponents won the day. The warheads have been deployed, strengthening the hand of those who believe that nuclear wars can be fought and won.

A decade ago, President Obama made a fateful bargain to secure Senate approval of the New START arms limitation treaty he had reached with Russia. He agreed to a major upgrade of the aging American nuclear complex, including production facilities and laboratories, with a controversial price tag nearing $100 billion. This was the seed of a modernization program that has since multiplied to include command and control systems, all the delivery vehicles of the nuclear triad—bombers, ICBMs, and submarines—refurbishment of existing warheads, and the development of a range of new warheads and weapons.

The need for modernization results partly from aging systems that require replacement and partly, in an all-too-familiar pattern, from a perceived need to keep up with the Russians. Moscow began a sweeping modernization program in the early 2000s to keep up with American advances and compensate for weakness in its conventional forces. Rose Gottemoeller, the former deputy director general of NATO and chief US negotiator of the New START Treaty, argues that the real purpose of Russia's program, which includes exotic weapons like an underwater nuclear drone and a nuclear-propelled cruise missile, had more to do with politics than with security. These weapons are meant, she says, to signal Russia's "continuing scientific and military prowess at a time when the country does not otherwise have much on offer."

Unfortunately, the program coincides with an American president who loves nukes. At the disastrous briefing session arranged for Donald Trump in the summer of 2017 in the Joint Chiefs' secure room at the Pentagon known as the "tank," he was shown a chart illustrating US and Russian success in cutting their arsenals from more than 30,000 warheads to about 6,000 each (which in both countries includes 2,500 retired warheads waiting to be destroyed). Like everything else that awful morning, it backfired. Why aren't we building back up to 30,000, Trump demanded in a tantrum, during which he called the assembled military and civilian leaders "dopes and babies." Defense Secretary Mark Esper leaves no doubt that modernizing the entire strategic nuclear force is the president's "priority number one." The modernization plan now includes a new fleet of ballistic missile submarines, a new stealth bomber, new ICBMs, the first new warhead design in more than thirty years, a sea-launched cruise missile, and a new air-launched cruise missile. The estimated price tag over the coming twenty-five years is $1.7 trillion (assuming, against experience, no cost overruns)—seventeen times Obama's down payment—and represents a policy that is as far as it is possible to go from Obama's plan to "reduce the role of nuclear weapons in our national security strategy"—of which Vice President Joe Biden was a strong supporter.

Some modernization is necessary, but there is no question that the current plan goes far beyond what is needed. Contractors are now driving it forward, and there is no one with sufficient standing to say "Stop." But there are ways to save hundreds of billions of dollars without loss to national security. For decades, the triad has been the sine qua non of nuclear force structure. The apparent need for missiles, submarines, and bombers is now so entrenched that it is difficult to remember that it emerged not out of strategic necessity but from fierce rivalry among the military services, the Air Force and Navy especially, each of which wanted its own nuclear weapons.

Of the three legs of the triad, ground-based ICBMs are both the most threatening weapons to the enemy, because of their number and huge megatonnage, and the most vulnerable, because they sit in fixed, easily targeted silos. They are therefore "use them or lose them" weapons that must be fired on warning of an attack, before they are hit by incoming missiles. This means that a president has about ten minutes—less than the time it takes to confirm an attack—to make a life-or-death decision for the country and probably for the planet. Rather than spend $150 billion or more to replace these missiles, the sensible step is to retire them. Ballistic missile submarines, backed up by bombers plus cruise and hypersonic missiles launched from ships and planes, can provide the necessary firepower and strategic depth for an ironclad deterrent and the capability for a devastating second strike.

Years from now, the Trump administration's wholesale withdrawal from international agreements, its "unsigning" of treaties, and its weakening of international organizations will stand out from the lies, the corruption, the incompetence, and the breaking of norms as one of its most damaging features. A partial list includes the Trans-Pacific Partnership (TPP) trade deal, NAFTA, the Paris Climate Accord, the Iran nuclear deal, the Arms Trade Treaty,

and, most recently, the World Health Organization. Among these, withdrawals in the nuclear arena may prove to be especially harmful.

The administration's hostile view of arms control was evident in its 2018 Nuclear Posture Review: The US "will remain receptive to future arms control negotiations if conditions permit." These agreements have their flaws. Negotiations take years and years. Often the sides agree to give up weapons they no longer want. Violations are not uncommon and, to satisfy domestic hawks, both sides frequently build new weapons to compensate for those they negotiate away. Nonetheless, over more than three decades of painstaking effort by Republican and Democratic administrations, a set of agreements was hammered out that built trust between the West and Russia, created a degree of transparency into what the other side was doing, and banned or severely limited particularly destabilizing types of weapons, such as missile defense systems and multiple-warhead missiles. Over time the agreements slowed the arms race from a gallop to a jog. Without them, the two sides might still be holding 65,000 warheads instead of 13,000.

The dismantling of these agreements began with President George W. Bush's withdrawal from the Anti-Ballistic Missile Treaty in 2001, but in the last few years Trump has wiped away almost everything that was still in place. In 2018 he announced that the US would withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty. Russian violations of the agreement, which Moscow had refused to acknowledge over many years, made this a close—and understandable—call. Still, withdrawing from an agreement gives the other side what it wants. And prompt American testing of a missile banned under the treaty suggests that Washington was eager to dispose of it.

The administration then announced its intention of leaving the Open Skies Treaty, a 1992 multilateral agreement that allows signatories to fly unarmed observation flights over the territory of the others to collect data on military forces and activities. Though its value to the superpowers has diminished with satellite technology, it remains important to European parties and has been a significant contributor to strategic stability.

The only remaining limit on strategic arms is New START, which is due to expire two weeks after the next president is inaugurated, unless extended by mutual agreement for a further five years. The treaty limits each side to 1,550 deployed strategic warheads and 700 launchers. The US now insists it will not extend the treaty unless China is included. Since both Russia and the US have about five times as many warheads as China (which may double its arsenal in the next ten years), Beijing has absolutely no reason to become part of US–Russian arms control talks at this point and has made that clear on many occasions. Moreover, although the administration has been talking about this for two years, it has taken no diplomatic steps—plans, proposals, or drafts exchanged—to make it happen. The policy bears all the signs of a poison pill designed to force New START's demise while obscuring the cause.

In addition, news leaked in May—perhaps purposefully—that administration officials were discussing breaking the twenty-eight-year moratorium among the major powers on nuclear testing. The stated reason was to try to use a nuclear test to pressure Russia and China to agree to Washington's New START position. On the very long list of self-defeating moves this administration has made, breaking the moratorium belongs near the top. A nuclear test would not frighten Moscow or Beijing into doing what the US wants, it would drastically weaken global nonproliferation efforts, it would make the US an international pariah, and it would erase an important US advantage. The US has conducted more tests than any other country—more than one thousand to China's forty-five, for example—so if testing is resumed, every other nuclear power stands to gain much more than the US.

Taken together, the loss of New START, a tease—at least—on a resumption of testing, and the vast weapons modernization plan, all enhanced by work on new cyber and space weapons, applications of AI, and a range of new weapons capable of carrying either conventional or nuclear warheads, amount to a running leap into a new arms race, this time among at least three powers, perhaps joined by North Korea, Iran, and other new nuclear states. The Trump administration seems eager for it, no matter the cost. "We know how to win these races," said the US arms control negotiator Marshall Billingslea recently, "and we know how to spend the adversary into oblivion."

Little can be done to reverse direction unless Donald Trump is defeated in November. Even if he loses, stopping a burgeoning arms race will have to compete for public attention with an overwhelming list of priorities: repairs to democratic governance, health care reform, racial justice, climate change, economic recovery—and enormous post-pandemic budget deficits. Only the last of these can help focus attention where it's needed. Without public pressure the military-industrial-congressional complex will push nuclear modernization forward step by multibillion-dollar-step without attention to the $2 trillion bottom line, locking in a new generation of threats that Russia and China will feel they must counter. The deficits, however, demand a more provident approach to the ballooning defense budget (now larger than everything else in the federal discretionary budget combined). A spasm of spending on what are essentially twentieth-century weapons, without a pause to rethink, is strategically irresponsible and fiscally unsound. Congress can instead insist that appropriated dollars not be spent on nuclear weapons tests, support the new president in restoring various arms limitation agreements, and undertake a serious, nonpartisan study of the actual need for a new fleet of ICBMs.

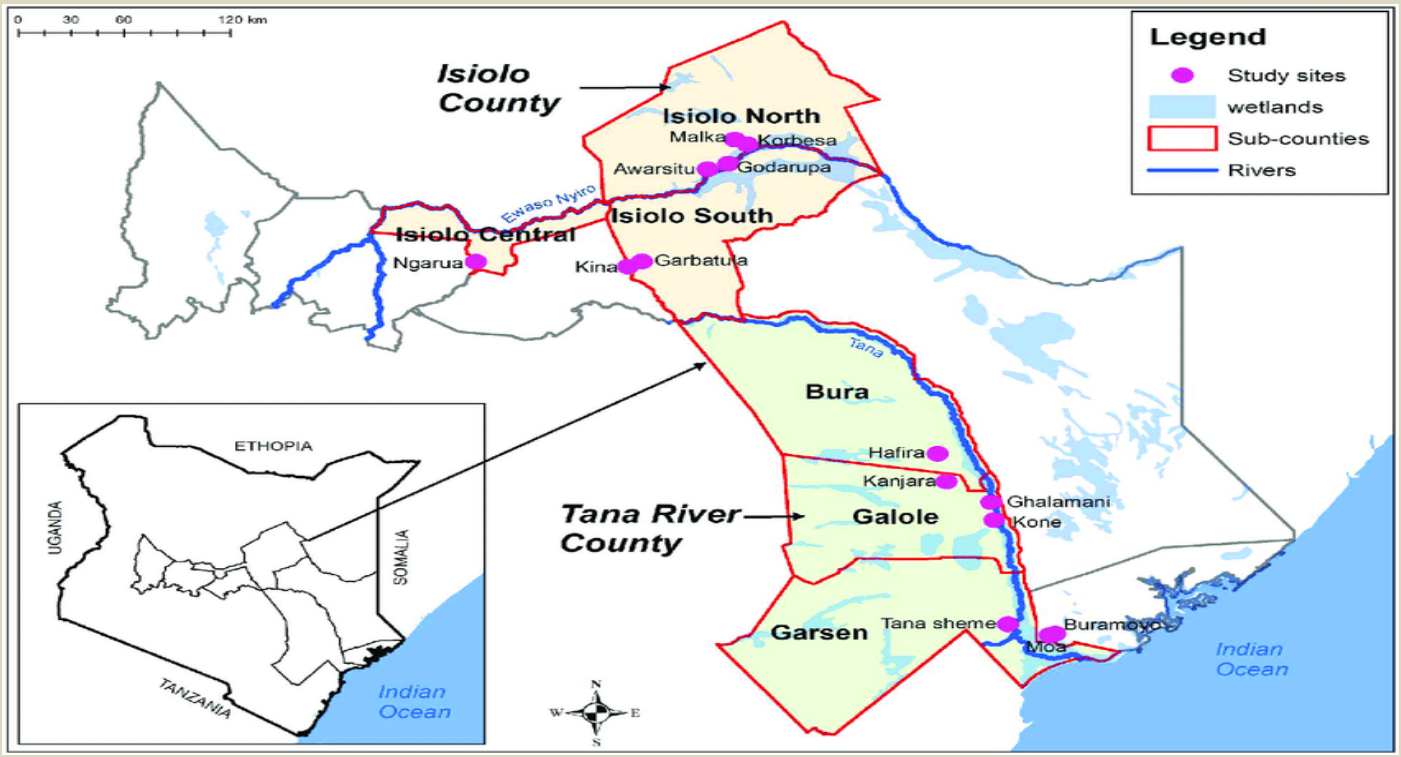
The single step from which profound policy change could flow, domestically and internationally, would be formal endorsement by the five original nuclear powers—the US, Russia, the UK, France, and China—of the Reagan-Gorbachev principle, jointly articulated

by the two leaders at their 1985 summit. It states simply, "a nuclear war cannot be won and must never be fought." International adoption would simultaneously indicate the nuclear powers' recognition of the rising dangers of nuclear conflict and the need to move toward nuclear forces around the world that are structured for deterrence, not war fighting. Words as principle have power. Eventually, these eleven words could underlie the next generation of arms control negotiations, strengthen the global nonproliferation regime, and help short-circuit a second nuclear arms race.

Jessica T. Mathews *was President of the Carnegie Endowment for International Peace from 1997 until 2015 and is now a Distinguished Fellow there. She has served in the State Department and on the National Security Council staff in the White House. (August 2020).*

Kenya – First Nuclear Power Plant within the decade

Source: https://newafricadaily.com/kenya–set–constructing–first–nuclear–power–plant–within–decade



Aug 05 – Kenya has set its sights on joining the club of commercial nuclear power users. The country's Nuclear Power and Energy Agency has submitted an environmental and social assessment report for a proposed US$5 billion nuclear power plant (1000MW; maximum capacity of generating 2,712 megawatts of electricit), which it says is on track to be completed in about seven years. A preferred site has been chosen near the coast in Tana River County, halfway between Mombasa and the Somalian border.

EDITOR'S COMMENT: I was just wondering: does Kenya has the required security infrastructure to ensure that the nuclear plant will be safely guarded the moment that Al Shabaab is very active in the neighboring Somalia? Kenya is East Africa's largest economy and It is good business for the US but what about the safety of the local people or the entire nation?

Armenian Ambassador on Azerbaijani threats of missile strike against Metsamor Nuclear Power Plant

Source: https://en.armradio.am/2020/08/03/armenian-ambassador-on-azerbaijani-threats-of-missile-strike-against-metsamor-nuclear-power-plant/

Aug 03 – Armenia has undertaken a number of measures to raise awareness about Azerbaijan's threat to strike the Metsamor Nuclear Power Plant, Armen Papikyan, Armenia's ambassador to the International Atomic Energy Agency, said in an interview with Energy Intelligence.

...

Q: What security arrangements are in place to defend Metsamor from any missile attack? And has the Armenian government evaluated what the impact of an attack on the plant would be?

A: We have adequate systems to defend the Metsamor NPP from any attack. Of course, not all of the systems are subject to disclosure, for security reasons. One can rest assured that the station cannot be attacked, as it is under the protection of the quite powerful and sophisticated air defense system. It is a multilayer defense, which includes the systems of Armenia and Russia. Armenia's sky is protected jointly with Russian respective units, based on a ratified international agreement. The safety and security of the NPP has always been a high priority for my government — first and foremost because it would have immediate implications for the security and safety of our population. It would be extremely difficult to imagine what could be the possible impact [of a successful attack]. We can recall the accident of Chernobyl. I think that is the easiest reply to your question.

Saudi Arabia, with China's help, expands its nuclear program

Source: https://www.wsj.com/articles/saudi-arabia-with-chinas-help-expands-its-nuclear-program-11596575671?mod=djemCapitalJournalDaybreak

Aug 04 – Saudi Arabia has constructed with Chinese help a facility for extracting uranium yellowcake from uranium ore, an advance in the oil-rich kingdom's drive to master nuclear technology, according to Western officials with knowledge of the site. The facility, which hasn't been publicly disclosed, is in a sparsely populated area in Saudi Arabia's **northwest** and has raised concern among US and allied officials that the kingdom's nascent nuclear program is moving ahead and that Riyadh is keeping open the option of developing nuclear weapons.

EDITOR'S COMMENT: Caution with Houthis' (Iranian) missiles – NW is as far as possible from Yemen but at the same time as close as possible to Iran or Israel; because today's allies might be tomorrow's enemies especially in this part of the world..

Flooding in North Korea threatens Yongbyon nuclear reactor

Source: https://www.aljazeera.com/news/2020/08/flooding-north-korea-threatens-yongbyon-nuclear-reactor-study-200813042919223.html

Aug 13 – A study of satellite imagery suggests recent flooding in North Korea may have damaged pump houses connected to the country's main nuclear facility, a US-based think-tank said on Thursday.Analysts at 38 North, a website that monitors North Korea, said commercial satellite imagery from August 6 to 11 showed how vulnerable the Yongbyon Nuclear Scientific Research Center's nuclear reactor cooling systems are to extreme weather events.

Forty US atomic tanks stored in Italy

Source: https://www.ilfattoquotidiano.it/in-edicola/articoli/2020/08/06/quaranta-nuove-atomiche-usa-entro-tre-anni-in-italia/5891464/

Aug 06 – According to a research last November by Hans Kristensen, an authoritative member of the Federation of American Scientists, the United States has 150, perhaps 100, nuclear devices stored inEurope and Italy would remain the European country with the highest number of bombs and the only one with two nuclear bases: Aviano and Ghedi. And Kristensen has estimated that there are 20 nuclear weapons in Aviano and 20 in Ghedi.

Combatting Potential Electromagnetic Pulse (EMP) Attack

Source: http://www.homelandsecuritynewswire.com/dr20200908-combatting-potential-electromagnetic-pulse-emp-attack

Sep 08 – The U.S. Department of Homeland Security (DHS) says it continues to prepare against evolving threats against the American homeland, most recently highlighting efforts to combat an Electromagnetic Pulse (EMP) attack which could disrupt the electrical grid and potentially damage electronics.

Last week, the department is releasing the Electromagnetic Pulse (EMP) Program Status Report as part of an update on efforts underway in support of *Executive Order (E.O.) 13865 on Coordinating National Resilience to Electromagnetic Pulses*. E.O. 13865 establishes resilience and security standards for U.S. critical infrastructure as a national priority.

EMP weapons have the potential to disrupt unprotected critical infrastructure within the United States and could impact millions over large parts of the country. Since the President's signing of the E.O. in March 2019, DHS, through the Cybersecurity and Infrastructure Agency (CISA), in coordination with the Science and Technology Directorate (S&T) and the Federal Emergency Management Agency (FEMA), has taken actions to address known EMP-related vulnerabilities to critical infrastructure.

The EMP Program Status Report highlights efforts taken across the public and private sector to foster increased resilience to EMP events. "Through data analysis, vulnerability and risk assessments, testing and pilot programs, and government and industry engagement, the department is identifying critical infrastructure and associated functions that are at greatest risk from an EMP, and developing and implementing best practices to reduce the risk,: DHS says.

"EMP attacks are part of the emerging threats against our nation and demand a response," said Senior Official Performing the Duties of the Deputy Secretary Ken Cuccinelli. "That is why DHS is taking these contingencies very seriously, working diligently to mitigate our risks and equipping our state and local partners with the resources they need to do the same. We've made significant progress and look forward to the work ahead."

"As the Nation's risk advisor, one of CISA's priorities is understanding and mitigating threats associated with EMPs," said CISA Director Chris Krebs. "Over the past year, we have worked with interagency and industry partners to identify the footprint and effects of EMP threats across our National Critical Functions, and are developing sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to EMPs."

In 2018, DHS released the Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD), which was the Department's first articulation of a holistic, long-term, partnership-based approach to protecting critical infrastructure and preparing to respond and recover from potentially catastrophic electromagnetic incidents.

Dozens More Mystery Drone Incursions Over U.S. Nuclear Power Plants Revealed

By David Hambling

Source: https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/amp/

Sep 07 – I recently described how a swarm of drones flew in a restricted area at Palo Verde Nuclear Power Plant on two successive nights last September. A new cache of documents obtained under the Freedom of Information Act (FoIA) reveals how 24 nuclear sites suffered at least 57 drone incursions from 2015 to 2019 – and Palo Verde itself was overflown again in December, despite new security measures.

The documents were obtained from the U.S. Nuclear Regulatory Commission by Douglas D. Johnson on behalf of the Scientific Coalition for UAP Studies (SCU). The SCU's main interest is in anomalous aerospace phenomena, more commonly known as UFOs, but Johnson uncovered a series of incidents involving something less exotic but potentially more threatening: commercial drones.

In the September incidents, a swarm of five or six large drones flew over the Unit 3 nuclear reactor at Palo Verde in Arizona for about eighty minutes, a length of time which suggested they were carrying out a thorough survey of the site. The documents released at the time referred to a similar incident at Limerick Nuclear Generating Station in Pennsylvania.

Johnson sent a follow-up request to get more details. The response was a terse list of fifty-seven security incidents (SIDs) involving drones, running from December 2014 to October 2019. This provides little more than the date and location, with no details of the number or type of drones involved. We do not know how many involved multiple, simultaneous drone flyovers. At the time the list was generated, three of the incidents were listed as 'Open' and five 'Closed Resolved.' but the overwhelming majority, 49 of them, were 'Closed Unresolved.' This indicates that for 85% of the cases the NRC has no idea who the perpetrators are or what they intended, and has given up on finding them.

There were seven drone incidents in 2017, rising to 21 in 2018, the last full year for which numbers were given.
Twelve of the sites had only reported a single incident, but others had seen several. Limerick had five drone sightings, Perry Nuclear Power Plant in Cleveland, Ohio, had six and Diablo Canyon near San Luis Obispo in California had no less than seven separate incidents from December 2015 to September 2018, all of them unresolved. The scale and number of intrusions indicate that this is not a local issue, and raise the possibility that drone overflights could be carried out by a large, coordinated organization.
While most of the sites were nuclear reactors, there were also **three drone incursions over spent nuclear fuel storage sites**, including Trojan in Oregon and Rancho Seco in California where radioactive waste is stored in steel canisters inside giant concrete casks.
The new release also indicates that a third incident occurred at Palo Verde in December 2019, this time apparently with only two drones, described as 'industrial-sized craft' three feet across, similar to those previously seen. As with the two previous incidents, they were exploring the Unit 3 reactor area. Following the September drone incident, Palo Verde was supposed to be protected by drone detection technology provided by 'Area Armor' (likely a typo for Aerial Armor) to pinpoint the drone operator within a 13-mile radius. The idea was that anyone flying a drone would be rapidly apprehended by site security personnel. This does not appear to have worked, and again the incident was closed as unresolved.
The big question is how much of a danger such drone overflights pose, and there has been some lively online discussion on this point. While reactors themselves are protected by thick concrete domes able to withstand the impact of a crashing airliner, the above-ground pools in which spend nuclear fuel is stored may be far more vulnerable.

A 2011 report by the Institute of Policy Studies noted that over 40,000 tons of highly radioactive waste is stored in pools, many above ground: "some of the largest concentrations of radioactive material on the planet." These pools are not heavily protected, but are in light structures similar to big-box stores and car dealerships.

A 2003 report noted how vulnerable such pools were to terrorist action, simply by making a hole in the pool to drain out the cooling water and causing the stored fuel to overheat: "We warned that U.S. spent fuel pools were vulnerable to acts of terror. The drainage of a pool might cause a catastrophic radiation fire, which could render an area uninhabitable much greater than that created by the Chernobyl accident."
Robert Alvarez, author of the 2003 and 211 reports, reiterated the danger from terrorist attacks on fuel pools in 2017.
Greenpeace sought to highlight how easy it would be to hit such a target by crashing a drone into a French nuclear plant in 2018.
How effective small drones would be is open to question. Certainly, small drones can be highly destructive against vulnerable targets, shown in incident where they blew up ammunition dumps and destroyed thousands of tons of munitions in Ukraine. The two-pound warhead fired by the shoulder-launched M72 rocket launcher can make a dime-sized hole through two feet of reinforced concrete. The drones seen at Palo Verde could carry something significantly bigger.
Drones might also locate, identify, distract or even target security personnel as part of a larger terrorist action. **If drone flyovers become routine, security may cease to consider they are a danger – until it is too late.**
The documents indicate that even within the Nuclear Regulatory Commission, the evaluation of the threats, vulnerabilities and consequences of drone overflights is still ongoing. In one meeting on security, "Staff pointed out that no flyovers have yet exhibited a threat to nuclear power plant."
That may sound reassuring. But as long as swarms of mystery drones are able to fly over nuclear facilities with impunity, there must surely be cause for concern.

***David Hambling** is the author of "Swarm Troopers: How small drones will conquer the world," following cutting-edge military technology in general and unmanned systems in particular. New science fiction collection "Time Loopers: Four Tales from a Time War" out now in paperback and Kindle.*

Do Russia's Sunken Nuclear Submarines Pose Environmental Danger?

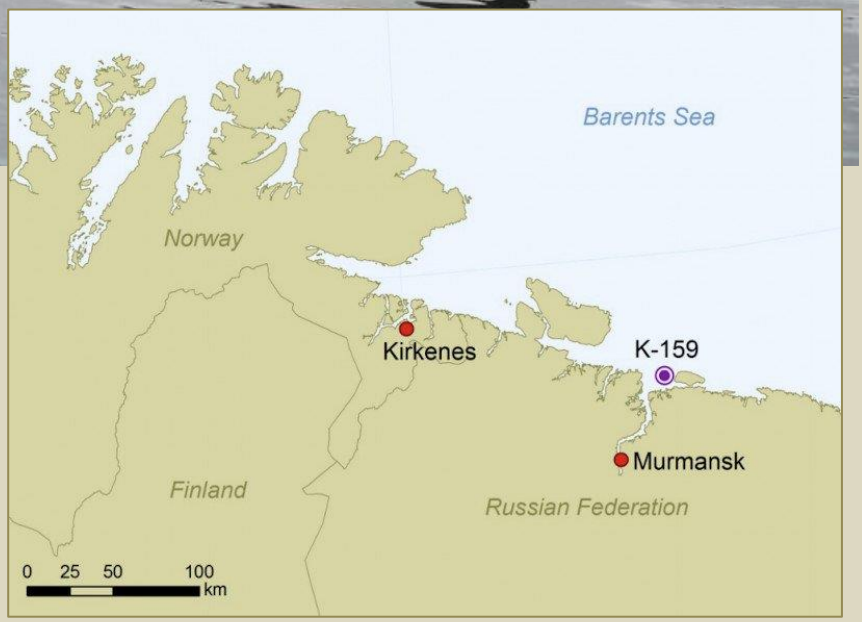
Source: https://www.popularmechanics.com/military/navy-ships/a33902569/russia-sunken-nuclear-submarines/

Sep 04 – Governments and environmental groups are worried a rupture of nuclear fuel supplies could cause a nuclear catastrophe, impacting local fishing areas. The Russian government is working to solve the problem, which some experts are calling a potential "Chernobyl in slow motion on the seabed."
A legacy of the Cold War threatens Russia's people and environment, potentially irradiating a large portion of the Barents Sea and closing it to commercial fishing. Two Soviet nuclear-powered submarines are sitting on the bottom of the ocean and could unleash their radioactive fuels into the surrounding waters.

The Soviet Union built four hundred nuclear-powered submarines during the Cold War. The vast majority were either scrapped, or still serve with the Russian Navy today. A few subs, however, are trapped in precarious circumstances, lying on the seabed floor with their uranium fuel supplies still intact. The BBC reports on efforts to render two such ships, *K-27* and *K-159,* safe.

The first ship, *K-27,* was a Soviet Navy submarine prototype equipped with a new liquid metal reactor. In 1968, the six-year-old sub suffered a reactor accident so serious, nine Soviet sailors received fatal doses of radiation. The submarine was scuttled off the Russian island of Novaya Zemlya in 1982 with its reactor still on board.

The second ship, *K-159* (shown above before sinking), was a *November*-class submarine that served a fairly typical career with the Soviet Northern Fleet before retirement in 1989. In 2003, however, the *K-159* sank while in the process of being dismantled, killing nine sailors. The ship still resides where it was lost, again with its reactor on board.



Environmentalists in Norway and Russia are concerned that eventually the reactors on both submarines will break down, releasing huge amounts of radiation.

This content is imported from {embed-name}. You may be able to find the same content in another format, or you may be able to find more information, at their web site.

The effects of these leaks could range from increasing local background radiation to declaring local fish and animals off limits, particularly Barents Sea fishing stocks of cod and haddock, costing local fishermen an estimated $1.5 billion a year.

While Russia's state-owned nuclear corporation, Rosatom, has been tasked with cleaning up the ships, the effort is underfunded, resulting in a race against time (and saltwater corrosion).

ICI International CBRNE INSTITUTE

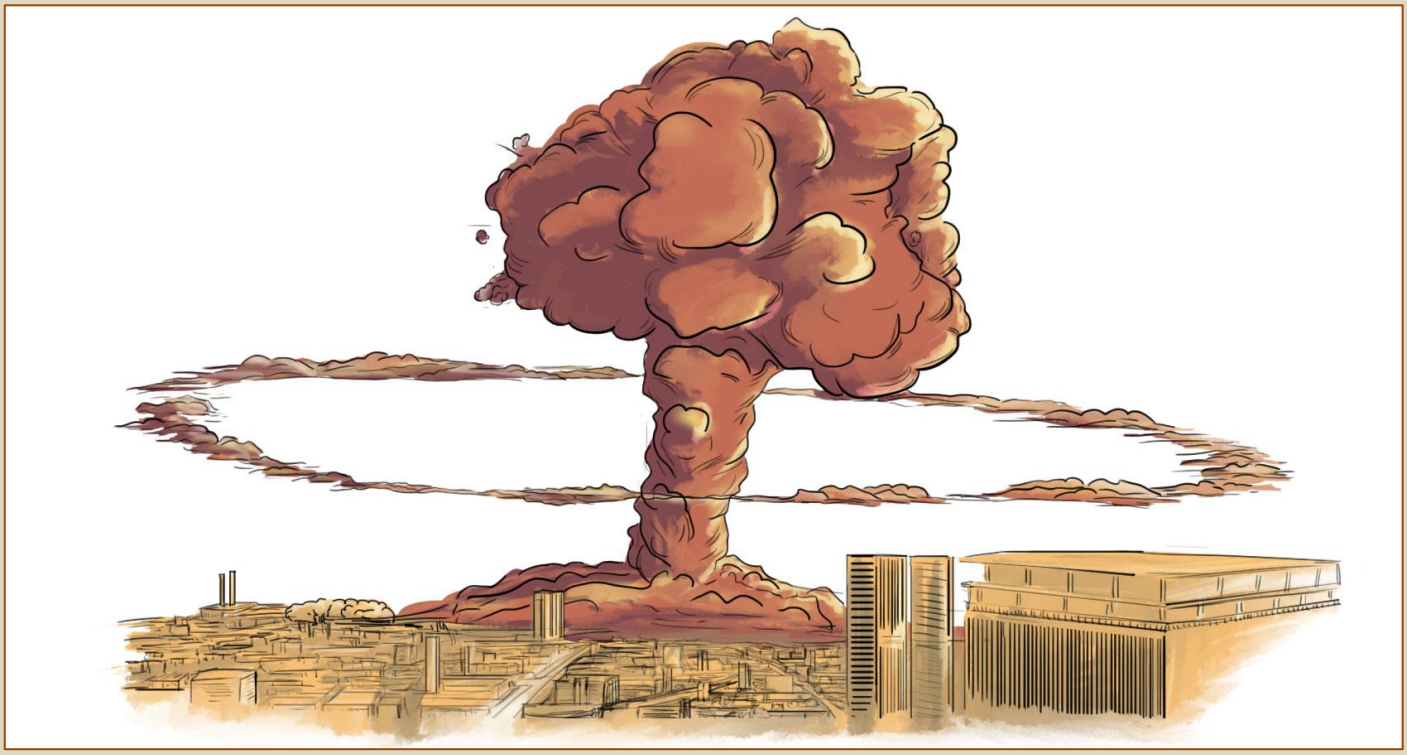
CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

How powerful was the Beirut blast?
Source: https://graphics.reuters.com/LEBANON-SECURITY/BLAST/yzdpxnmqbpx/



Aug 14 – Experts estimate the massive warehouse explosion that sent a devastating blast wave across Beirut could be one of the strongest non-nuclear explosions ever recorded.
Published Aug. 14, 2020
"On a scale, this explosion is scaled down from a nuclear bomb rather than up from a conventional bomb," said Roland Alford, managing director of Alford Technologies, a British company that specialises in disposal of explosive ordnance. "This is probably up there among the biggest non-nuclear explosions of all time."
Experts have estimated the size of the blast as being the equivalent of 200 to 300 tons of high explosives. **Here's what that figure looks like compared to other accidental explosions and conventional weapons. [see the infographic at source's URL].**

Hellfire missile
Power in TNT equivalent = 0.01 tons
U.S. air-to-ground tactical missile.

Mk-82 500lb bomb
Small U.S. unguided bomb.
0.1 tons

Mk-84 2,000lb bomb
American general-purpose bomb which entered service in the Vietnam war.
0.5 tons

Tomahawk missile
Intermediate-range cruise missile launched from U.S. Navy ships and submarines at subsonic speed.
0.5 tons

GBU-57 30,000lb bomb
The Massive Ordnance Penetrator (MOP) is a precision-guided "bunker buster" bomb.
2.4 tons

Oklahoma bombing - 1995
Ammonium nitrate mixed with other substances to make a bomb in an explosion that blew up a federal building in Oklahoma City, killing 168 people.
TNT equivalent = 2.5 tons

Chernobyl disaster - 1986
10 tons
Explosion and fire after a reactor meltdown at the Chernobyl power plant. The world's worst nuclear accident.

GBU-43B (MOAB)
11 tons
"Mother of All Bombs" (MOAB) is the U.S. most powerful non-nuclear weapon, it was first deployed in combat in Afghanistan, 2017.
10-20 tons

W54 Davy Crockett nuke
A small unguided nuclear rocket developed by the U.S. in the 1950s
12.5 tons

Texas fertiliser plant - 2013
An ammonium nitrate deposit exploded in the Texas town of West. 14 people died and about 200 more were injured.

Tianjin
Explosions at a warehouse storing various chemicals including 800 tonnes of ammonium nitrate killed at least 116 people.

CHINA
Tianjin, China - 2015
21 tons

FRANCE
Toulouse
Toulouse, France - 2001
40 Tons
An ammonium nitrate deposit exploded killing 31 people.

FOAB - ATBIP
44 Tons
The Russian bomb nicknamed the "Father of All Bombs" (FOAB) is reportedly the most powerful non-nuclear weapon in the world.

LEBANON
Beirut
Beirut blast
300-400 tons

Oppau, Germany - 1921
1,000 Tons
GERMANY
Oppau
An explosion of ammonium sulphate and nitrate fertiliser at the Oppau plant in Germany killed 565 people.

Halifax, Canada - 1917
2,900 Tons
CANADA
Halifax

Loaded with highly volatile explosives, the French steamer Mont-Blanc collided with the Norwegian ship Imo. Around 1,950 people were killed and about 9,000 more were injured.

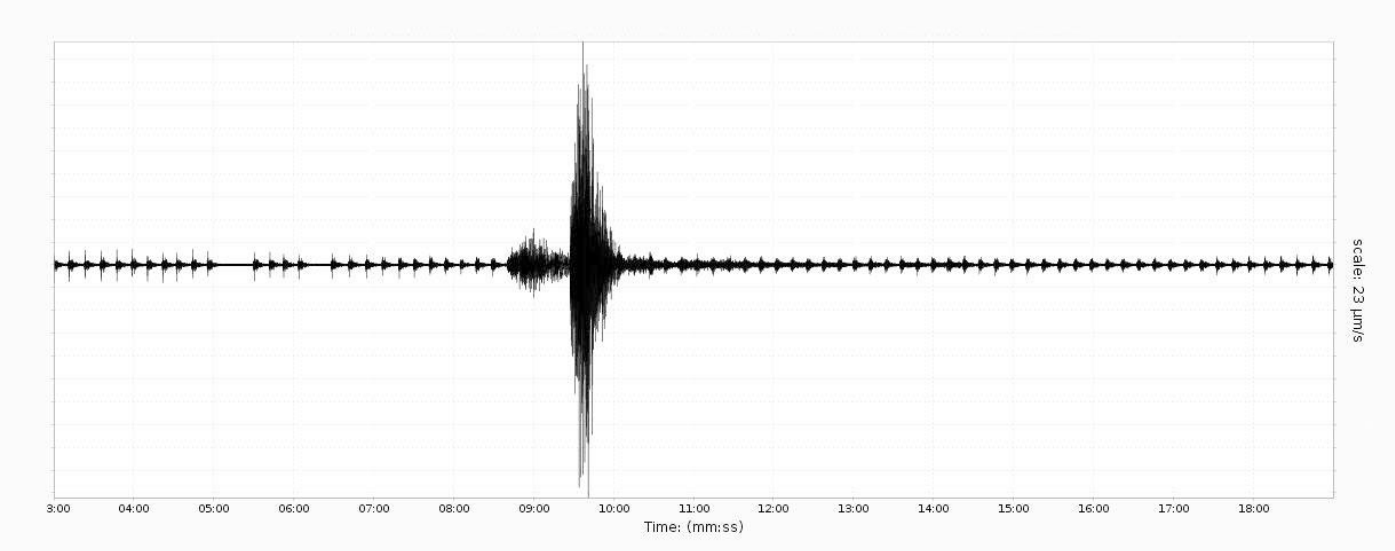
LITTLE BOY

Hiroshima, Japan - 1945
15,000 tons
JAPAN
Hiroshima
The first nuclear bomb used in war. Dropped by the U.S., the bomb killed tens of thousands and flattened the Japanese city of Hiroshima in an instant.

George William Herbert, an adjunct professor at the Middlebury Institute of International Studies Center for Nonproliferation Studies and a missile and effects consultant, used two methods to estimate the yield of the explosion. One used visual evidence of the blast itself along with damage assessments. The other calculation was based on the amount of ammonium nitrate reportedly at the source of the explosion.
Both techniques estimate the yield as a few hundred tons of TNT equivalent, with the overlap being 200 to 300, Herbert told Reuters.
Aerial footage shows damage at the blast site in Beirut two days after the explosion. August 6, 2020 | Reuters/Bader-Photography.com
The blast rattled buildings on the Mediterranean island of Cyprus, about 100 miles (160 km) away.

A string of explosions

Seismological data suggests that six blasts preceded the main explosion, the last of them a combustion of fireworks that apparently set off a warehouse full of ammonium nitrate, an Israeli analyst said on Thursday.
The six blasts were at 11-second intervals during the Aug. 4 incident, with the main explosion following the last by around 43 seconds, Boaz Hayoun of Israel's Tamar Group told Reuters.
Hayoun, a former military engineering officer whose current roles include overseeing safety standards for explosives use in Israel, said his analysis was based on data from seismological sensors stationed across the region.
"I cannot say categorically what caused this, but I can say these blasts were at the same location," he told Reuters.



Readings from a seismograph obtained by Reuters showing the explosion in Beirut on August 4, 2020. IRIS (Incorporated Research Institutions for Seismology)

Among the sensors cited by Hayoun was an array installed about 70 km (43 miles) off Lebanon's coast by the international geological project IRIS - which cast doubt on his conclusions.
IRIS said its sensors picked up more than five "small bursts" at intervals of around 11 seconds before the main Beirut explosion, a sequence that continued after the incident.
"I do not believe that they are associated with the large explosion in Beirut," Jerry Carter, director of IRIS data services, told Reuters.

"They could be from a seismic survey," he added, referring to geologists carrying out airgun bursts for underwater mapping.
Lebanese officials have blamed the explosion, which killed at least 172 people and left much of the capital in ruins, on a huge stockpile of ammonium nitrate catching fire after being stored unsafely at the port for years.
President Michel Aoun has said investigators would also look into the possibility of "external interference" such as a bomb, as well as negligence or an accident as causes.

Next-Generation Explosives Trace Detection Technology

Source: http://www.homelandsecuritynewswire.com/dr20200825-nextgeneration-explosives-trace-detection-technology

Aug 25 – Explosive materials pose a threat whether they are used by domestic bad actors or in a theater of war and staying ahead of our adversaries is a job that the Departments of Homeland Security and Defense share. Our research and development work are no different.

Most recently, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) transitioned technology to the Defense Advanced Research Projects Agency (DARPA), technology which is "representative of S&T's deep body of work in cataloging, detecting and thwarting explosive threats," S&T says. "Now this body of work will help keep our warfighters and our nation safe from weapons of mass destruction (WMD) threats."

The technology—a **Next-Generation Mass Spectrometry Explosive Trace Detector** (Next-Gen Mass Spec ETD)—was developed due to emerging explosive threats and evolving tactics by terrorists to evade detection. For the past decade, S&Tsays it has made it a top priority to equip and enhance DHS security personnel with next-generation capabilities that can rapidly identify and defeat these threats.

For example, we all know that explosive threats are a major concern in aviation security. They are the reason we remove our shoes as we go through airport checkpoints and why the Transportation Security Administration (TSA) scans every piece of luggage and cargo before loading them onto planes. The sheer variety of explosive materials, the many vehicles for deploying them, and the increasing tactics used to avoid detection pose a tremendous risk not only to American (and global) aviation, but across the entire homeland security enterprise.

Adapting S&T's Existing ETD Tech to Help DARPA Detect Weapons of Mass Destruction

S&T has been working not only with TSA, but also U.S. Customs and Border Protection and the U.S. Secret Service, to develop Next-Gen Mass Spec ETD capabilities for use at aviation checkpoints, border crossings, and other security operations across the country.

The program team realized that this technology could easily be modified to meet a pressing DARPA need as well. "The original intent of developing this Next-Gen Mass Spec ETD technology was to give Transportation Security Officers (TSOs) an alarm resolution tool that identifies, confirms and defeats current and emerging explosive threats," said S&T Program Manager Michael Palamar.

Many of us may have experienced being swabbed at airport checkpoints in a procedure called alarm resolution screening. TSOs use ETDs to determine whether harmful substances are present on cargo or the passengers transporting it—they use a sampling coupon to swab a piece of carry-on or checked baggage or a passenger's hands, place the coupon inside an ETD unit, and then analyze it for the presence of potential explosive residues.

Palamar continued, "We were surprised and pleased to find out that this same technology is equally adaptable for enhancing warfighters' capabilities to detect biological and WMD threats."

DARPA's SIGMA+ program is tasked with detecting illicit materials via highly-capable sensors and networks that alert authorities to chemical, biological, radiological, nuclear and explosives threats. They were looking to deploy chemical sensors that not only will provide early warning of WMDs, but that could also be scalable to cover a major metropolitan city and its surrounding region. A high-resolution and high-sensitivity mass spec technology that has been ruggedized for field operations was a logical choice for the SIGMA+ program.

S&T's years of taking ETD technology to the next level resulted in the Next-Gen Mass Spec ETD that will help DARPA meet its capability need. Key features of S&T's system include:

- **Enhanced capabilities to counter emergent threats**. This technology is designed to meet the most demanding requirements for explosive threat detection, including detection of homemade explosives.
- **Upgradable threat library and shortened threat library upgrade cycles**. The high spectral resolving power and sensitivity of industry partner Bruker Detection Corporation's triple-quadrupole mass spec technology play a key role in allowing faster threat identification and confirmation of specific threats.
- **Adaptable to operations in challenging environments**, such as adverse weather and high vibration environments.

The technology underwent two rounds of developmental testing and evaluation at S&T's Transportation Security Laboratory and one round of testing at TSA's Systems Integration Facility. It is also undergoing ruggedization for uses in air cargo facilities. In each of these testing and evaluation events, the technology showed proven capabilities in detecting and identifying emergent explosive threats.

Allowing DARPA to Communicate WMD Threats in Domestic Urban Environments

Now, with some modification, this critical, cutting-edge technology has been reconfigured for DARPA to use as an air-breathing sensor for early WMD warning.

"DARPA's SIGMA+ program has a requirement to deploy highly-capable chemical sensors as part of a mobile sensor architecture to provide WMD early warning," noted DARPA Program Manager Dr. Mark Wrobel. "S&T's development of an air-sampling variant of Bruker's compact triple-quadrupole mass spectrometer has provided a capability for SIGMA+ that would otherwise not have existed."

Leveraging S&T's Next-Gen Mass Spec ETD engine, DARPA integrates it with an air-breathing front end for sampling air and detecting chemical and explosive trace vapors and their pre-cursors in metropolitan environments. The high sensitivity of the detection engine is instrumental in giving DARPA a real-time detection capability against WMD, and the upgradable threat library and compressed library upgrade cycles play a key role in enabling the communications of WMD threats to responsible authorities—thus enhancing national security.

Thoi Nguyen, a contract scientist supporting S&T's development and analysis of the Next-Gen Mass Spec ETD for the last five years, seconded Dr. Wrobel's comment. "S&T tested and evaluated several other mass spec technologies for explosives detection. This technology came out on top both in high- probability of detection and low probability of false alarm."

The Power of Collaboration

S&T's work on Next-Gen Mass Spec ETD technology continues with TSA and other DHS agencies, "but it is always a proud moment when a new use case is not only identified but put into operational practice," S&T says.

Commenting on this fruitful collaboration, S&T's Dr. Laura Parker said: "It is a credit to the progress and impact of this next-generation ETD technology that S&T was able to collaborate with DARPA and share this technology. As government program managers, we are committed to using taxpayers' money more efficiently, and this technology transition is a win-win."

Four terrorists of Palestinian Islamic Jihad group blow themselves up accidentally while preparing to bomb Israel

Source: https://www.opindia.com/2020/08/four-palestinians-islamic-jihad-terrorists-killed-accidentally-trying-to-launch-bombs-at-israel/

Aug 26 – Four terrorists of the Palestinian Islamic terror groups were reportedly killed after they blew themselves up while preparing bombs at one of the camps of Gaza City near Shejaiya on Monday.

According to the reports, the four terrorists are identified as members of the Palestinian Islamic Jihad armed wing, who blew themselves accidentally while loading a rocket targeting the Israeli population.

In another similar incident, four members of the Islamic Jihad group had died in April 2018 near the southern Gaza Strip, following an 'accident' while preparing to attack Israel.

As bombs exploded near the terrorist camps in the northern Gaza City, Palestian media had claimed that the explosions were due to Israeli Air Force strikes. However, Israeli security officials denied carrying out strikes against the terror groups in that area, adding that it appeared to have been a "work accident".

The terror group later announced that four terrorists – Iyad Jamal al-Jidi, Muataz Amir al-Mubid, Yahya Fareed al-Mubid and Yaaqoub Zaydieh were killed in the blast during "preparations to remove the criminal entity from our occupied land". Meanwhile, a Hamas member speaking to the media on Monday that they will continue to inflict violence against

the Jewish homeland until their demands were met. “It is our right to break this siege,” Hamas leader Ismail Radwan said.

Russian Army develops system to detect suicide bombers in crowds using Syrian experience

Source: https://tass.com/defense/1194013

Aug 26 – Servicemen of the Russian Ground Forces' Fifth Scientific Regiment developed a system to detect the so-called suicide belts in crowded areas, using experience gained in Syria. The new system is presented at the Army-2020 international military and technical forum.

The new system includes a set of sensors, software and a mobile operator’s dashboard. It is capable of detecting suicide belts and improvised explosive devices (IEDs), stuffed with shrapnel, on large areas: at mass event venues, crowded places, checkpoints and transport infrastructure.

"If there is a suicide bomber in the crowd, the system will detect them thanks to unique radio frequency signature, characteristic only of suicide belts or IEDs. The operator will receive information about the object’s location, it’s distance to the nearest sensor, and - in case of moving targets - about the target’s movement, which would allow the operator to sound an alarm and give command to neutralize the threat," a representative of the 5th Scientific Regiment and one of the system’s developers told TASS.

According the developer, the system’s creation was prompted by the Syrian experience.

"The work began about 3 years ago, when our servicemen detected and seized a large number of belts and IEDs during transportation of militants, repatriation of refugees and mine defusing operations," the developer said.

The seized suicide belts and improvised explosive devices were studied and catalogued; this led to discovery of features, unique to improvised explosives. "For example, our system will never mix up a terrorist with a man carrying a bag of bolts from a store," the developer said.

He underscored that the system finalizes its tests and will soon be shipped to a security agency.

Scientific regiments

Currently, there are 17 scientific regiments in Russia, involving over 650 people. There are also four scientific and production regiments, involving over 200 people.

The Army-2020 international military-technical forum opened at the Patriot conference and exhibition center on August 23 and will run until August 29. Some demonstrations are underway at the Alabino shooting range, the Kubinka airbase and the Ashuluk range in the Astrakhan Region. The forum’s organizers expect guests from about one hundred countries. More than 1,500 organizations and manufacturers will present about 28,000 exhibits. Nearly 700 pieces of modern weaponry and other military hardware will be on display.

The New Team Sniffing Out Landmines

By Kylie Bielby

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/the-new-team-sniffing-out-landmines/

Aug 26 – You may remember our story about Magawa, the landmine detection rat that the *Homeland Security Today* team sponsors via APOPO, the global non-profit that trains Magawa and his fellow giant pouched rats. We even suggested that the rats may be taking over from dogs in the sniffing stakes…

Well the dogs have had something to say about that and now, on National Dog Day, APOPO has announced the inclusion of technical survey dogs to its team.

Over 60 million people living in 59 countries from Angola to Cambodia, do so in daily fear of landmines and other remnants of past conflict. Landmines remain as painful and dangerous reminders of the past, continuing to threaten personal safety, economic development and food security. Agricultural land is left unsafe to farm and grazing livestock is dangerous. Trade routes remain closed, cutting off communities and denying

families displaced by war the chance to return home safely. Yet detecting these weapons is very tedious and therefore expensive while global funding is declining.
Clearing minefields creates safe ground on which homes can be built and land can be cultivated. It gives new horizons and hope to people living at risk in vulnerable communities. By removing landmines and other explosive remnants of war (ERW), APOPO lays the foundation for recovery and restoring livelihoods.
Using an integrated approach of survey, vegetation-cutting machines, human deminers with metal detectors and mine detection rats, APOPO and partners have been releasing safe land quickly so that people can get their lives back on track.
With over 20 years of experience in research, training and successful operational use of mine detection rats, APOPO is uniquely positioned to train technical survey dogs. The APOPO dog training center is based in Cambodia and employs respected and experienced dog training experts with an extensive knowledge of land release methods and international as well as national demining authority standards. APOPO trainers carefully select Belgian Malinois puppies for training, and as our security friends know, this breed combines an excellent nose with a keen intellect.

HeroDOG Cyklon with his trainer (APOPO)

So how does it work? Prior to landmine clearance, areas need to first be surveyed. Traditional survey methods include the use of metal detectors, that require ground preparation and vegetation cutting. This makes the survey slow and expensive.
APOPO uses the special technical survey dogs (a.k.a. HeroDOGs) who can survey deep into an area without the need to prepare the ground or cut any vegetation. Michael Heiman, Program Manager for APOPO Mine Action Cambodia says a single technical survey dog can effectively survey an area of up to 4000 m2 per day across challenging terrain with high levels of vegetation. “Sniffing out the chemical compounds of explosives found in landmines they ignore scrap metal making them much faster at surveying hazardous areas than metal detectors.”
The dogs are trained to indicate when they find the smell of explosives from a safe distance away. Each dog is equipped with the Swiss developed SMART system – a backpack with Global Positioning System (GPS), a speaker and a video camera, that shows and records the dog’s search pattern and location. This allows the handler to instruct the dog through verbal command. When the dog finds an explosive item, the dogs are trained to sit down at a distance of at least one meter and wait patiently for their handler’s next command. This distance keeps the dogs safely out of harm’s way. The system also has the advantage

of creating a GPS validated search record, an improvement over existing pen and paper search documentation procedures.
A team of HeroDOGs surveys an area on a minefield twice as fast as traditional methods. On top of that the system generates maps with the survey progress and all the findings, which allows for better evidence-based decision-making on which areas will be released and which need to be cleared.
APOPO's detection animals are highly valuable assets, making animal welfare and safety a top priority. Just like the HeroRATs, the HeroDOGs are well cared for, receive an excellent diet, regular exercise, stimulation and enrichment and individualized attention from expert handlers.
HeroDOGs and HeroRATs play complementary roles. Technical survey dogs are used prior to clearance, together with the initial

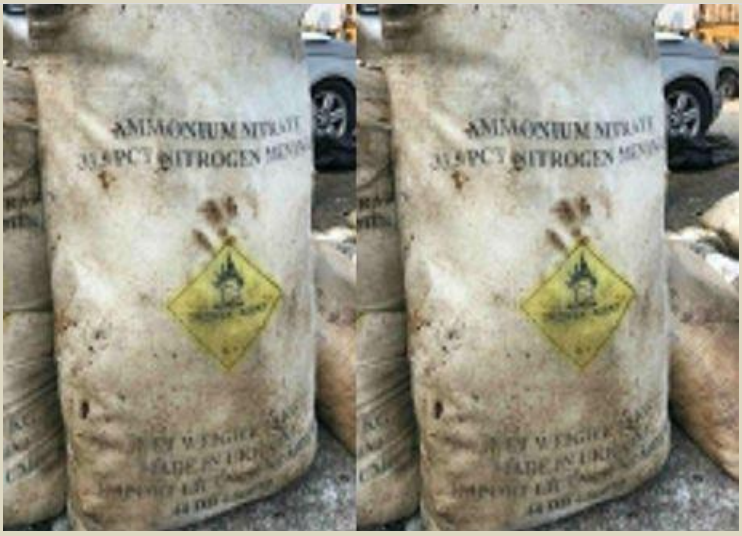
historical and geographical surveys that have been carried out to assess the probability of landmines. Detection rats are excellent for clearance of wide mine contaminated areas that have evidence of contamination.
APOPO says the use of HeroDOGs in technical survey applications will pave the way for even more effective use of APOPO's HeroRATs combining the dog's surveying speed and the rat's accuracy of detection. Together, the animals will hugely reduce the time needed to clear a minefield and deliver safe land back to impacted communities.

***Kylie Bielby** has more than 20 years' experience in reporting and editing a wide range of security topics, covering geopolitical and policy analysis to international and country-specific trends and events. Before joining GTSC's Homeland Security Today staff, she was an editor and contributor for Jane's, and a columnist and managing editor for security and counter-terror publications.*

Army Finds 4 Tons of Ammonium Nitrate near Beirut Port

Source: http://www.naharnet.com/stories/en/274664-army-finds-4-tons-of-ammonium-nitrate-near-beirut-port

Sep 04 – The army has discovered more than 4 tons of ammonium nitrate near Beirut's port, a find that's a chilling reminder of the horrific explosion a month ago that killed 191 people.
According to the military, army experts were called in for an inspection and found 4.35 tons of the dangerous chemical in four containers stored near the port. There were no details on the origin of the chemicals or their owner.
The find comes almost exactly a month after nearly 3,000 tons of ammonium nitrate stored at Beirut's port for six years detonated, wreaking death and destruction. Along with 191



people killed, more than 6,000 were injured and entire neighborhoods were devastated. The blast left nearly 300,000 people homeless and caused damage worth billions of dollars.

The military statement said that customs officials had called in the army to inspect containers at a facility near the port, where they found 4.35 tons of ammonium nitrate. It said army experts were "dealing with the material," an apparent reference that it was being destroyed.

Days after the Aug. 4 blast, French and Italian chemical experts working amid the remains of the port identified more than 20 containers carrying dangerous chemicals. The army later said that these containers were moved and stored safely in locations away from the port.

French experts as well as the FBI have taken part in the investigation into the Aug. 4 blast, at the request of Lebanese authorities. Their findings have yet to be released.

So far, authorities have detained 25 people over last month's explosion, most of them port and customs officials.

Army Chief Says Port Disaster Could Have Been Avoided

Source: http://www.naharnet.com/stories/en/274666-army-chief-says-port-disaster-could-have-been-avoided

Sep 04 – Army chief General Joseph Aoun announced Friday that the catastrophic explosion at Beirut's port could have been avoided had authorities acted in a different way.

"From the very first moments after the port blast, the army took charge of the area's security, seeing as that was its responsibility, even without the presence of an (official) authorization," Aoun said in Ras Baalbek, where he unveiled a statue honoring troops and citizens who fell in a battle to rout Islamic State militants from the town's outskirts and in suicide blasts inside the town itself.

"The magnitude and size of the disaster made the port's security, public safety and the search for survivors and missing people under the rubble its priority. We worked silently for several days, because words have no value compared to the blood of innocents, the moaning of the wounded and the tears of grief and pain," the army chief added.

"We grieved with them, because we lost eight martyrs and we have more than 300 wounded (soldiers). We got angry with them because this tragedy could have been avoided," Aoun went on to say.

He also noted that despite its several missions, which increased in number after the explosion, the army "will not allow terror to return" to the country.

"Our many responsibilities, which are an honor to us, will not deviate our attention from two enemies that do not rest whenever they seize chances: terrorism and the Israeli enemy," Aoun pledged.

US accuses Hezbollah of storing explosive chemical in Europe

Source: https://www.startribune.com/us-accuses-hezbollah-of-storing-explosive-chemical-in-europe/572444922/

Sep 17— Militant group Hezbollah has stored chemicals that can be used to make explosives in several European countries, a senior State Department official said Thursday as he appealed to countries in Europe and elsewhere to impose bans on the organization.

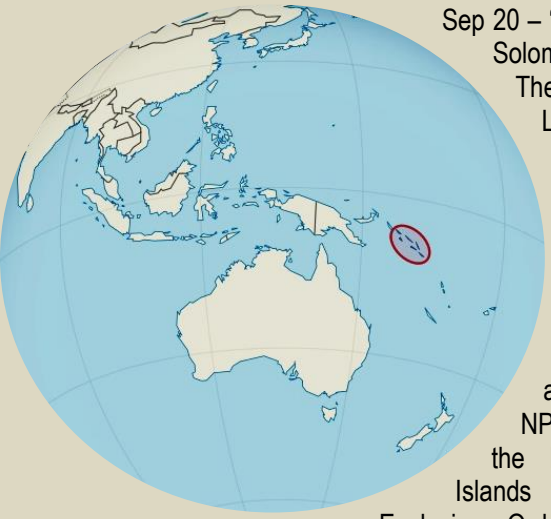
Hezbollah operatives have moved ammonium nitrate from Belgium to France, Greece, Italy, Spain and Switzerland in recent years and are suspected to still be storing the material

throughout Europe, said Nathan Sales, the State Department coordinator for counter-terrorism.
Ammonium nitrate is a chemical compound commonly used as a fertilizer, but it can be used to make explosives. It can also be dangerous in storage, as demonstrated by the huge explosion last month in the Lebanese capital of Beirut.
Sales, without offering evidence, said the U.S. believes that Iran-backed Hezbollah has since 2012 transported ammonium nitrate around Europe in first aid kits with cold packs that contain the compound. The United States believes these supplies are still in place throughout Europe, possibly in Greece, Italy and Spain.
"Why would Hezbollah stockpile ammonium nitrate on European soil?" he said. "The answer is clear: Hezbollah put these weapons in place so it could conduct major terrorist attacks whenever it or its masters in Tehran deemed necessary."
Sales made the remarks in an online forum hosted by the American Jewish Committee, which has called upon more countries to ban Hezbollah and its operations.
The U.S. has designated Hezbollah as a foreign terrorist organization since 1997, but some countries distinguish between the organization's military wing and the political wing.
The EU lists Iran-backed Hezbollah's military wing as a banned terrorist group, but not its political wing, which has been part of Lebanese governments in recent years. Some individual countries, including Germany and the U.K., have outlawed the group in its entirety. Sales called on more countries to do the same.
Hezbollah is a "unitary organization that cannot be subdivided into a military and so-called political wing," he said. Without a full ban, the group can still raise money and recruit operatives. "Hezbollah is one organization," he said. "It is a terrorist organization."

➲ **Sep 20** – France's foreign ministry said there was no evidence that Hizbullah stores chemicals in France that can be used to make explosives.

Two NPA staff died in tragic accident in the Solomon Islands

Source: https://www.npaid.org/news/two-npa-staff-died-in-tragic-accident-in-the-solomon-islands



Sep 20 – "We can confirm that two of our colleagues have died in a tragic accident in the Solomon Islands, says deputy Secretary General at Norwegian People's Aid, Per Nergaard. The two perished are British citizen Stephen «Luke» Atkinson, and Australian citizen Trent Lee. This is a tragic accident. So far, we know that there has been an explosion with fatal consequences. Our main priority now is to offer assistance to relatives and colleagues, and to clarify what has happened."

NPA's activities on Solomon Islands have temporarily been put on hold, and NPA is working together with the Royal Solomon Islands Police Force which is investigating the incident.

The accident took place in the **Solomon Islands**, where NPA is assisting the Government in developing a centralised database that gives an overview of the extensive amounts of explosive remnants of war contamination dating from the Second World War.

NPA is working with the Royal Solomon Islands Police Force, Explosive Ordnance Disposal Team, to develop an effective nation-wide information collection system.

"We are devastated by what has happened, and for the loss of two good colleagues. Our thoughts and deepest condolences go out to their families, relatives and staff," says NPA's Secretary General Henriette Killi Westhrin. "The safety and security of our staff is our highest priority, said Nergaard, emphasising that the investigation needs to be completed before there can be a conclusion on the cause of events."

Norwegian People's Aid has 1850 deminers working in 19 countries worldwide.

ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Editing for the Caliphate: Assessing Islamic State's Editing Process and Equipment

By Carsten Beyer

Source: https://gnet-research.org/2020/08/20/editing-for-the-caliphate-assessing-islamic-states-editing-process-and-equipment/

Aug 20 – For the past six years, Islamic State's media has awed potential recruits and shocked their enemies. The media has been abuzz over the years about the sophisticated and slick media output that the group has been able to produce, mostly with regards to their videos and their English language magazines, Dabiq and Rumiyah. Watching footage of late 2017's "Flames of War II" from Al-Hayat, or this year's nearly 53-minute documentary "To Be Absolved Before Your Lord" from Wilayah Yemen would draw the viewer into a world where lightning-fast cuts of combat footage and documentary-style storytelling are the norm.

Likewise, the anashid from Ajnad and Al-Hayat showcase audio that is cleanly recorded and mastered, while magazines like Dabiq and Rumiyah, along with their weekly Arabic-language newsletter Al-Naba show high-quality production values, modern and calligraphic fonts, glossy infographics, and the use of templates for a consistency in branding efforts.

This blog contribution analyses both the process and technology, both the software and hardware, that Islamic State has used since 2015, the date where editing software that they use is identifiable. As can be seen below, Islamic State media software, much like their camera equipment as pointed out by Yorck Beese, has not developed with Hollywood technology but with the home consumer and, at best, the journalistic editing market, and arguably that of the semi-professional.

The Media Editing Process

Before getting into the specifics of software and hardware used, it would be best to have an overview of the Islamic State editing process as a whole. Internal documents captured in Afghanistan and published by the CTC refer to the editing process as "processing the media material (montage)", the third out of five steps of in manufacturing media material. The internal document titled "The Essential Duties of the Media Mujahid" says that once raw materials are captured, or "documented", the media mujahid can start "processing the materials that were used to record the event." The document discusses several components of this task; formatting text news, designing and processing images into photo reports, and editing raw video and audio materials to produce final releases. The use of the term "montage", however, is further complicated in this document, in that it is not only the general editing role, but also "montaging raw video materials to produce video releases", which the document "Organizational Structure of the Media Office" says is taken care of by the montage team, who "produces filmed projects and turns them into video releases, and delivers them to the Exterior Publishing Team."

An internal letter released by the dissident Scientific Heritage Foundation dated April/May 2018 included a petition to the Delegated Committee from a group of personnel in the media department, and included their positions in the media department at the end of the document. These positions include editing roles such as "film editing and design" and "Al-Naba' designer", but also reveals there is a "joint film editing office for the near and distant wilayas", which likely serves as a link to the wilayat outside of Iraq and Syria, although the exact purpose is unclear.

Another internal document, "The Table to Evaluate Video Releases" highlights the importance of the editing process, at least for videos, as they are weighed at 40% of the Media Monitoring Committee's own evaluation table against the 30% for both the narrative development and cinematography elements. A sample of this evaluation from Rajab 1437 (April/May 2016) in practise illustrates the wide variation of final scores, ranging from a weak 25% score on the video "Sinai, the Land of Epic Battles and Sacrifice" from Wilayah Dimashq (albeit being published nonetheless, likely after heavy revision) to an excellent 95% score on the video "Invading Villages to Spread the Guidance" from Wilayah Halab. A report using additional internal documents and interviews conducted by Asaad Almohammad and Charlie Winter note that once the media products are edited, they are then sent to the Media Monitoring Committee and then the Media Council for review, revision (if needed), and finally sent on to be published both internally and externally.

Video Editing

Virtually nothing is known about the editing software that the Islamic State used in its days when it was known as Al-Qaeda in Iraq and the Islamic State of Iraq and Syria. Starting in 2015 however, there have been but a few brief looks into the software that they use to edit videos. The earliest of these previews can be found in the May 2015 video "Media Man, You Are a Mujahid Too" from Wilayah Salahuddin, where a media editor is using Adobe Premiere Pro to edit an earlier segment of the video on a MSI gaming laptop. On the taskbar at the bottom of the laptop, one can faintly see the logos of Adobe After Effects, Adobe Photoshop, TrueCrypt, and HandBrake, the latter two being a disk encryption application and an open-source transcoder for digital video files respectively. The most revealing look into Islamic State's video editing

capabilities is shown in the October 2018 video "Inside the Caliphate #8" from Al-Hayat, where snippets of the editing process is shown in Adobe Premiere Pro.

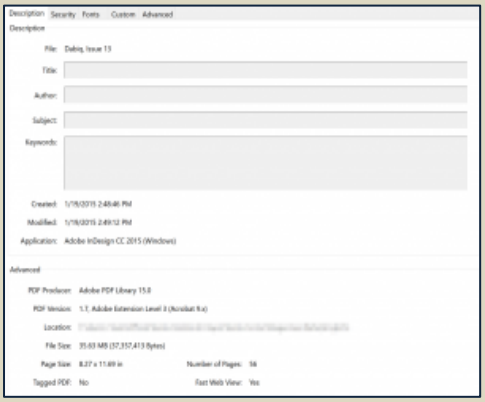
A glimpse of an IS media operative using the editing timeline in Adobe Premiere Pro

In the editing timeline for the aforementioned video, raw footage and simple effects such as cross dissolve can be seen in a multi-layered fashion. What is interesting to note is the names of some of the video files, taken from the Information Bank discussed throughout the CTC article by Almohammad and Winter, which are arranged in a pattern that shows the name of the wilayah, the title of the video, and a two-to-four digit number sequence. It is unknown exactly how the Information Bank handles file organisation, although it would be assumed that it is organised in a similar fashion to the bins in the Premiere Pro project displayed in "Inside the Caliphate #8" are, with folders sorting *anasheed*, closed captioning, commentary, footage (further subdivided into "additional 01", "attacks (*isdarat*)", and "*bayaah*").

Audio Production

Islamic State utilises two primary audio Digital Audio Workstations (DAW) for their media, the first of which is Adobe Audition. Its earliest appearance is found in the April 2015 video "Bulletin Radio from Wilayah Ninawa" from the aforementioned wilayah, alongside Winamp, a free audio media player. This video serves partly as a behind-the-scenes look at the Al-Bayan Radio station in Mosul, where it broadcasted daily news bulletins in at least six languages, played Qur'an recitations and *anashid*, and was a source of religious lectures and *fatwas*. With regards to hardware, Al-Bayan Radio was recorded in a professional studio, using what looks like a Montarbo 783 Mixing Console, along with a studio mic equipped with a pop filter and a shock mount. Other microphones can be seen used throughout the so-called caliphate's territory to record *anashid*, sermons, people interviewed for video releases, and broadcast announcements. The most common of these (aside from studio mics) are lavalier microphones (lav mics), and dynamic microphones, both of which are both compact enough to be carried around wherever the IS media team needs them.

Technicians at al-Bayan record a radio programme (left) an IS media official records video narration using MAGIX Samplitude (right)



A look at the EXIF data from Dabiq (issue #13)

The other DAW that Islamic State frequently uses is MAGIX Samplitude, which was the software of choice used by Mohammed Khalifa, the infamous English narrator of Islamic State to record narration and English daily news bulletins.

The first appearance of Samplitude in use is in the January 2016 video "Rather, They Are Alive with Their Lord" from Wilayat Al-Raqqah, which acts as a small documentary about the life of the *munshid* (*anashid* singer) Maher Mesha'al, who recorded *anashid* for the Ajnad Foundation. At the end of the video, Mesha'al is seen recording a *nasheed* in a small homemade studio with a studio microphone and Samplitude running in the background. Similarly, in the March 2017 video "And You Will Be Superior" from Wilayah Nineveh, a man is seen in front of an MSI laptop and studio microphone

recording narration for the aforementioned video, script in hand. Connecting all of this to the left of the laptop is an audio interface that looks similar, if not identical to a PreSonus AudioBox USB 96 2×2 USB Audio Interface.

PDFs and Photos

From Al-Hayat's various magazines to the weekly Al-Naba newsletter, the Islamic State has been consistent in using PDF files that fit an A4 paper size for standard printing and viewing. A forensic analysis of these files reveal that they are made mostly using Adobe InDesign, varying between being produced on a Windows or Macintosh computer. There are exceptions to this however, namely the pre-Dabiq newsletters Islamic State News and Islamic State Reports, both of which were made in Adobe Illustrator, and the Russian-language magazine Istok, which was created with CorelDRAW X6. Delving further into the metadata of Istok, one would find that three of the documents had the author "MSI", likely a default placer that means it was created on an MSI gaming laptop, while one of them had the author "adm", likely short for "admin."

Both Al-Naba and Rumiyah have also been consistently created with Adobe InDesign, the vast majority of them produced on Windows. A forensic analysis conducted by BadTigrou, a self-described ethical hacking enthusiast, reveals that it took the team behind Rumiyah roughly 11 days to write, translate, upload, and publish each issue. The English version of the magazine was the first to be finished, serving as the template for the other translation teams, who then translated and, in some cases, added additional exclusive articles (such as the article "Ubijajte imame kufra na Balkanu" in the Bosnian version of Rumiyah #8).

Currently, there is one piece of evidence that shows photo editing software in use shown at the end of the June 2019 video "Then They Will Be Overcome" from Wilayah Fallujah, where a media operative is seen editing a "breaking news" text statement in Adobe Photoshop using a pre-designed template that has been in use since late 2016, when Islamic State changed the branding style of its media products to its current form. It could be assumed, given the presence of the Adobe Photoshop icon, that Islamic State media editors frequently use Photoshop, and likely Adobe Illustrator to create the infographics seen in Al-Naba and Rumiyah. Additionally, exif data from a variety of posters, pamphlets, and billboards from Islamic State's publishing house Maktabah al-Himmah show that Photoshop, InDesign, and Illustrator are consistently in use.

Surprisingly, despite the decline of both the physical territory and media output of the so-called caliphate over the past several years, with the latest wilayah video release being earlier this week as of this writing, video quality and production/editing efforts seem to remain largely unfazed, and will likely continue this trend for the near future.

New Technique to Prevent Medical Imaging Cyberthreats

Source: http://www.homelandsecuritynewswire.com/dr20200825-new-technique-to-prevent-medical-imaging-cyberthreats

Aug 25 – Researchers at Ben-Gurion University of the Negev have developed a new artificial intelligence technique that will protect medical devices from malicious operating instructions in a cyberattack as well as other human and system errors.

BGU researcher Tom Mahler will present his research, "A Dual-Layer Architecture for the Protection of Medical Devices from Anomalous Instructions" on 26 August at the 2020 International Conference on Artificial Intelligence in Medicine (AIME 2020). Mahler is a Ph.D. candidate under the supervision of BGU Profs. Yuval Elovici and Prof. Yuval Shahar in the BGU Department of Software and Information Systems Engineering (SISE).

Complex medical devices such as CT (computed tomography), MRI (magnetic resonance imaging) and ultrasound machines are controlled by instructions sent from a host PC. Abnormal or anomalous instructions introduce many potentially harmful threats to patients, such as radiation overexposure, manipulation of device components or functional manipulation of medical images. Threats can occur due to cyberattacks, human errors such as a technician's configuration mistake or host PC software bugs.

As part of his Ph.D. research, Mahler has developed a technique using artificial intelligence that analyzes the instructions sent from the PC to the physical components using a new architecture for the detection of anomalous instructions.

"We developed a dual-layer architecture for the protection of medical devices from anomalous instructions," Mahler says. "The architecture focuses on detecting two types of anomalous instructions: (1) context-free (CF) anomalous instructions which are unlikely values or instructions such as giving 100x more radiation than typical, and (2) context-sensitive (CS) anomalous instructions, which are normal values or combinations of values, of instruction parameters, but are considered anomalous relative to a particular context, such as mismatching the intended scan type, or mismatching the patient's age, weight, or potential diagnosis. "For example, a normal instruction intended for an adult might be dangerous [anomalous] if applied to an infant. Such instructions may be misclassified when using only the first, CF, layer; however, by adding the second, CS, layer, they can now be detected."

The research team evaluated the new architecture in the computed tomography (CT) domain, using 8,277 recorded CT instructions and evaluated the CF layer using 14

different unsupervised anomaly detection algorithms. Then they evaluated the CS layer for four different types of clinical objective contexts, using five supervised classification algorithms for each context.
Adding the second CS layer to the architecture improved the overall anomaly detection performance from an F1 score of 71.6 percent, using only the CF layer, to between 82 percent and 99 percent, depending on the clinical objective or the body part. Furthermore, the CS layer enables the detection of CS anomalies, using the semantics of the device's procedure, an anomaly type that cannot be detected using only the CF layer.

Giant Library of Islamic State Group's Online Propaganda Discovered

Source: https://www.bbc.com/news/technology-54011034

Sep 05 – One of the largest collections of online material belonging to the group calling itself Islamic State has been discovered by researchers at the Institute of Strategic Dialogue.
The digital library contains more than 90,000 items and has an estimated 10,000 unique visitors a month. Experts say it provides a way to continually replenish extremist content on the net.
But taking it down is difficult because the data is not stored in one place. And despite counterterrorism authorities in Britain and the U.S. having been alerted to this growing repository, it continues to grow.

COVID-19 Exacerbates Huge Cybersecurity Staffing Shortage

Source: https://www.hstoday.us/industry/covid-19-exacerbates-huge-cybersecurity-staffing-shortage/

Sep 08 – The push to work from home during the coronavirus pandemic is straining cybersecurity professionals around the country tasked with ensuring workers are able to not only work efficiently from remote locations — but to do so safely. This rapid shift is a tall order for an industry that was already in need of skilled professionals long before the pandemic took hold.
Cybersecurity workers were taken off some or all of their typical security duties to assist with other IT-related tasks, including equipping mobile workforces, according to an April survey from global nonprofit (ISC)2, the largest association of certified cybersecurity professionals. The survey of 256 cyber pros found nearly half were re-tasked and that a quarter said cybersecurity incidents increased since the transition to remote work, with some seeing as many as double the number of incidents. Separate data from another nonprofit cybersecurity group, the Information Systems Security Association, found a 63% increase in cyberattacks related to the pandemic, calling Covid a "once-in-a-lifetime opportunity for hackers and online scammers."
"We are outnumbered—the people that are doing bad things, whether it's a nation-state type of activity or cybercrime—the good guys and gals were vastly outnumbered prior to the pandemic," says David Shearer, CEO of (ISC)2. "It has a compounding effect to what was already a challenge… take all of this technology we are becoming more and more reliant on and it's scaling in a massive pace."

Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures

Source: https://www.nowpublishers.com/article/BookDetails/9781680836868
E dited by **John Soldatos**, University of Glasgow and INNOV-ACTS LIMITED, UK | **James Philpot**, European Organization for Security, UK | **Gabriele Giunta**, Engineering Ingegneria Informatica S.p.A., Italy
Publication Date: 17 Sep 2020
Suggested Citation: John Soldatos (ed.), James Philpot (ed.), Gabriele Giunta (ed.) (2020), "Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680836875

Description
Modern critical infrastructures comprise of many interconnected cyber and physical assets, and as such can be considered as large scale cyber-physical systems. Hence, the

conventional approach of addressing cyber security and physical security separately is no longer effective. Rather more integrated approaches that address the security of cyber and physical assets at the same time are required. This book presents integrated (i.e. cyber and physical) security approaches and technologies for some of the most important infrastructures that underpin our societies. Specifically, it introduces advanced techniques for threat detection, risk assessment and security information sharing, based on leading edge technologies like machine learning, security knowledge modeling, IoT security and distributed ledger infrastructures. Likewise, it presets how established security technologies like SIEM, pen-testing, vulnerability assessment and security data analytics can be used in the context of integrated Critical Infrastructure Protection.

The novel methods and techniques of the book are exemplified in case studies involving critical infrastructures in four industrial sectors, namely finance, healthcare, energy and communications. The peculiarities of critical infrastructure protection in each one of these sectors is discussed and addressed based on sector-specific solutions.

The advent of the fourth industrial revolution (Industry 4.0) is expected to increase the cyber-physical nature of critical infrastructures as well as their interconnection in the scope of sectorial and cross-sector value chains. Therefore, the demand for solutions that foster the interplay between cyber and physical security, and enable Cyber-Physical Threat Intelligence is likely to explode. In this book we have shed light on the structure of such integrated security systems, as well as on the technologies that will underpin their operation. We hope that Security and Critical Infrastructure Protection stakeholders will find the book useful when planning their future security strategies.

Patient Dies After Ransomware Attack on Düsseldorf Hospital

Source: https://securityboulevard.com/2020/09/patient-dies-after-ransomware-attack-on-dusseldorf-hospital/

Sep 18 – According to reports, the network failure announced by Düsseldorf University Hospital (UKD) last week – which turned out to be a ransomware infection – has resulted in a patient dying.

"In the morning hours of Thursday (September 10th), larger parts of the IT systems of the Düsseldorf University Hospital were gradually no longer usable," the institution said in a notice last week. "This has far-reaching consequences for hospital operations, as activities in the computer system are necessary for many processes. For this reason, the UKD has canceled the emergency care," reads a machine-translated version of the notice.

On September 11, a day after the network failure, UKD was already investigating a "possible hacker attack."

The Associated Press now reports:

"German authorities say a hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment."

Hackers reportedly left an extortion note on a hospital server, indicating a ransomware operation. However, it appears the attack was directed at an affiliated university, not at the hospital.

Local police were able to reach the hackers and notify them that they'd hit the hospital instead of the university, as the extortion note claimed. When they learned of their blunder, the hackers provided a decryption key.

"The hackers are no longer reachable, they said," the AP report states.

Heise Online reports that the hackers' entry point likely was a vulnerable Citrix VPN appliance. The vulnerability in question is CVE-2019-19781 – dubbed "Shitrix" by the ever-spirited Internet community.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

& Robotics

DRONE NEWS

10 TINY Micro Robots and Nano Drones

Source (video): https://www.youtube.com/watch?v=j_Nws3R4fsA&feature=emb_logo

Even if advances in robotics mean fewer humans on the battlefield, the fight will increasingly focus on those that remain.

By Zak Kallenborn

Source: https://www.defenseone.com/ideas/2020/08/robot-war-kill-humans/168038/

Aug 27 – Last week's lopsided showdown between a human F-16 pilot and an artificially intelligent one — the robot won 5-0 — was just the latest sign that we need to be thinking harder about the changes that smart machines are bringing to the battlefield. Among them: as relatively cheap robots play larger roles, the focus of warfare will shift to attacking and defending the humans that operate, maintain, and even build them.

Now and for the foreseeable future, military robots still need humans. Robots are not (yet) capable of the complex thinking required for warfare; advances in speed and computational power do not automatically bring basic common sense. A robot cannot tell the difference between a farmer with a gun and a soldier.

So the military frequently focuses on the concept of human-machine teaming: the machine does what it does best, and the humans do the rest.

In the short term, humans are needed to make decisions on the use of force. Autonomous systems can beat an F-16 jockey in a dogfight, but they cannot decide whether a target is worth striking. Current Department of Defense policy does not allow autonomous weapons to make decisions on the use of force without appropriate human judgement.

However, the longer term is less clear. As single robots grow into massive swarms and become true weapons of mass destruction, humans will lack the cognitive capacity to manage the complexity without the aid of computers. Still, proponents of autonomous weapons bans may succeed in creating policies, laws, and treaties mandating that humans remain in control of firing decisions.

Humans will also be needed to create, maintain, and manage the robot army. Human programmers write the algorithms and software that operate the robot. Tacticians, strategists, and policy-wonks need to formulate the best ways to test, employ, control, and manage them. When a robot returns from combat, human maintainers will inspect, repair,

and otherwise maintain the robot. Any base or outpost where the robots are stationed will also need staff to sustain and operate it. All this means that killing the human operator and maintainers of robotic systems will often impose a much higher cost than disabling the robots. If the battlefield consists of fighting robots, the only cost is treasure. The destruction of a robot results in the loss of the time and money spent to build it. Robotic warfare seems to favor the small and many over the big and expensive, so the loss of a few robots may be quite low.

A screen capture from the Alphadogfight challenge produced by DARPA on Thursday, August 20, 2020. DARPA / Patrick Tucker

It is much harder to recruit, train, and equip the humans that support them. According to a recent RAND study, American drone pilots are already understaffed and over-stressed. While greater levels of autonomy will reduce the need for and stress on human pilots, humans are still needed. Killing the human-half of a human-machine team would prevent the machine from being strategically effective or even firing at all (if current limitations continue). Eliminating the maintainers and other support staff would also cause harm across the robotic fleet. Even if robots are decisive on the battlefield, they cannot maintain themselves off the field.

A robotic war also incentivizes attacking the people and facilities of the defense industrial base. Sabotage or destruction of a robotics factory or disrupting the factory's supply chain would have much greater impact than destroying a few robots in the field. Of course, adversaries may launch non-violent information attacks, particularly against facilities in the American homeland. For example manipulating the algorithms that allow unmanned systems to see, fly, and make decisions would create problems in every robot that used those algorithms.

The higher the seeming safety of soldiers, the higher the psychological impact of their death. A major advantage of unmanned systems is the reduced risk to soldiers. Remote pilots fly Predator drones from hundreds of miles away in a safe, and secure base. The sense of security is not only for the soldier, but for their mom and dad back in the United States. Violating that sense of security could create much broader effects on public support for a war effort. During the 1992-93 U.S. intervention in Somalia, images of American soldiers being dragged through the streets quickly turned public and policymaker opinion against the conflict. Dragging a robot through the streets of Mogadishu is unlikely to have the same effect.

Perhaps the F-16's loss to an AI was a fluke, but even if not, humans are not leaving war anytime soon. The United States and other militaries should focus on the vulnerabilities and value in targeting humans. Militaries should conduct war games and simulations to understand what roles are most critical to maintaining a robotic army. Analysis should also focus on how best to protect people in those roles.

Zachary Kallenborn *is a national / homeland security consultant, specializing in unmanned systems, drone swarms, homeland security, weapons of mass destruction (WMD), and WMD terrorism. His research has been published in Studies in Conflict and Terrorism, the Nonproliferation Review, War on the Rocks, the Modern War Institute at West Point, and Defense One. His research has been written about and shared in Forbes, Popular Mechanics, Homeland Security Today, the National Interest, and Yahoo News. His most recent study examines whether drone swarms could be considered weapons of mass destruction.*

Air Force One with Trump on board nearly hit by drone, report says

Source: https://www.independent.co.uk/news/world/americas/us-politics/trump-air-force-one-drone-plane-maryland-land-joint-base-andrews-a9675126.html

Aug 29 – Air Force One, with Donald Trump aboard, was nearly struck on Sunday night as it approached a military airport outside Washington, according to reports.

The aircraft appeared yellow and cross-shaped, and came near the executive jet around 5:54pm on Sunday, according to wire reports.

Mr Trump was returning from a long weekend at his Bedminster, New Jersey, golf resort. He also visited his younger brother, Robert Trump, who passed away on Saturday night in a New York hospital.

The drone did not strike Air Force One.

Federal safety officials have struggled in investigating such events in the past.

One reason is that most commercial drones are small and weigh only a few pounds. Some military aircraft have been hit by them, but were not taken down or seriously damaged.

The remotely piloted aircraft are not supposed to fly higher than 400 feet.

As commercial drones became more and more affordable last decade, some aviation experts warned they would be hard for the government to regulate and prevent from causing havoc for large planes and helicopters.

EDITOR'S COMMENT: Perhaps Secret Service learnt something from this incident – if it is true of course. Something like (1) they did not see it coming; and (2) despite the ability of Air Force One to sustain a missile attack or whatever, what about a swarm attack aiming the 4 tourbines of the aircraft? (with or without IEDs) – especially during take off or landing.

I Saw Israel's Revolutionary New Tactical Drones Up Close

By Seth Frantzman

Source: https://www.meforum.org/61442/israels-new-tactical-drones

Aug 26 – Israel has been a pioneer in drone innovation since the 1980s when it used drones effectively to find and then suppress Syrian air defense in Lebanon. Since then Israelis have been behind a few of the successful long-range and high altitude drones and an Israeli based in the United States helped invent the MQ-1 Predator. However, the next generation of drones won't be large armed drones deployed by air forces. Instead, they will be small drones that are operated by infantry and special forces units on the ground. Here, Israeli technology, including start-ups, is pointing the way again.

SpearUAV, which makes drones that are deployed from a canister or capsule, is seeking to transform the way unmanned aerial vehicles (UAVs) are deployed on the battlefield. It has made a line of UAVs, called Ninox, which come in several sizes from what it calls its Ninox 40 to Ninox 103. Spear unveiled Ninox earlier this month and showed off photos and video of the drone being deployed from a grenade launcher or from tanks and vehicles. Once fired out of its capsule the drones unfold and can conduct their missions.

SpearUAV's capsuled Ninox 40 micro-tactical drone can be deployed by firing it from a 40 mm grenade launcher. (SpearUAV)

I drove down to Tel Aviv to see the drone up close. One of the issues facing infantry and special forces units that want to use drones is that often they have had to get a hold of commercial drones because military-grade counterparts were not available or were still in the slow process of procurement. Several problems are involved when it comes to tactical drones. One issue is cost. Militaries want small drones that platoons can use but these types of drones need to be rugged or expendable because the nature of ground forces hiking through mountains or fighting in cities is that their equipment gets tossed around.

Second, tactical small drones need to be easy to use. While an air force operator of an MQ-9 Reaper drone can be trained for months and works in an air-conditioned command post, the soldier in the field needs to use their rifle and potentially pilot a drone on the side. That means using a tablet or some simple technology that soldiers already know how to use from civilian life, such as pointing and clicking on a screen. The company envisions the operator having an easy fold-down screen incorporated into a tactical vest, resting where a soldier might otherwise carry ammunition in pouches.

SpearUAV attempted to solve these challenges by putting their drones into a capsule. Think of basically deploying a drone from a tube, like the kind Pringles chips come in. This has the advantage that the UAV could be fired into the sky like a grenade or flare or it could be put on a tank in place of a smoke canister. This also means the drone can be easily packed into the field without concerns it might get dust or mud or water in it.

At the company's headquarters in Tel Aviv, the place is festooned with different types of Ninox drones and the tubes they go in. There are prototypes and final models and three-dimensional printers doing work while engineers work on computers. On display are the Ninox 40, a 250-gram UAV that can fly for forty minutes; the Ninox 66 made for use with tanks and other vehicles with fifty minutes flight time, and the Ninox 103 that is designed for larger payloads with sixty minutes of flight time.

Gadi Kupperman, the founder and CEO, says that the systems were developed as a direct response to the need of military forces for immediate intelligence capabilities. "This is a groundbreaking technology that will revolutionize the battlefield."

Founded in 2017 the company is an example of Israel's defense industry potential. Small, agile, and full of former soldiers with expertise in engineering, it illustrates the kind of field expertise innovation that Israel has tended to be good at. This means creating quick solutions to problems of the modern battlefield. For instance, Israel pioneered the Iron Dome air defense system and also the Trophy protection for tanks.

Boaz Ben-Haim, head of business development is a former pilot like Kupperman. They both came from other large Israeli defense companies and they say their two-dozen staff have similar backgrounds. Ben-Haim brings an example of one of the Ninox 40 drones to showcase. The material the drone is made out of is strong and feels different than what one is used to handing a commercial drone, which tends to feel vulnerable and fragile. The whole drone can be folded easily so it resembles a stick that can be stuffed into a tube. "We are creating a new dimension for the foot soldier," Ben-Haim says.

For the average infantry soldier or special forces warrior not much has changed in terms of the basic equipment they have had access to over the years. Ben-Haim notes that their lethality hasn't changed. Giving them drones, especially drones that may have munitions on them, what is called a loitering munition, would increase lethality. "For managing today's chaotic battlefield, the soldier needs affordable, scalable, accessible equipment," Ben-Haim says. What this means is not letting the cost of these drones balloon. Instead, these encapsulated UAVs could even be expendable, which means not needing to have them come back to base and be repaired or their batteries recharged.

The capsules were designed with existing platforms in mind, so the Ninox 66 can fit in smoke grenade launchers that are already used by main battle tanks. Upgrades to the drone itself could include a better camera or communications or different payloads. The main advantage the drone has is that since it sits inside a ruggedized capsule it can be moved around on the battlefield up until the point of deployment.

There are successes and hurdles to cross to bring these kinds of encapsulated UAVs to the front line. First of all, the drone is in the pipeline of Israel's Ministry of Defense with aspirations to be operational with the Israel Defense Forces. Then there are the issues of export to other friendly countries abroad. This system is ideal for countries that are focusing on hi-tech for frontline units and which are transforming their large armies into smaller, more lethal forces that are open to using new technology. This could mean countries like Australia or the United States. Other countries, such as the Philippines are also acquiring small drones for units fighting terrorism. Homeland security applications for small tactical drones also could see the Ninox used on border fences or facilities.

The coronavirus pandemic has made demonstrating weapons systems like this more difficult. That means finding local partners in various countries and also eventually having logistic support in other countries that might procure one of the drone types. Because incorporating a drone into grenade launchers could take time and because not all units use launchers as a standard-issue, the deployment of the drone through a launch tube, like a mortar, may be the first way it sees action. This is a learning curve developed from how flares are fired because a flare is also deployed from a tube.

The Firefly is a loitering munition that weighs only 3kg, so it can be carried into battle by soldiers.

The company notes that the concept of using expendable drones is new. However, Israel has been pioneering a number of drones that are expendable, usually in the format of what is called a "loitering munition." For instance, Rafael's FireFly is deployed from a canister and is designed to slam into a

target. Rafael views its FireFly as part of its Spike family of precision-guided missiles, not as a drone. Nevertheless, the FireFly's ability to hover over a target means it functions like a drone.
Like the Ninox it is also designed to be easy and intuitive to use. UVision also makes a line of loitering munitions and its Hero-20 weighs only 1.8 kilograms and is designed to be packed into battle. These systems have not been widely incorporated into infantry units which means most militaries have not taken tactical drone use to the next level. Ben-Haim notes that one of the issues facing drone operators and militaries is the need to get UAVs over a target quickly. A smuggler penetrating a border fence might only be in the area for a few minutes before driving away. Being able to deploy a drone quickly to follow the smuggler's vehicle is essential. Deploying it from a tube from a vehicle also means it doesn't take up much real estate on armored vehicles. Today's vehicles are already festooned with a plethora of radar and communications and other weapon systems, so adding drones to their roof means taking up space. Putting the drone in a tube saves space.
After decades of the global war on terror, the U.S. military is shifting defense strategy to confront near-peer competitors such as Russia and China. That means using fewer counter-insurgency measures and needing more technology that can operate against enemies seeking to jam weapons systems or operating in GPS-denied environments. Tactical drones have come on the scene at this crossroads in military history. They may be ideal for a wide range of specializations, from special forces operations in places like Niger to anti-cartel operations in areas where drug trafficking is a threat. In large numbers, they could be incorporated onto armored units and infantry platoons. This requires militaries to adapt and decide to systematically acquire different types and layers of drones for units the way militaries once incorporated light machine guns or mortars.

***Seth Frantzman** is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at The Jerusalem Post.*

Robot takes contact-free measurements of patients' vital signs

Source: https://news.mit.edu/2020/spot-robot-vital-signs-0831

Caption: Using four cameras mounted on a dog-like robot developed by Boston Dynamics, the researchers have shown that they can measure skin temperature, breathing rate, pulse rate, and blood oxygen saturation in healthy patients, from a distance of 2 meters. Credit: Courtesy of the researchers

Aug 31 – During the current coronavirus pandemic, one of the riskiest parts of a health care worker's job is assessing people who have symptoms of Covid-19. Researchers from MIT and Brigham and Women's Hospital hope to reduce that risk by using robots to r emotely measure patients' vital signs.
The robots, which are controlled by a handheld device, can also carry a tablet that allows doctors to ask patients about their symptoms without being in the same room.

"In robotics, one of our goals is to use automation and robotic technology to remove people from dangerous jobs," says Henwei Huang, an MIT postdoc. "We thought it should be possible for us to use a robot to remove the health care worker from the risk of directly exposing themselves to the patient."
Using four cameras mounted on a dog-like robot developed by Boston Dynamics, the researchers have shown that they can measure skin temperature, breathing rate, pulse rate, and blood oxygen saturation in healthy patients, from a distance of 2 meters. They are now making plans to test it in patients with Covid-19 symptoms.
"We are thrilled to have forged this industry-academia partnership in which scientists with engineering and robotics expertise worked with

clinical teams at the hospital to bring sophisticated technologies to the bedside," says Giovanni Traverso, an MIT assistant professor of mechanical engineering, a gastroenterologist at Brigham and Women's Hospital, and the senior author of the study.
The researchers have posted a paper on their system on the preprint server techRxiv, and have submitted it to a peer-reviewed journal. Huang is one of the lead authors of the study, along with Peter Chai, an assistant professor of emergency medicine at Brigham and Women's Hospital, and Claas Ehmke, a visiting scholar from ETH Zurich.

Measuring vital signs
When Covid-19 cases began surging in Boston in March, many hospitals, including Brigham and Women's, set up triage tents outside their emergency departments to evaluate people with Covid-19 symptoms. One major component of this initial evaluation is measuring vital signs, including body temperature.
The MIT and BWH researchers came up with the idea to use robotics to enable contactless monitoring of vital signs, to allow health care workers to minimize their exposure to potentially infectious patients. They decided to use existing computer vision technologies that can measure temperature, breathing rate, pulse, and blood oxygen saturation, and worked to make them mobile.
To achieve that, they used a robot known as Spot, which can walk on four legs, similarly to a dog. Health care workers can maneuver the robot to wherever patients are sitting, using a handheld controller. The researchers mounted four different cameras onto the robot — an infrared camera plus three monochrome cameras that filter different wavelengths of light.
The researchers developed algorithms that allow them to use the infrared camera to measure both elevated skin temperature and breathing rate. For body temperature, the camera measures skin temperature on the face, and the algorithm correlates that temperature with core body temperature. The algorithm also takes into account the ambient temperature and the distance between the camera and the patient, so that measurements can be taken from different distances, under different weather conditions, and still be accurate.
Measurements from the infrared camera can also be used to calculate the patient's breathing rate. As the patient breathes in and out, wearing a mask, their breath changes the temperature of the mask. Measuring this temperature change allows the researchers to calculate how rapidly the patient is breathing.
The three monochrome cameras each filter a different wavelength of light — 670, 810, and 880 nanometers. These wavelengths allow the researchers to measure the slight color changes that result when hemoglobin in blood cells binds to oxygen and flows through blood vessels. The researchers' algorithm uses these measurements to calculate both pulse rate and blood oxygen saturation.
"We didn't really develop new technology to do the measurements," Huang says. "What we did is integrate them together very specifically for the Covid application, to analyze different vital signs at the same time."

Continuous monitoring
In this study, the researchers performed the measurements on healthy volunteers, and they are now making plans to test their robotic approach in people who are showing symptoms of Covid-19, in a hospital emergency department.
While in the near term, the researchers plan to focus on triage applications, in the longer term, they envision that the robots could be deployed in patients' hospital rooms. This would allow the robots to continuously monitor patients and also allow doctors to check on them, via tablet, without having to enter the room. Both applications would require approval from the U.S. Food and Drug Administration.
The research was funded by the MIT Department of Mechanical Engineering and the Karl van Tassel (1925) Career Development Professorship.

Coronavirus: On patrol with Yas Mall's robot security guards

Source: https://www.thenational.ae/uae/health/coronavirus-on-patrol-with-yas-mall-s-robot-security-guards-1.1071076

Sep 02 – Robot security guards are on patrol at Abu Dhabi's largest mall to help keep shoppers safe during the Covid-19 pandemic.
Two robots equipped with surveillance and thermal cameras roam the floors of Yas Mall every day and night to report live to the operations room.
The sophisticated security team was drafted in to ensure "an extra eye" is cast over the sprawling venue when upholding health and safety measures have never been more important.
"If people are not wearing their masks, they are reported to the control room and are then reminded to put on their masks," said Yasser Al Marzooqi, head of retail at Aldar Properties, which manages Yas Mall.
The mall machines can also serve as mobile customer care agents.

"If people are lost or want to know more information, they can approach the robot, and since it is connected to the control room and has intercom as well, it could interact with customers," Mr Al Marzooqi said.
Yas Mall has already cut out direct interaction with customer care agents.
Instead, shoppers can find an iPad at the information desk and speak to an agent through video conference.
Mall maps and information screens have also been replaced.
"The idea was to limit the number of human guards," said Saeed Al Ali, head of security.
"During Covid-19, the robots can serve as thermal cameras to test the temperature of shoppers as they walk to conduct ongoing inspections.
"Also, if there are social gatherings [over the permissible number] that the security guards may have not noticed, the robots' live feed could alert the operations room."
The pair are fitted with seven cameras each, a face-recognition feature and intercom devices.
The movement of the robots can be remotely controlled from the operations room, or programmed to follow a route through the mall.

From Train Station to Hospital – Medical Drone Delivery

Source: https://i-hls.com/archives/103703

Sep 02 – Due to the impact of the global COVID-19 pandemic, the necessity to respond to changes in the logistics industry has become real and the use of drones may help realize automatic, contactless delivery. Japan has been accelerating the development of drone delivery technology for medical and other supplies. Tokyo could benefit greatly from this capability because there are many natural barriers, mainly the islands that are part of the city.
Japan Airlines has joined a consortium of transportation and technology specialists to test drone deliveries of medicines and food in Tokyo. The project will be particularly focused on developing efficient and safe drone operations in urban settings.

As part of the collaborative effort, KDDI will provide the drone operations platform for the project. Japan Airlines will offer safety management of flights, business development and feasibility assessment of pharmaceutical deliveries, while East Japan Railway will allow the tests to be performed from its stations. Weathernews will supply weather data for flights, and Terra Drone will offer air traffic control support.

To demonstrate the use of drones for pharmaceutical deliveries, **the project will transport medicines from Mediceo Corp.'s Tokyo warehouse to nearby St. Luke's International Hospital**. Food deliveries will be tested from restaurants to offices in close

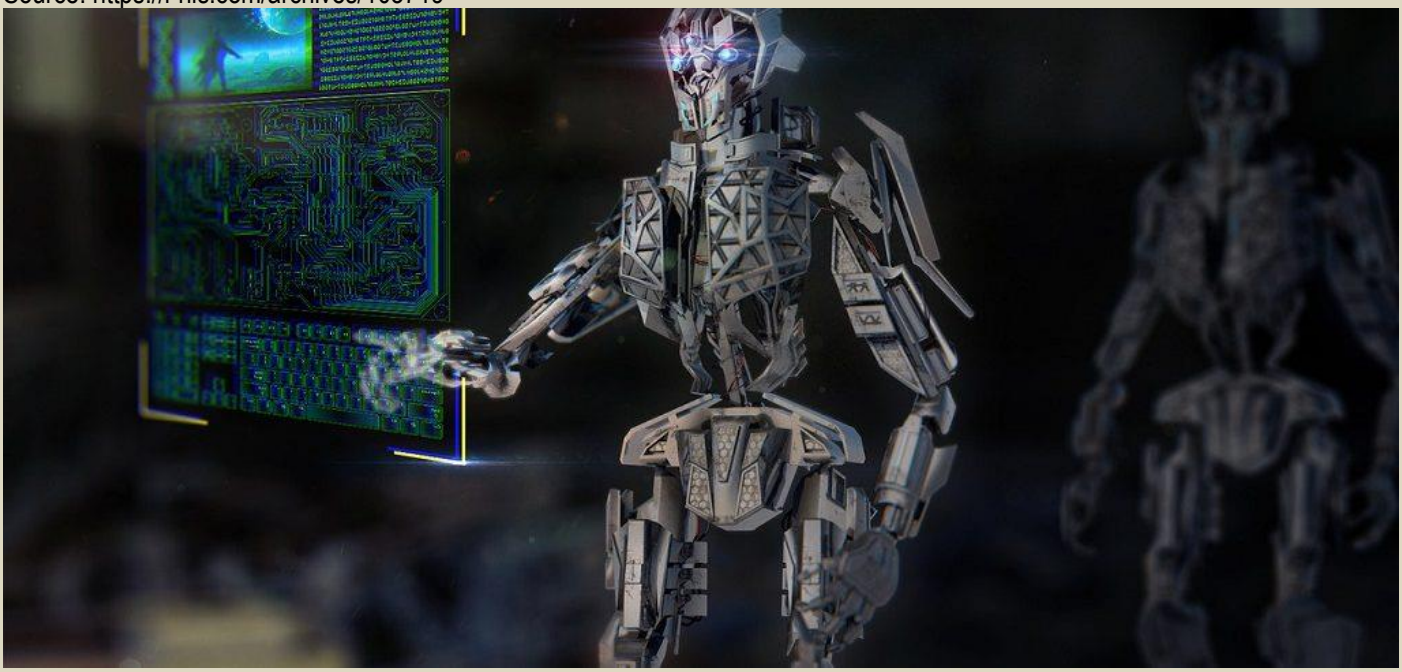
proximity to the East Japan Railway stations in Tokyo.

The project began in August and will end in March 2022, as reported by freightwaves.com.

EDITOR'S COMMENT: The St. Luke's Intern Hospital was the hospital that received more than 600 victims within 1 hour following the Tokyo subway sarin incident (1985).

Instead of Saying IDF Say Israel Robot Army: Far-Reaching Vision or Realistic Forecast?

Source: https://i-hls.com/archives/103719



Sep 03 – Leading Israeli defense industry officials portray the challenges of the future battlefield and conclude: The road leads to autonomy

At the AUS&R 2020 Unmanned Systems Broadcast Edition organized by iHLS for the ninth year, which will be online on September 7, Israel's most prominent defense industry officials gather to discuss transformations in the unmanned systems at the battlefield, competition by the civilian industries, and whether soldiers will still be required at the future battlefield.

In recent years, all the defense industries have been entering the "low altitude level" field – the airspace underneath the flight space of helicopters and fighter aircraft, where drones and unmanned aerial vehicles operate.

The question arises why do the large industries that usually make billion-dollar deals choose to join this field that offers cheap off-the-shelf products at this particular point in time. World giant companies, such as Boeing, have launched activities in this realm recently, in both capabilities' development and the acquisition of companies in the field.

Moshe Levy, IAI EVP and CEO of the Military Aircraft Division, asserts: "We tend to focus on the individual components that are essentially cheap and accessible, which makes them attractive. The role of the defense industries is to produce the integrative solution for customers."
Shuki Yehuda, EVP, CTO & R&D, at Elbit Systems Headquarters explains: "Our customers are looking for systemic solutions and capability, they are not interested in separate products. In each component there is very little money and the competition at the civilian market is harsh. The opportunity lies in the ability to provide systemic solutions for the world's defense industries.
Dr. Uzi Landau, Chairman of the Board, RAFAEL, said that first and foremost, the defense industries have started operating in this field because the State of Israel needs it. He added that the low and close-to-ground altitude field is going to grow considerably during the coming years. Dr. Landau: "The technology is developing dramatically. These systems will play a more and more massive role in all the Army's maneuvering systems." According to Landau, the next stage will be the autonomous vehicles revolution, which will completely change warfare.
According to American evaluations, within 20 years most of the ground warfare at the battlefield will be fully autonomous. Experts say that instead of soldiers – we will send an army of drones and unmanned systems to the battlefield. Shuki Yehuda from Elbit Systems explains that although this forecast is a bit optimistic however the question is certainly not if, but rather when. "It may take another decade, but it will arrive. Exactly as the autonomous vehicle."
Dr. Landau from RAFAEL explains: "The mass of information at the future battlefield is beyond the capabilities of the human brain. Real-time operational decisions will be made automatically. The systems will direct the various UAVs and drones almost without any human interference. Eventually, the human factor will have to make decisions based on all the data streamed by UAVs."
Regarding Israel's role in this game, Shuki Yehuda, Elbit's EVP, CTO & R&D, asserts that Israel needs this major capability. "While it doesn't have the vertical capability to manufacture fighter aircraft, Israel has a full vertical capability at the close-to-ground altitude. This capability is a major force multiplier at the battlefield, both against terrorist threats and powerful states threats. Israel has the opportunity to lead this revolution globally. With Israel's capabilities, it can be the global spearhead in this field."
One of the challenges faced by the defense industries is the development rate by the civilian industries, said Conference Chairman Col. (res.) Ofer Haruvi, formerly IAF's Head of UAV Department, who asserted that we live now in a world where development cycles are becoming shorter. The R&D and investment rates in the civilian sector are higher than those of the defense industries. Technologies are changing in extreme speed and the industries do not have some dozens of years for development, as we have seen in the past. The industries must accommodate themselves to this changing reality.
Moshe Levy, IAI VP, said the defense industries market is essentially a conservative market. For the first time, the basis becomes commercial products and all that is happening in the civilian sector. There is a tension between the civilian and military rates. This is also true regarding consumers and industries. The solution to this challenge is that we are approaching civilian companies, bringing agility to the defense establishment.
RAFAEL's Chairman said that these exactly were the reasons behind the recent acquisition of Aeronautics by RAFAEL. He added that the civilian industry has been conquering more and more fields that were dealt exclusively with by the military industry in the past. Currently, fields such as autonomous capabilities and communications are civilian spheres. This is true not only regarding the extent of investments in R&D but also in large scale sales and growing reliability. Our approach is "to ride the wave", namely to take from the civilian industry what it's got and integrate our own unique systems, securing and preparing it to war. The civilian industry does not do these things."

Troubling Drone Incursions Have Occurred Over Guam's THAAD Anti-Ballistic Missile Battery

Source: https://www.thedrive.com/the-war-zone/36085/troubling-drone-incursions-have-occurred-over-guams-thaad-anti-ballistic-missile-battery

94th Army Air and Missile Defens—Public Domain

Earlier this year, it came to *The War Zone*'s attention that a series of bizarre and highly concerning events took place in the late Winter of 2019 at Andersen Air Force Base on the Island of Guam. As we understand it, between late February and early March of last year, the massive installation experienced repeated incursions by

unmanned aircraft that appeared to be extremely interested in one highly sensitive area of the highly strategic base, the U.S. Army's Terminal High Altitude Area Defense (THAAD) battery that is tasked with defending the island from ballistic missile attacks.

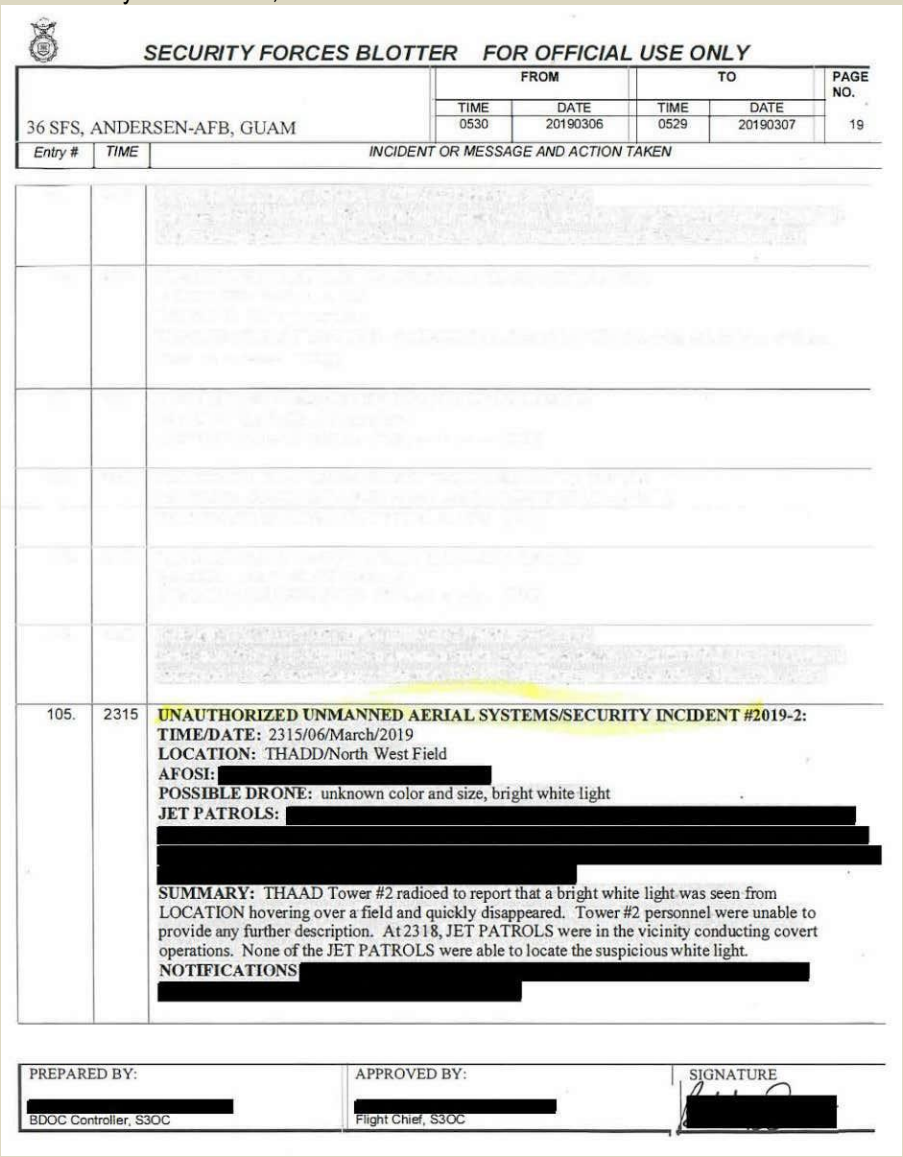
The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power PlantBy Tyler Rogoway and Joseph Trevithick Posted in The War Zone
The Strike On Saudi Oil Facilities Was Unprecedented And It Underscores Far Greater IssuesBy Tyler Rogoway Posted in The War Zone
America's Startling Short Range Air Defense Gap And How To Close It FastBy Tyler Rogoway Posted in The War Zone
Huge Pacific Exercise Centered On Guam Brings Allies Together Amid Growing China ThreatBy Jamie Hunter Posted in The War Zone
Another THAAD Anti-Ballistic Missile System Test Could Be ImminentBy Joseph Trevithick Posted in The War Zone

The incursions, which were said to have occurred in late March and early April 2019, had been observed by personnel manning guard towers that loom over the highly secure THAAD area situated towards the northern end of the air base, often referred to as "North West Field." Andersen itself takes up the northern and western reaches of the entire island.

Andersen Air Force Base takes up the entire northwestern end of Guam. The air base is located to the southwest, with the weapons storage areas and other critical sites being located to the northwest. The THAAD battery sits near where the abandoned runway-like feature exists on the northwestern portion of the base.

The intruding craft were described as "quadcopter-like" vehicles with bright spotlights that flew from over the water and then across the North West Base area at not much higher than treetop level, about 20 to 30 feet above the ground. On a number of nights, the craft would make multiple incursions in the very early morning hours. They would show up, disappear, then come back a few hours later.

The spotlight that shone down from the craft made it hard for personnel to make out a detailed description of the craft, although estimates range from being three to five feet in diameter largely based on the size of the spotlight. The craft would maneuver dynamically, appearing with the spotlight on, then disappearing, just to reappear moments later over to one side or another with the spotlight on, which was unsettling to those that witnessed it. Supposedly, there was a concerted effort to identify, track, and down the mysterious craft, but it doesn't seem that those efforts were successful based on our understanding of events.



SECURITY FORCES BLOTTER FOR OFFICIAL USE ONLY

	FROM		TO		PAGE NO.
36 SFS, ANDERSEN-AFB, GUAM	TIME 0530	DATE 20190306	TIME 0529	DATE 20190307	19

Entry #	TIME	INCIDENT OR MESSAGE AND ACTION TAKEN
105.	2315	**UNAUTHORIZED UNMANNED AERIAL SYSTEMS/SECURITY INCIDENT #2019-2:** **TIME/DATE:** 2315/06/March/2019 **LOCATION:** THADD/North West Field **AFOSI:** [redacted] **POSSIBLE DRONE:** unknown color and size, bright white light **JET PATROLS:** [redacted] **SUMMARY:** THAAD Tower #2 radioed to report that a bright white light was seen from LOCATION hovering over a field and quickly disappeared. Tower #2 personnel were unable to provide any further description. At 2318, JET PATROLS were in the vicinity conducting covert operations. None of the JET PATROLS were able to locate the suspicious white light. **NOTIFICATIONS** [redacted]

PREPARED BY:	APPROVED BY:	SIGNATURE
[redacted] BDOC Controller, S3OC	[redacted] Flight Chief, S3OC	[redacted]

This information was highly interesting if not downright alarming, but we had to find hard evidence that at least something similar did indeed happen during this timeframe.

We got just that straight from the U.S. Air Force. *The War Zone* was able to confirm that at least one of the incidents described above did occur through the Freedom of Information Act (FOIA), by which we obtained a copy of the relevant entry from the Air Force's 36th Security Forces Squadron's internal crime blotter. The is unit is part of the 36th Wing at Andersen Air Force Base.

The entry describes the "possible drone" as being of an "unknown color and size, [with a] bright white light." Army personnel at "THAAD Tower #2" had radioed in at "2315," or 11:15 PM – it's unclear if this was local time on Guam or Zulu Time, also known as Greenwich Mean Time – to report "a bright white light was seen from [their] LOCATION hovering over a field and quickly disappeared."

"Tower #2 personnel were unable to provide any further description," the blotter entry continues. "At 2318, JET PATROLS were in the vicinity conducting covert operations. None of the JET PATROLS were able to locate the suspicious white light."

The "JET PATROLS" that are referenced in the document are not aircraft, but are Jungle Enforcement Teams of the 36th Security Forces Squadron. The Air Force describes the teams as being "tasked with preventing security breaches, apprehending poachers, and securing the perimeter around the jungle." The team's personnel move silently through the jungle that permeates much of the base at night and have unique human tracking skills. You can read all about this specialized security force in this official media release.

Interestingly, the 36th Security Force Squadron's blotter lists this incident as "Unauthorized Unmanned Aerial Systems/Security Incident #2019-2," which implied that there was at least one other similarly classified drone incident at Andersen Air Force Base before this one by that point in the early 2019 calendar or fiscal year. Another FOIA request confirmed that there was a "2019-1" blotter entry, but the Air Force withheld information about that event citing privacy and law enforcement exemptions. Agencies typically withhold records for law enforcement reasons because of a potential risk of exposing sensitive tactics, techniques, or procedures, or because of an ongoing investigation. It is then doubly interesting that the March 2019 incident near the Army's THAAD battery at North West Field was not also subject to the exemptions.

U.S. Indo-Pacific Command (INDOPACOM) forwarded a separate FOIA request regarding this incident, any other similar occurrences around the same timeframe, to the U.S. Army. *The War Zone* is still awaiting a response to that request, as well as another one to the Guam Police Department. We inquired directly to the 36th Wing and INDOPACOM, but never got a response.

We found this information to be highly troubling for a number of reasons. The most important is that this craft was able to penetrate its way over an air defense system that is tasked with defending the highly strategic island from ballistic missile attacks. In other words, that THAAD battery is largely what stands in the way of a country like North Korea from holding the island at imminent risk. The system is even capable of shielding against a lower volume barrage from a peer state competitor, such as China.

Guam would be near the top of Beijing's targeting list during a conflict with the United States and its growing ballistic missile arsenal has been developed largely to deny the U.S. the utility of its regional bases during the open stages of a conflict. The island has already been outright threatened by Kim Jong Un's regime.

The thing is that destruction of enemy air defenses (DEAD) is not defined by a platform, it is a mission. Traditionally we associate the objective of destroying enemy air defenses with standoff cruise missile attacks and 'wild weasel' fighter jet operations, but DEAD can be carried out by a team of special operators with some well-placed explosives or via a barrage of naval gunfire. Even carefully deployed malware that targets the software that an air defense system and its mechanical component run on could potentially be destructive enough to be considered a DEAD method.

With that said, America's preeminent adversaries in the entire region would make taking out the THAAD battery on Guam a top priority during a conflict or even as part of a limited demonstration of force. Why barrage it with ballistic missiles or attempt a cruise missile launch from a forward-deployed submarine or even a clandestine commando raid when you can just fly a drone loaded with explosives into it? And no, you don't need some high-end drone system to do this as real-world events have highlighted many times over. Drug cartels are now whacking their enemies with off-the-shelf drone-borne improvised explosive devices and even U.S. allies are actually manufacturing hobby-like drones just for this purpose. Somewhat more sophisticated types can be launched from longer distances and can even home in on radar or other RF emissions sources, like THAAD's powerful AN/TPY-2 Radar and data-links, autonomously, beyond just striking a certain point on a map.

AN/TPY-2 radar used by THAAD.

Simply put, 'shooting the archer,' in this case an advanced anti-ballistic missile system that protects America's most strategic base in the entire region, via a relatively cheap drone is both an absurdly obvious and terrifyingly ironic tactic—the U.S. can shoot down ballistic missiles, but the critical systems used to do so remain extremely vulnerable to the lowliest of airborne threats—cheap drones.

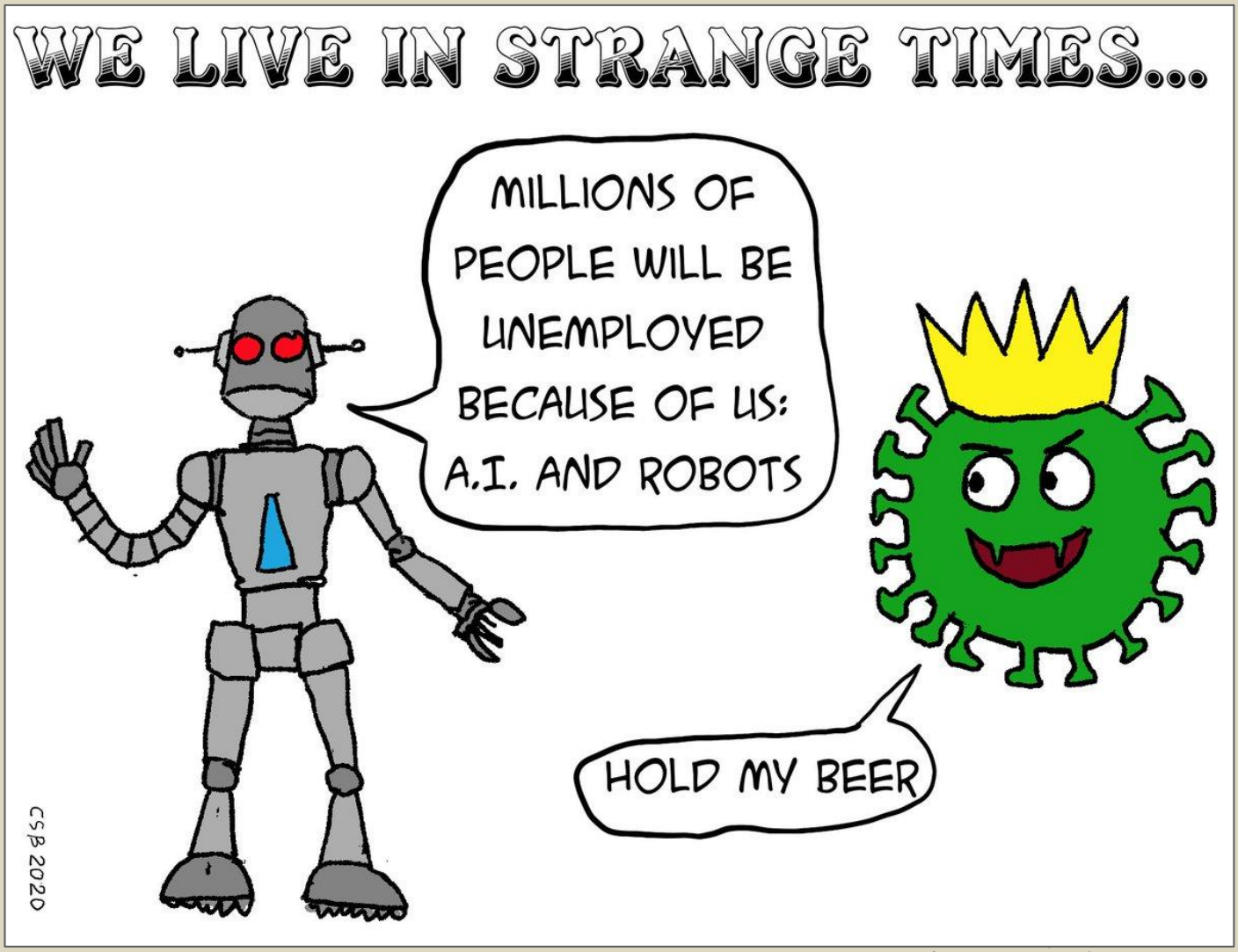
For those that follow our work, this is not news. The U.S. military was dangerously aloof when it came to the threat posed by low-end drones. We spent years highlighting this threat while seeing the U.S. military do very little to actually counter it, that is until ISIS was constantly dropping bomblets from drones or just flying explosive-laden drones into allied positions during the Battle of Mosul, Iraq.

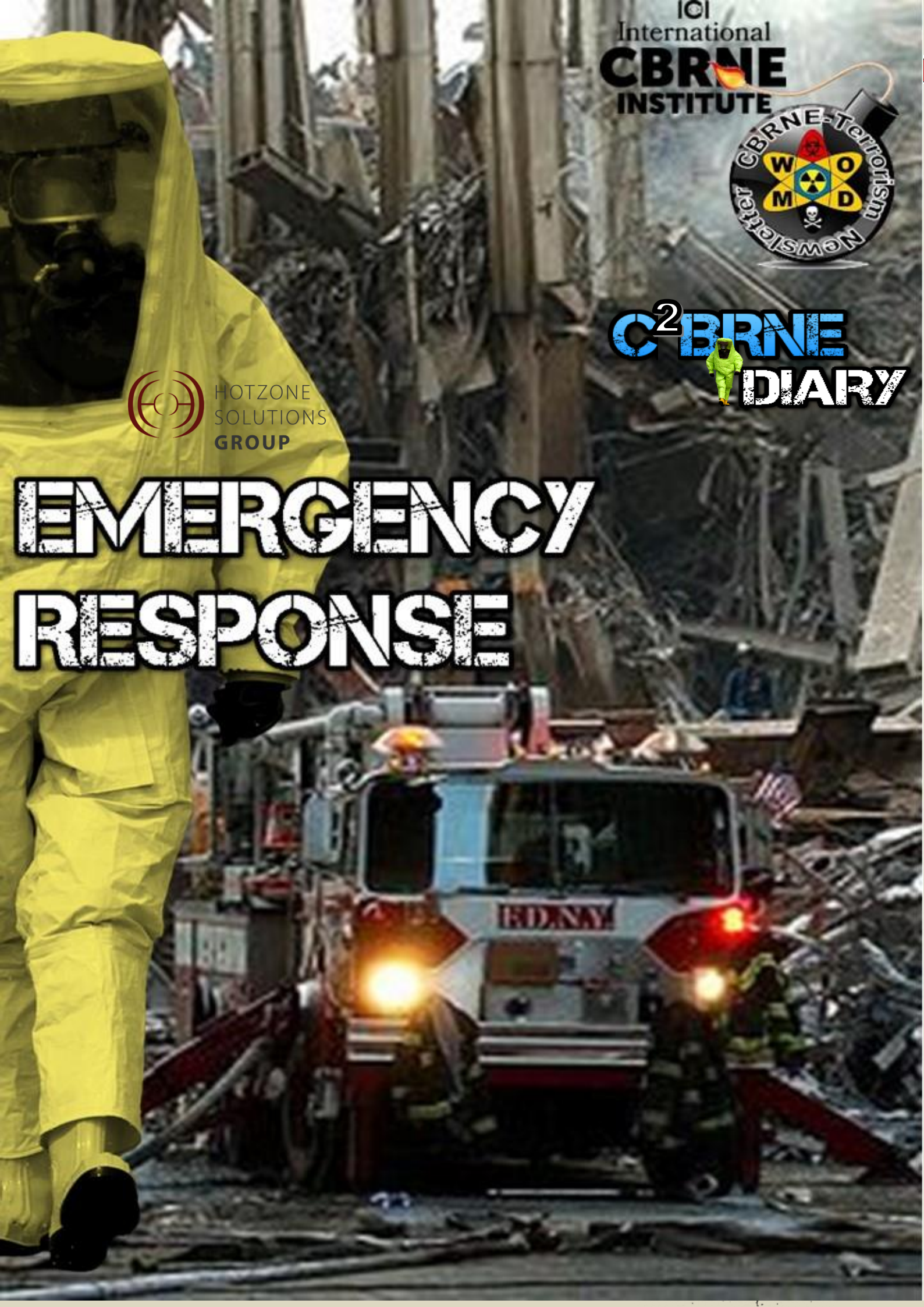
The threat has ballooned exactly as we predicted since then, with mass drone attacks on forward operating bases, attempted assassinations of ruling figures via drone, and even a successful drone assault right at the heart of Saudi oil production a year ago. In fact, the threat has gotten so bad that top U.S. commanders in the field are saying the constant presence of nefarious drones over or near their troops and equipment is what keeps them up at night.

In the meantime, it's abundantly clear that even America's most capable air defenses are vulnerable to the most meager of aerial capabilities—commercially available drones. If anything else, this is yet another, but possibly the biggest example of just how misplaced the U.S. military's priorities had become when it comes to investments in air defense over the last two decades or so. You can read how the Pentagon let its short-range air defense (SHORAD) capabilities wither on the vine to an appalling degree while concentrating on higher-profile, 'sexier,' and drastically more lucrative weapon systems in this past feature of ours. The Pentagon's appalling lack of vision regarding the emergence of this threat has made quickly ramping-up efforts to counter it that much more of a scramble, which is ongoing now. Still, America's potential enemies are already a step ahead, working on swarming low-end drone concepts that will overwhelm most countermeasures currently in the works.

So what is happening here? How does this all play into a rash of other troubling drone sightings, including highly similar ones that have occurred over American nuclear facilities and in other highly restricted airspace, as well as the ongoing buzz about unidentified aerial phenomena (UAP)? We will tie years worth of reporting on all these issues and others together very soon in a capstone piece.

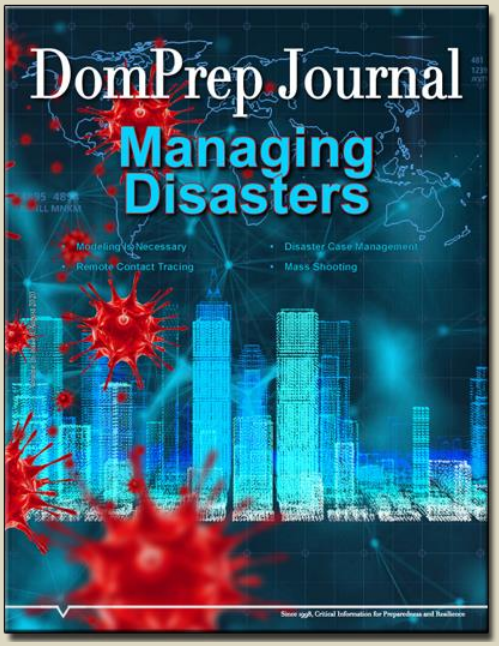
In the meantime, the events on Guam in 2019 serve as maybe the most outstanding reminder of how the Pentagon's fixation on high-end threats, and the huge gold-plated weapons programs that are put into play to counter them, have left even those very capabilities remarkably vulnerable to far less advanced attacks.




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

Domestic Preparedness Journal

August 2020, DomPrep Journal
Source: https://www.domesticpreparedness.com/journals/august-2020/



Featured in This Issue

Covid-19 offers opportunity for countries around the world to prepare for bio-terrorism threats

Source: https://scroll.in/article/971274/covid-19-offers-opportunity-for-countries-around-the-world-to-prepare-for-bio-terrorism-threats

Aug 26 – As the economic and health risks of the Covid-19 pandemic are predicted to persist into next year, there are growing reservations about society returning to normal.
The impacts of Covid-19, like the 2008 financial crisis and September 11, 2001, attacks before, are changing global consciousness and reopening uncertainties about security, privacy and public health.
Unfortunately, like 9/11 and the 2001 anthrax attacks, the current Covid-19 pandemic reveals systemic infrastructural and security deficiencies that rendered countries like the United States powerless.
This could have been avoided with better preparedness. However, preparedness requires maximum co-operation and transparency between government, researchers and industry.
As countries experience the ongoing economic and public health shocks caused by Covid-19, rogue actors seeking to take advantage of the pandemic may use bioweapons to similar effect.

Biosecurity threats are global

Like the current pandemic, any biosecurity threat or epidemic could easily become a global concern. Pathogens do not recognise borders and will spread indiscriminately, ultimately disproportionately affecting poorer nations.
Globalisation – which is being analysed as a contributor to the spread of Covid-19 – could also help thwart the spread of man-made or naturally occurring diseases, provided multilateral co-operation remains intact.
The response has to be global because pandemics and terror attacks have persisting and grave effects, not tied specifically to a single state and its economy.
Governments must take a proactive stance against the growth and development of deadly pathogens (engineered or naturally occurring), which might require an overhaul of the socioeconomic and political relationships that govern health and our shared environments.

Developing a collective response

The most crucial response is intergovernmental collaboration and compliance with medical experts. This would involve the sharing of information and effective mitigation strategies against bioterrorism.

The remarkable and unprecedented global unity today is demonstrated by scientists freely sharing information related to Covid-19 to speed up the development of a vaccine.

Governments and their collaborators must also stop the spread of disinformation to quell the panic and alleviate the public's fears.

This includes maintaining public trust in experts which must be differentiated from popular and political opinions that have led to chemical poisoning.

This has also been exacerbated with ongoing distrust for World Health Organization officials as false claims and pandering to China has led to failures in the initial response to Covid-19 including indecision within the scientific community.

Terrorist organisations will undoubtedly use the spread of bioweapons to create civil turmoil and instability, reinvigorating or inciting national contentions such as scarcity, ethnic tension or religious infighting. This applies to countries already destabilised by entrenched conflicts, which can rapidly metastasise through competition and inequality already present in developing countries.

Overcoming pandemics and terrorism will inevitably rely on national infrastructure such as employing the military, which the Canadian government has done to supplement medical resources. Deploying a nation's armed forces has the potential to apply the vast resources, equipment and labour that an organised and skilled military maintains.

Applying biotech

Countries like Taiwan and Singapore managed pandemic by implementing protocols that served to protect their citizens. These included analytic technologies to screen and isolate persons suspected of or confirmed to be infected with Covid-19.

In South Korea, over 20,000 people were tested daily to track and treat cases. Medical supplies were stockpiled and temporary hospital units were established to prevent scarcity and minimise black-marketeering.

However, medical equipment cannot be kept indefinitely and replenishment will likely require unconventional methods to fulfil the demand. Canadian universities have helped address the scarcities of medical equipment by employing 3D printers to produce masks and other supplies.

The Canadian government is also investing in novel detection and management technologies, which could be re-purposed to detect bioweapons. This also includes vaccine and antiviral development that can proactively work against future disease outbreaks.

The Canadian government has also increased funding for coronavirus-related projects.

Management strategies

Preventing the bioengineering, emergence, release and spread of pathogens will require aggressive strategies.

These include implementing regulations against the mistreatment and harvesting of wild and domestic animals to prevent their mixing and the unintentional mixing of viruses and infectious diseases. Managing land reclamation and protecting habitats can prevent biodiversity loss and reduce human contact with pathogenic viruses.

Other technologies in the fight against bioterrorism or pandemics include heightened surveillance and tracking in the form of smartphones and drones. Deployable 3D isolation units repurposed as mobile laboratories could also quickly respond to bioweapons threat.

Public co-operation

To guarantee safety, the public has to be willingly compliant with government policies. In Canada, closing the national border and enacting quarantine Laws mitigated the spread of Covid-19, but the public's co-operation was essential to the public good.

Recommendations from health-care professionals and epidemiologists must be implemented at every stage and directed by governments.

The consequences of neglecting to act expeditiously are apparent in the United States, which has been marred by bureaucratic red tape, equipment scarcity and vacillating in leadership responses.

Lessons from previous pandemics can prepare us for both future inevitable global outbreaks and possible bioterrorist attacks.

Trushar R Patel *is an Assistant Professor and Canada Research Chair at the Department of Chemistry and Biochemistry at the University of Lethbridge.*

Michael Hilary D'Souza *is a Masters Student of Biomolecular Interactions and Biophysical Modelling of RNA viruses at the same institution.*

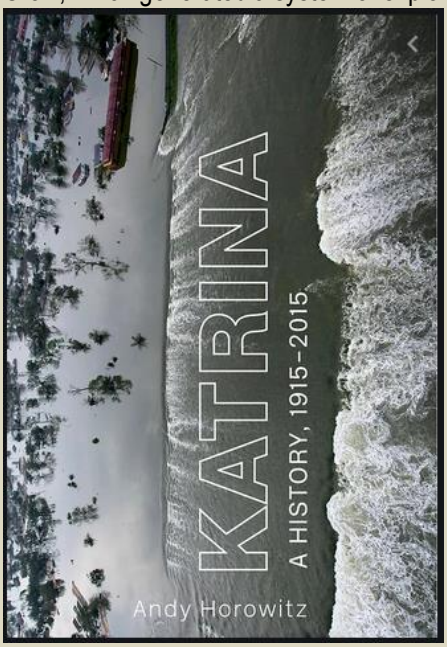
Why Hurricane Katrina Was Not a Natural Disaster

By Nicholas Lemann

Source: https://www.newyorker.com/books/under-review/why-hurricane-katrina-was-not-a-natural-disaster

Aug 26 – When we came home to New Orleans for the first time after Hurricane Katrina, over Thanksgiving weekend of 2005, my then three-year-old son, looking out the window on the drive in from the airport, said, "You told me we were going to New Orleans, but now we're in Iraq." This was three months after the storm hit. The floodwaters had receded, the Superdome had emptied, the national press had left, and we weren't anywhere near the city's most famous devastated neighborhood, the Lower Ninth Ward—but still what you saw was a landscape of abandoned buildings, moldy refrigerators set out on sidewalks, downed trees and electrical wires, and a thick impasto of mud covering everything. Even now, fifteen years after Katrina, New Orleans has not fully recovered, in population and otherwise.

By the standards of one's middle-school geography class, New Orleans ought to be one of America's most prosperous cities, instead of one of its poorest. It is the natural port for the vast interior of the country, from the Rockies to the Appalachians. In its immediate vicinity are many natural resources: rich soil for growing rice and sugarcane, and plenty of cotton, sulfur, seafood, and, beginning in the early twentieth century, oil. Then there are the city's celebrated charms—the food, the music, the generally soft, seductive atmosphere. But New Orleans peaked, relative to other American cities, back in 1840, and has been losing ground ever since. It looks today like an especially severe example of the resource curse, because its economy of extraction was based originally on slavery—antebellum New Orleans was the country's leading marketplace for the buying and selling of humans—and then on Jim Crow, which generated a system of exploitation that pervades every local institution, as well as a deep, evidently permanent mistrust between the races.



And then there is New Orleans's relationship to nature. Half of the city is below sea level; only a relatively small portion, the section that was originally settled, is habitable by traditional definitions. The city is surrounded by an endless borderland that shifts between river, marsh, swamp, and ocean. Katrina was only one of a long series of hurricanes that have struck near the mouth of the Mississippi. In New Orleans, civic monumentalism was always bound up in the racial order—consider the Confederate statues that the city built, in the early twentieth century, and only recently removed—but not every expression of it was explicitly racial. Another important project, from the same period, was the creation of an elaborate system of drains and pumps, supervised by an engineer named A. Baldwin Wood, which was supposed to make the entire area within the great crescent bend of the river, all the way to the shore of Lake Pontchartrain, permanently flood-proof. As Andy Horowitz, a young historian at Tulane University, writes in "Katrina," his new history of the event, it was twentieth-century New Orleans—the part built after the drainage system was constructed—that flooded in the late summer of 2005.

If there's a standard Katrina narrative among non-New Orleanians, it runs something like this: the storm was as devastating as it was because of real-time official incompetence, especially by the George W. Bush Administration. Its main victims were poor African-Americans, particularly in the Lower Ninth Ward, and today, thanks to the indomitable spirit of the community, the city has vibrantly come back to life. By stretching the frame backward by a hundred years, and forward by ten, Horowitz presents a strikingly different story, and a more depressing one. The main thrust of Horowitz's account is to make us understand Katrina—the civic calamity, not the storm itself—as a consequence of decades of bad decisions by humans, not an unanticipated caprice of nature. "Usually, we imagine disasters as exceptions," he writes. "We describe them as external attacks, ahistorical acts of God, blows from without. That is why most accounts of Katrina begin when the levees broke and conclude not long after. But these stories have a denuded sense of what happened, why, or what might have prevented the catastrophe. Somebody had to build the levees before they could break." He leaves readers with a strong sense that it's only a matter of time before there is a similar disaster in New Orleans, and that, in whatever lull there is between now and then, things aren't great.

Horowitz's story begins with oil, which seemed like a bonanza when it was discovered in Louisiana, in 1901, but which set in motion two long-running problems. Almost immediately, the state government realized it could finance itself by taxing the oil companies. (As Horowitz points out, in those days, "states' rights" may have been primarily code for preserving racial segregation, but it also meant considering distant offshore rigs to be on Louisiana property.) It was during the era when oil revenues were flowing freely that the state's grandest public buildings—the vast Charity Hospital, in New Orleans, and the state capitol building and the campus of Louisiana State University, in Baton Rouge—were built.

In 1950, a landmark Supreme Court decision, which severely restricted the zone in which the state could tax offshore oil rigs, ended that party. The state has never successfully developed another way of paying for a competent government. The oil companies also ravaged southern Louisiana's previously trackless freshwater marshes, by drilling and by building access canals that allowed saltwater from the Gulf of Mexico to flow in. The result was a relentless, yearly loss of land—or, to represent more accurately what it looks like, "land"—and greater vulnerability to hurricanes.

A combination of civic boosterism and excessive faith in engineered water-control systems led New Orleans to keep reclaiming swampland for housing, building canal systems for commercial ship traffic, and dredging spillways that were supposed to draw floodwater away from the city when the need arose. These systems all failed during Katrina. A severe hurricane in 1915, Horowitz reminds us, caused relatively little damage and so enhanced New Orleans's hubris. But in 1965 Hurricane Betsy—which I lived through as a boy, huddled next to my parents, as far as we could get from any windows that might blow in—was a demonstration of the folly of a half century's worth of misguided building. The storm caused massive, sustained flooding. Two hundred and sixty thousand people had to leave their homes. Betsy coincided with the high-water mark of Lyndon Johnson's Great Society; Johnson immediately came to New Orleans to show his concern, and Louisiana's leading politicians, then all still Democrats, demanded, and mostly got, generous federal emergency aid. But it's always easier to address a pressing crisis than to prevent the next one, so the pattern of continued development without adequate flood protection continued. An ambitious long-term hurricane-protection plan passed by Congress and signed into law by Johnson was never completed.

Katrina flooded out many white people as well as Black people, and, within Black New Orleans, many working-class and middle-class people as well as poor people. That was because the largest wiped-out neighborhoods—Lakeview, Gentilly, New Orleans East—were places where New Orleanians of both races had moved to ascend the ladder by a step or two, often enabled by government-backed lending programs that didn't sufficiently appreciate the risk of flooding. New Orleans's extensive public-housing projects, all Black and all poor, were in older parts of the city, and mostly didn't flood. But the dynamic of recovery was all about race. New Orleans is a Black-majority city. The mayor, Ray Nagin, a Black businessman elected with more white than Black votes in 2002, appointed an urban-planning committee, headed by a white real-estate developer, to guide the city's recovery. (Nagin was later convicted of taking bribes from city contractors.) The committee soon unveiled a plan that entailed not rebuilding some of the Black neighborhoods that had flooded. Many residents were outraged; on the Martin Luther King, Jr., holiday in 2006, Nagin gave a speech disowning the plan and committing himself to rebuilding "a chocolate New Orleans." He was reëlected a few months later, this time with more Black than white votes, and the idea of shrinking the residential footprint of New Orleans to something closer to what it had been a century earlier became disreputable. Instead, the idea was that every homeowner should get prompt and generous help in order to return and rebuild.

But that didn't happen, either. A series of measures that would have provided enough relief to rebuild New Orleans completely either wasn't enacted or proceeded at the leisurely pace that is customary in Louisiana. New Orleans has a large racial gap in resources—the Black poverty rate is triple the white poverty rate—so whites were able to move back more quickly and with less hardship. For a decade after Katrina, New Orleans was a whiter city than it had been before. That fed into a venerable tradition, in Black New Orleans, of suspicion of what white New Orleans might be up to. Back in 1927, when the Mississippi River flooded disastrously (because of heavy spring rains, not a hurricane), New Orleans's white city fathers ordered the dynamiting of the levee below the city, in the hope of preventing flooding. Since then, the idea that breaches in the flood walls were not accidental has been common in Black New Orleans—and, in fact, Horowitz unearths some evidence that official decisions may have contributed to one of the major breaches, in the Lower Ninth Ward, during Hurricane Betsy. After Katrina, the spectacle of a Black refugee population in the Superdome, along with the short-lived plan from Mayor Nagin's committee to wipe out some Black neighborhoods, revived these sentiments. And, on the white side of town, lurid stories about Black criminality, that ancient fear of white Southerners, circulated widely. So did wishful conversations about the possibility of New Orleans becoming a white-majority city again, as it hadn't been since the nineteen-seventies.

Hurricane Betsy hit New Orleans during what was, it's now clear, the final period of the New Deal political order. In the South, people still looked to government to solve big problems, as long as racism wasn't included on the list of big problems, and the Democrats, the party of government, still held power. By the time Katrina hit, the Democrats had moved left on race and right on political economy, and the Republicans were in power nationally. Three major public institutions, all serving mainly Black clienteles, withstood the storm physically but not politically: Charity Hospital, the large-scale housing projects, and the unionized, government-managed public-school system. All were replaced by smaller, more privatized, more gentrified alternatives. Instead of Charity, New Orleans has the new, lower-capacity University Medical Center; instead of the projects, lower-density, more middle-class housing developments; instead of the old public schools, the country's most extensive charter-school system, with mainly Black students and mainly white teachers. One could see these changes as evidence of civic rebirth, but it would be fairer to say that they represent a reordering of priorities, an embrace of a different political vision, and a racial recalibration. As Horowitz mordantly puts it, "What came to be known as New Orleans's 'recovery' involved . . . a decision to evict

people from their homes in the face of a homelessness crisis, a decision to close the hospital in the midst of an epidemic of suicide, and a decision to help children by firing their parents."

New Orleans is a little corner of some other culture grafted onto the periphery of the United States. Horowitz points out that the state of Louisiana, in the last census before Katrina, had the lowest level of population mobility in the United States. Almost ninety per cent of Black New Orleanians had been born there, as compared with sixty per cent of Black Atlantans. The standard American idea of leaving an impoverished, provincial place to find opportunity elsewhere just doesn't play in New Orleans: people who choose to make their lives elsewhere are the subject of hushed, sorrowful conversations, as if they had been banished because of some kind of disgrace. Just about everybody had to leave New Orleans for at least a few weeks after Katrina. If New Orleanians had been cost-benefit-calculating androids, a great many of them would have realized that it made sense to build a new life elsewhere. But the preference to return was strong, for both whites and Blacks and in all income categories. Did people imagine that they were coming back to a different New Orleans, or did they understand the essential bargain? Dense family and neighborhood ties, and a rich local culture unattainable elsewhere in the United States, in exchange for a society that is essentially premodern in what it can offer many of its citizens?

It is not possible to make New Orleans completely hurricane- and flood-proof, but if one wanted to try there would be two over-all approaches. One would be to depopulate the city and deindustrialize southern Louisiana, creating a small-footprint eco-paradise—the New Orleans that nature seems to want. That violates the strong preferences of the residents and a poor area's hunger for money. The other option would be to invest in a protective infrastructure so mighty that, at least plausibly, New Orleans could survive anything. After Katrina, as after Betsy, such plans were drawn up, but nobody wanted to pay for them. New Orleans had to settle for levee enhancements that fell far short of providing invulnerability to a Category 5 hurricane, and wound up returning to something not too different from its pre-Katrina state. The city is an irresistibly alluring place that does far better by its white citizens than its Black ones. Life is sweet when it isn't tragic. Lodged somewhere in everyone's consciousness is the knowledge that what happened in 2005 is going to happen again.

Nicholas Lemann *is a staff writer at The New Yorker and a professor at Columbia University's Graduate School of Journalism. His most recent book is "Transaction Man: The Rise of the Deal and the Decline of the American Dream."*

From 9/11 to COVID-19: Old habits, lessons learned and work to be done

By Jeff Schlegelmilch and Ellen P. Carlin

Source: https://thehill.com/opinion/healthcare/515461-from-9-11-to-covid-19-old-habits-lessons-learned-and-work-to-be-done

Sep 19 – Nineteen years ago, the challenges of the new millennium began to show themselves in the most unspeakable of terms. The shock of a terrorist attack on U.S. soil potent enough to bring down New York's iconic World Trade towers, leave parts of the Pentagon in the rubble, and down a jetliner in the fields of Pennsylvania continues to ripple through our health, our security culture, and our now-ingrained, if flawed, approach to disasters.

The terrorists who perpetrated the Sept. 11, 2001 attacks took the lives of 2,977 people that day, with many more later succumbing to the enduring effects of toxic exposures at ground zero. That same month, a bioterrorist placed anthrax spores into the U.S. mail system, an act that took five more lives and further paralyzed a nation, and gave outsized attention to the threat of bioterrorism.

We were not ready for either of these events. In a hasty response, the American government embarked on its largest re-organization since World War II, became embroiled in two major wars, and redefined the use of covert action. With a defense and security doctrine focused heavily on adversaries bent on kinetic impacts within the homeland, the focus of homeland readiness became weighted towards mass casualty events and preparing for what seemed like the inevitable use of weapons of mass destruction on our people. The newly-minted "public health preparedness" community became focused on preparing for anthrax or a smallpox attack and, to a lesser extent, a host of other potentially weaponized biological agents.

Federal biodefense programs pumped billions into developing pipelines and national stockpiles of pharmaceutical countermeasures in anticipation of a bioterrorist attack. New paradigms of state and local response systems were built from existing public health and emergency management systems to support this.

All of a sudden, preparedness became a national effort that became flush with resources, mandates and expectations that normally take years — even generations — to establish. It was messy, and perhaps too focused on adversarial threats rather than natural hazards, but that was our most recent experience, and the threats seemed palpable, imminent and existential.

Around 2005, the emergence of virulent strains of avian flu in Asia and the readiness failures laid bare by Hurricane Katrina resulted in still new paradigms. Whole-of-community

responses were going to be required. Federal leadership and governance to coordinate complicated public health preparedness needed to evolve.
Laws like the Post-Katrina Emergency Management Reform Act and the Pandemic and All-Hazards Preparedness Act were signature legislative efforts to tackle the most recent failures. These laws further clarified agency responsibilities and expectations and created new entities such as the Assistant Secretary for Preparedness and Response at the Department of Health and Human Services.
But none of these laws sufficiently addressed the drivers of natural hazards and pandemics — climate change, injudicious land use, and structural inequalities embedded in our society. Meanwhile, the spending of the early post-9/11 years started to wane, and agencies and planners began to settle into a more balanced status quo — with mixed success in the inevitable disasters that have followed.
We fell into patterns of funding disaster preparedness without understanding whether it was having any impact. We fine-tuned legislation instead of creating strategic resources like a public health emergency fund, and a requirement to integrate climate change projections into preparedness. And we increasingly relied on easily undone executive orders and one-off emergency supplemental funding bills for disasters.
Today, COVID-19 is re-exposing old vulnerabilities and revealing entirely new ones. Some of what was put in place since 9/11 did help with the pandemic response. Nearly two decades of public health planning has helped engage the private sector and provide blueprints for communities to respond to pandemics. But mostly we were caught flat-footed.
We opted not to invest in high-risk, high reward initiatives like on-demand vaccine and treatment technologies. We ignored warning signs that diseases like this were becoming more likely to emerge in the first place. Like 9/11, Amerithrax, and Katrina, COVID-19 is yet another tragic inflection point in the arc of history for disaster management.
The failure to prevent the attacks of 9/11 has been called a failure of imagination. Perhaps it is because we typically react to the last disaster without imagining the next one. More than a signature 9/11 failure, it is a recurring theme in our approach to disasters. Now, the future is here — we need to learn from past mistakes, to heed the warnings of experts, and to act based on future threats and our growing vulnerabilities to them.
Perhaps our imperative on this anniversary of 9/11, as we endure another national catastrophe, is to ensure that the nearly 200,000 Americans who collectively lost their lives to 9/11 and COVID-19, and the many more affected by these and other disasters, are remembered in the actions we take to prevent future tragedies.

Jeff Schlegelmilch *is director of the National Center for Disaster Preparedness at Columbia University's Earth Institute, and the author of the book "Rethinking Readiness: A Brief Guide to Twenty-First-Century Megadisasters."*
Ellen P. Carlin *is an assistant research professor at the Georgetown University Center for Global Health Science and Security and director of Georgetown's Global Infectious Disease graduate program.*

Risk Assessment and Mitigation Lessons Learned from the Charlie Hebdo Attack

By David Pounder

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/risk-assessment-and-mitigation-lessons-learned-from-the-charlie-hebdo-attack/

Sep 10 – Last week, the French satirical magazine *Charlie Hebdo* republished cartoons of the Prophet Muhammad. This action was in advance of the trial of 14 people who were accused of supporting two Islamist attackers to carry out an attack on *Charlie Hebdo* on Jan. 7, 2015. This support included providing weapons and logistical support, key elements in many complex coordinated terrorist attacks that occurred in Europe in the mid-2010s. It was the publication of the cartoons in the first place that was a contributing factor in the attack. Reviewing these incidents can help provide valuable lessons learned, which can help organizations plan and prepare for a potential future attack.

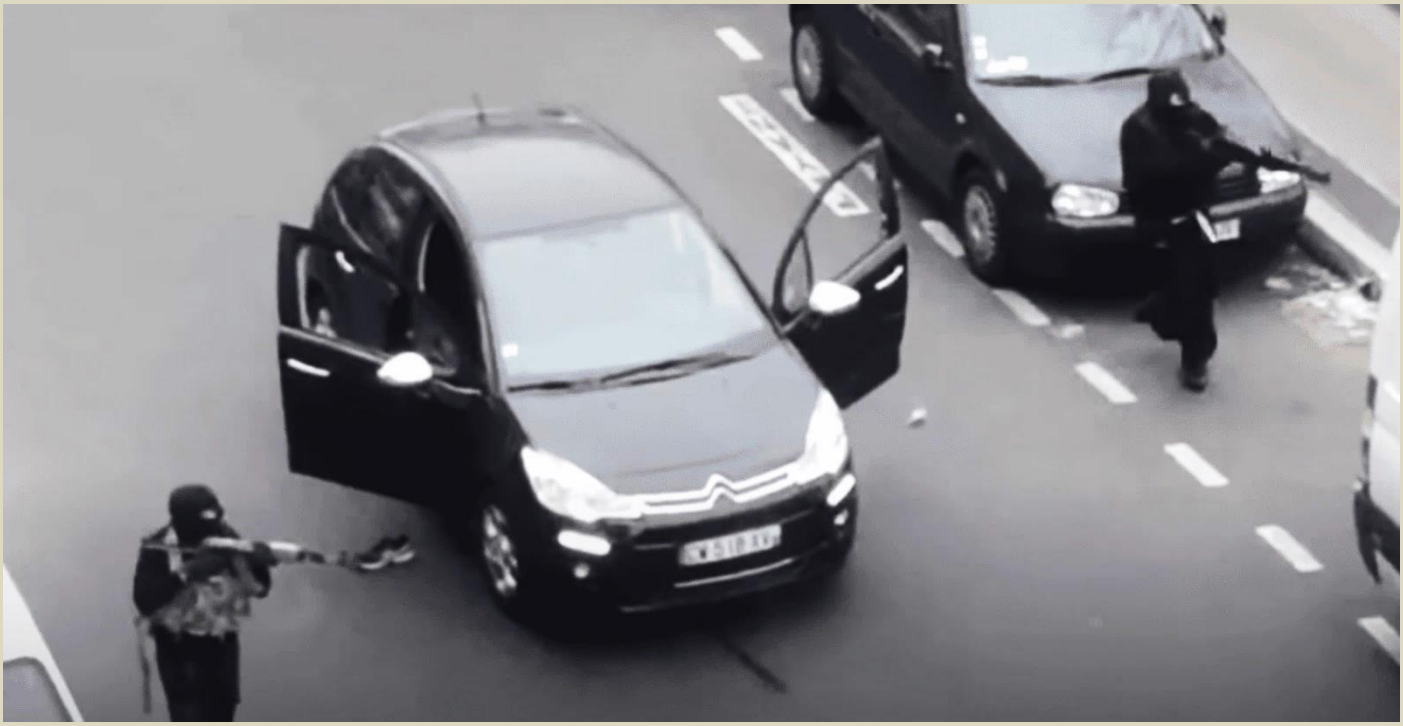
Background

Charlie Hebdo is a French satirical weekly newspaper that pokes fun at a wide variety of topics and institutions. As such, it has a history of controversy, especially for targeting religious groups, and particularly Islam. While there is nothing that specifically says depictions of Muhammad are forbidden in the Koran, it is widely believed by most Muslims to be an absolute prohibition. For many, depictions (pictures or statues) of Muhammad, or any of the other prophets of Islam, should not be pictured in any way as they could be thought to encourage the worship of idols.

- The cartoons in question, one which depicts Muhammad wearing a bomb-shaped turban, were first published in 2005 by the Danish newspaper *Jyllands-Posten*. It

was then reprinted by *Charlie Hebdo*, which, as expected, led to outrage and death threats against the editorial team.

- In 2006, Islamic organizations under French hate speech laws unsuccessfully sued over the newspaper's re-publication of the cartoons of Muhammad.
- The cover of a 2011 issue, retitled *Charia Hebdo* (French for Sharia Weekly), featured a cartoon of Muhammad.
- The newspaper's office was fire-bombed and its website was hacked.
- In 2012, the newspaper published a series of satirical cartoons of Muhammad, including nude caricatures which came days after a series of violent attacks on U.S. embassies in the Middle East, which themselves were purportedly in response to the anti-Islamic film *Innocence of Muslims*. This prompted the French government to close embassies, consulates, cultural centers, and international schools in about 20 Muslim countries. Riot police surrounded the newspaper's offices to protect it against possible attacks.
- In 2013, cartoonist Stéphane "Charb" Charbonnier, who had become the director of publication for *Charlie Hebdo* in 2009, stated, "We have to carry on until Islam has been rendered as banal as Catholicism." Al-Qaeda in turn added him to their most wanted list. In addition, he had strongly defended the cartoons as symbolic of freedom of speech. "I don't blame Muslims for not laughing at our drawings," he told the Associated Press in 2012. "I live under French law. I don't live under Koranic law."



Timeline of the Attack

The above background help set the stage for the attack described below. Note, the account captured is derived from multiple open source reports and news articles including the BBC and NPR.

07 January 2015.

- At 11:30 local time, brothers Said and Cherif Kouachi drove their car up to the *Charlie Hebdo* building and stormed the offices. They wore masks, dressed in black and were armed with AK-47 assault rifles. However, they initially went into the wrong address, before realizing the *Charlie Hebdo* offices were on the second floor a couple doors away. This in and of itself is an indicator that the threat actors did not do a high degree of surveillance in support of their plan. Most likely they did online research which can be effective in early planning phases, but physical surveillance and eyes on the target is generally needed to ensure the plan can be executed as intended.
    - Once inside the office building, the men asked the maintenance staff in the reception area where the magazine's offices were, before shooting and killing a caretaker.
    - On the second floor, the men then grabbed one of the magazine's cartoonists and forced her to enter the code for the keypad entry to the newsroom on the second floor – where a weekly editorial meeting was taking place. The keypad securing the second floor is an effective security

measure for external access, but it is encouraged that this is reinforced with another access level inside.
    - Once in the *Charlie Hebdo* offices, the men shot and killed the editor's police bodyguard before asking for editor Stephane "Charb" Charbonnier and four other cartoonists by name. Once identified, the attackers killed them, along with three other editorial staff and a guest who were attending a meeting.
    - Witnesses said they had heard the gunmen shouting "We have avenged the Prophet Muhammad" and "God is Great" in Arabic while calling out the names of the journalists.
- Police responded to the offices as the gunmen were leaving the building.
    - The gunmen left using the same car they arrived in.
    - A police car arrived and blocked their initial escape route. The gunmen opened fire on the police car and fled via an alternate route.
    - During the escape, video footage captured the attackers getting out of their vehicle and shooting a police officer who was on a nearby sidewalk. One of the attackers then walked up to the injured policeman and killed him at close range. It is not clear if the police officer had recognized the car and attempted to engage or if he was on a regular patrol.
    - The attackers then abandoned the car, hijacked another car and disappeared. In the abandoned car, police found Molotov cocktails and two jihadist flags, which could be an indication that the Molotov cocktails could have been used as a secondary attack method or if the security situation was tougher than anticipated.
    - This is the first indication of a well thought out escape plan, which is the last phase of the Hostile Events Attack Cycle. Not only did they leave the scene but they had an alternate route in mind, and an extensive support network in place to hide them. Related to escapes in general, some extremist, or active shooter attacks, do not plan on an escape. Some attackers plan on taking their own life, or plan to fight to the death. In the most recent U.S. Secret Service report, "Mass Attacks in Public Spaces – 2019", **15 percent of attacks ended with police arriving on the scene and killing the attacker, and approximately 20 percent resulted in suicide either at the scene or after leaving the scene. Almost half of the attacks resulted in the attackers being able to leave the scene on their own.**
- Paris had been then put on alert and a major security operation was launched with an additional 500 police deployed around the capital.

08 January 2015.

- At approximately 08:45 local time, as police continued their search for the *Hebdo* attackers, a lone gunman killed a policewoman and injured another man in a southern Paris suburb. The attacker was armed with a machine gun and a pistol. Initially this was thought to be a separate incident, but the police later confirmed they were connected.
- At 10:30 local time, the *Hebdo* attackers robbed a gas station northeast of Paris, taking food and gas. According to the gas station manager, the two men also had rocket-propelled grenade launchers in addition to their assault weapons. They had been driving the same car they hijacked after their initial attack, which is another indicator of a support network that would allow them to conceal their car after police had mobilized to search for them.
- There would be reports of sightings around the suburbs and a police chase throughout the day on 08 January but no additional threat-based activity. In the meantime, police were able to confirm the identities of the attackers and their backgrounds.

09 January 2015.

- The attackers hijacked another vehicle in another Paris suburb with one of the attackers being wounded in a shootout with police. This engagement with police resulted in a high-speed chase leading back to Paris.
- The chase led to a printworks in Dammartin-en-Goele, on an industrial estate on the outskirts of the town.
- Police surrounded the building and culminated shortly thereafter. The brothers, who had talked to local mediaand indicated they would die "martyrs'" deaths, emerged from the building, firing at police. Both suspects were killed and two police officers were injured.
- During this time, another situation took place where a gunman took several people hostage at a kosher supermarket at Porte de Vincennes in the east of Paris after a shootout. The attacker threatened to kill people unless the *Charlie Hebdo* attackers were allowed to go free.
- Once the situation at the printworks was concluded, police launched a rescue operation at the supermarket. The gunman was killed and 15 hostages were freed. However, four hostages were killed. The gunman was later confirmed to have shot and wounded a jogger on 07 January, which was believed to have been an isolated incident at the time.

WHAT CAN BE LEARNED?

The threat actors in these instances had all pledged allegiance to the Islamic State, which was on the rise, having just taken large swaths of territory in Iraq and Syria and proclaiming the establishment of the Islamic Caliphate the year prior. Because all the gunmen in these attacks were killed, it is not completely possible to dig into the details of each individual and their respective motivations, but some points are worth noting:

- **Was the appropriate risk identified?**
  - Charlie Hebdo clearly understood they were a target based on their content and prior incidents (firebombing in 2011 and threats against journalists). They even had a layer of security intended to protect the organization which included a keypad lock and a security guard. Considering the threat environment at the time, to include several incidents in and around Paris in previous years, it would be important to ensure that coordination with local authorities was done, as well as ensuring employees knew to report any suspicious activities in and around the area.
  - Understand the associated or indirect risk. For example, for businesses that may be in and around Commercial Real Estate properties, it is important to understand who the tenants are within the property and if they bring additional risks or threats. If a tenant is threatened, or has taken or made a provocative action, it can have an increased risk for landlords and nearby / adjacent / collocated tenants and facilities. This equally applies to businesses that may have VIPs or other high-profile figures in and around the property. Election season is upon us and there could be public appearances that may increase the risk. Threat actors could identify these as an opportunity to plan and carry out an attack putting not just that business at risk, but those in and around it.
- With risk identification and a risk assessment, it is important to be self-aware and **understand triggering events**. These are events that can push individuals over the line from bystander to someone who takes action. This incident and the *Capital Gazette* shooting in 2018 had been triggered by incidents several years in the past. The *Capital Gazette* shooter was angry over a news report, while the *Charlie Hebdo* attackers were angry over the depiction of Muhammad to the point that they were calling out the names of the journalists they wanted to kill. But these incidents served as triggers that would propel them to action.
- **Be aware of coordinated attacks.** It may never be known if the supermarket attack was planned from the onset or done as a response to help the *Hebdo* attackers; however, organizations are encouraged to consider coordinated or simultaneous attacks. Terrorist groups have long advocated for diversionary tactics in which one attack or incident could draw the attention of security forces while another attack, potentially larger and to greater effect, could be carried out.
- **Understanding influenced attacks.** In 2015, international terrorism looked different than it does currently. It has been widely reported that the Islamic State and al-Qaeda, while still wielding great influence and inspirational ability, have not had the ability to carry out large-scale attacks as they had done in years prior. Both the U.S. Department of State Country Reports on Terrorism 2019 and the European Union Terrorism Situation and Trend report (TE-SAT) 2020 noted declines in international terrorist group activity, while pointing out the rise in violent extremism. But while these groups may not have the same ability to directly impact an attack, they still possess the ability to heavily influence threat actors.
  - On 07 September, the Islamic State group claimed that its fighters carried out an attack in Tunisia that saw one security officer killed and another injured. No direct evidence was given but as has been the case, the group's influence can extend far beyond direct communication with the group. And that is because they can employ resources for others to use, such as the below.
  - Last week, the Institute of Strategic Dialogue (ISD) identified one of the largest digital library collections of online material belonging to the Islamic State, which contained more than 90,000 items and has an estimated 10,000 unique visitors a month. The site includes everything an attacker or group would need to know to plan and carry out an attack, and more.
- **Bleed over to extremist attacks.** While international terrorism may be showing declining numbers (though it is important not to dismiss these groups), violent extremist groups have been on the rise. And there are indications that the groups share a lot in common including the ways in which they use propaganda and exploit civil unrest. Additionally, last week it was reported that the extremist group Boogaloo Bois tried to make an arms deal with Hamas to fund a domestic terror camp ("The enemy of my enemy is my friend").
  - A new report from Politico noted that the Department of Homeland Security is currently drafting a report that will identify domestic violent extremists as the greatest terror threats to the U.S.. The document is currently in draft form but notes, "Foreign terrorist organizations will continue to call for Homeland attacks but probably will remain constrained in their ability to direct such plots over the next year."

However, extremist groups will continue to exploit "social grievances" which have been driving lawful protests.
- Specifically, "Lone offenders and small cells of individuals motivated by a diverse array of social, ideological, and personal factors will pose the primary terrorist threat to the United States. Among these groups, we assess that white supremacist extremists – who increasingly are networking with likeminded persons abroad – will pose the most persistent and lethal threat." Different versions of this document interchange Domestic Violent Extremism with White Supremacists, but the theme remains the same.

MITIGATION

Whether it is international terrorism or domestic violent extremism, the Commercial Facilities Sector has been impacted by it all. And as such, it is important to learn the lessons from previous incidents to remind organizations and reinforce key security principles that may get overlooked or brushed aside.

- **Conduct Risk Assessments.** This has been a repeated theme but it cannot be overstated enough. These helps set the foundation for the rest of the security plan. At a minimum, these should be completed on an annual basis, but they should also be considered on an ad hoc basis should the organization undertake a new direction or plan a new product.
- **Know the Threat.** This may seem simple, but it can be challenging depending on the business line. Was there a decision made that could impact a specific group or affect an individual? If so, is that being seen through customer service or social media platforms? Have there been increases in certain criminal activity in and around your brick-and-mortar locations, or through online targeting? This can be challenging. For example, *Charlie Hebdo* was aware of the threat because their business centered on making jokes, but similarly the *Capital Gazette* reported on an incident that occurred, as was their journalist responsibility. The likelihood of an increased threat may have been higher in the *Charlie Hebdo* incident, but both were targeted and both resulted in multiple deaths. Therefore:
  - It is important to continuously assess and reassess the threat.
  - Consult with local law enforcement.
  - Continuously review threats from customer service and social media.
  - Check in with your neighbors and see if they have experienced increased threats which could create an associated risk for your organization.
- **Implement Security Measures.** Based on the risk assessments and the threat, the organization can then implement the appropriate level of security for the risk and the threat.
  - Once implemented, it is encouraged that organizations evaluate the effectiveness of the measures and improve as needed.
  - In addition, while some measures will be long term and ever-present, organizations can also include added in Random Access Measures (RAM). These are measures that can be implemented at any time and without prior notice. For example, a RAM could be implementing 100 percent ID card screening and bag check in and out of the office. Or it could include setting up a new direction for entrance or exits. A benefit to RAM is that it will disrupt potential threat surveillance and operational planning. It could cause the threat to think twice about attempting their action.
- **Communicate with Employees.** Once these decisions are made, it will be necessary to ensure the employees are kept aware of what is going on and trained on what to be alert for, and trained on how to respond to potential incidents. Employees represent the first line of defense in many areas and educating them on these areas can have long-term impacts and create a positive security culture and move the organization to a better state of preparedness.

David Pounder *is the Director, Threat and Risk Analysis at Gate 15 and serves as an Information Security Officer for a leading financial organization. He advises on both physical and cyber security issues, and specializes in counterterrorism, force protection, and counterintelligence efforts.*

Making Highways, Tunnels, and Bridges More Resilient to Extreme Events

Source: http://www.homelandsecuritynewswire.com/dr20200918-making-highways-tunnels-and-bridges-more-resilient-to-extreme-events

Sep 18 – The **EU-funded RESIST project** aims to provide a methodology as well as tools for risk analysis and management for critical highway structures (in the case of bridges and tunnels) that will be applicable to all extreme natural and man-made events, or cyber-attacks to the associated information systems. Its goal is to increase the resilience of seamless

transport operation and protect the users and operators of the European transport infrastructure by providing them optimal information.

RESIST (RESilient transport InfraSTructure) is a 36-month project that has received funding by the EU's Horizon 2020 Research and Innovation Program, and was launched on 1 September 2018. Its consortium consists of 17 partners from 9 European countries with representatives from academia, construction and the transport industry.

RESIST aims to provide a methodology as well as tools for risk analysis and management for critical highway structures (in the case of bridges and tunnels) that will be applicable to all extreme natural and man-made events, or cyber-attacks to the associated information systems. Its goal is to increase the resilience of seamless transport operation and protect the users and operators of European transport infrastructure by providing them with optimal information.

Nowadays, there are several issues to be confronted regarding transport operations. Firstly, road transport is the most vulnerable mode to extreme weather events (heavy storms, floods) or extreme natural events (earthquakes). Moreover, a large number of bridges and tunnels, which are among the most critical land transport structures, have been in operation for at least half a century and therefore widespread signs of deterioration are obvious. Land transport structures need inspection, vulnerability assessment and appropriate interventions. Inspection, though, in inaccessible bridge and tunnel areas, or structures with high volumes of traffic, is expensive, time consuming and potentially dangerous while structural/vulnerability assessment is also a lengthy process which is especially painful after extreme events. Last but not least, the transport information systems can face dangerous cyber-attacks which can cause disruption of the transport operations. All the above show that not only all the transport operations but also, and more importantly, human lives are in jeopardy.

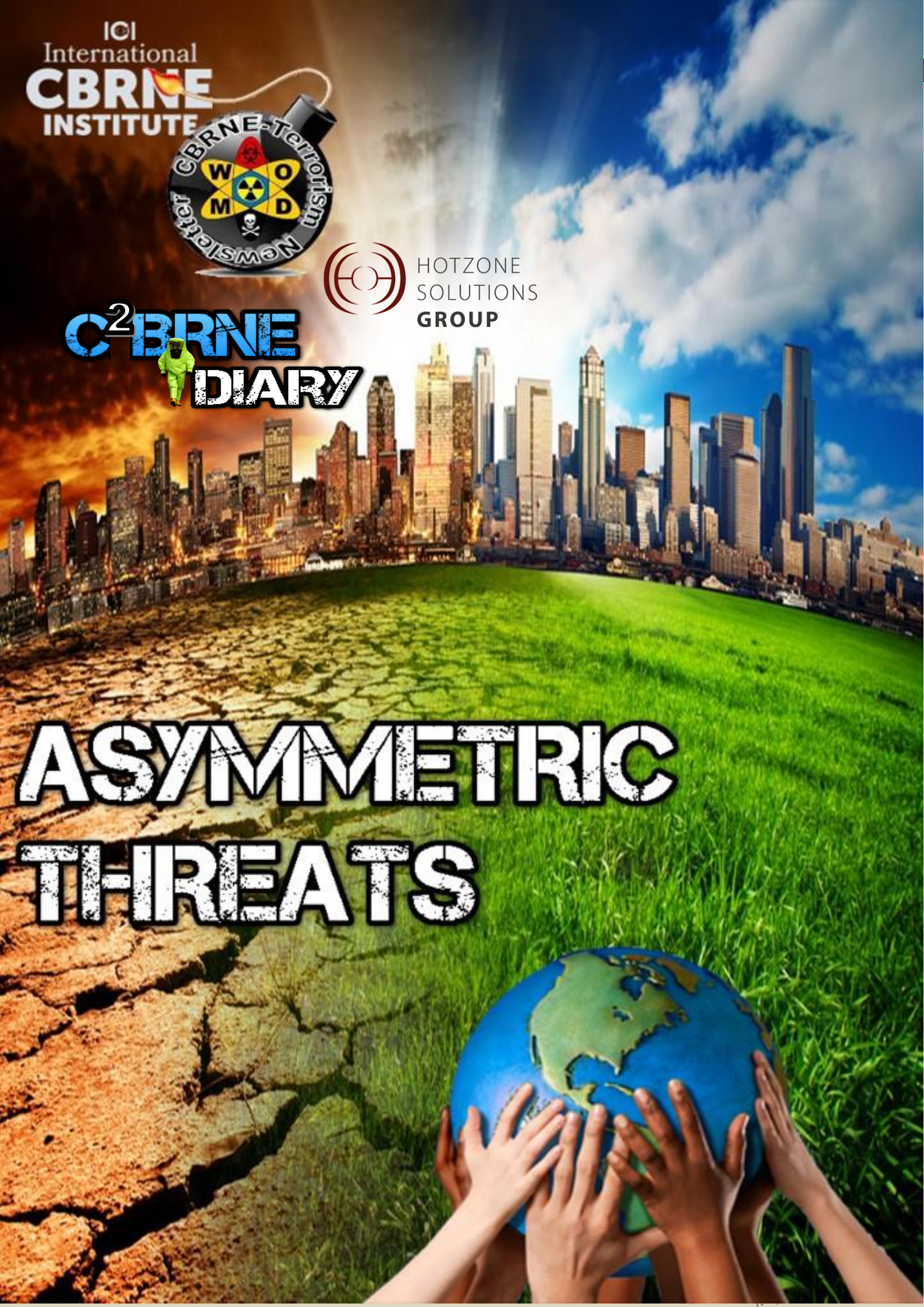
The RESIST project follows a holistic approach on strengthening the critical infrastructure of the road network having in mind that resilience to extreme natural and man-made events should be achieved by upgrading of the existing transport infrastructure, as opposed to building new, which is prohibitively expensive.

RESIST aspires to combine a number of aerial robots with structural vulnerability assessment modules, since aerial robotics have shown very promising results in the field of structural health monitoring providing speed, improved access and higher safety of human actors. Moreover, a mobility continuity module, providing to the project a comprehensive rerouting mobile application with multi-modal capabilities and relevant back office functionalities as well as a risk assessment and management module are in progress. In order to cover the case of the extreme event damaging local communication infrastructure, RESIST utilized the REDCOM node which is capable of completely substituting local communications. The RESIST technology will be deployed and validated at two pilots in real conditions and infrastructures.

Peristeri Bridge, Greece

The **1st Pilot** will be held at the Egnatia Bridge T9, in Peristeri area, Greece. There will be simulations used to assess the impact of various extreme events such as strong winds, floods, severe earthquakes, explosions, cyber security attacks, etc.

The **2nd Pilot** will be held at the Millaures Viaduct of the A32 Motorway and the St. Petronilla Tunnel of the A32 Highway in Italy where an actual field evaluation and demonstration of the proposed system in a GPS denied environment will take place.


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

Captivating Conflagration: Arson as a Terrorist Tactic

By Stevie Kiesel

Source: http://www.homelandsecuritynewswire.com/dr20200914-captivating-conflagration-arson-as-a-terrorist-tactic

Sep 14 – In 2018, the deadliest, most destructive wildfire in California's history tore through the state. The Camp Fire killed 85 and caused an estimated $16.5 billion in damage. The towns of Concow and Paradise were nearly completely destroyed. Not even a year later, Australia experienced an uncharacteristically destructive bushfire season that ultimately killed 34 people, burned nearly 50 million acres, and destroyed almost 6,000 buildings. The fires also wrought devastating impacts on the environment, and cleanup costs alone have exceeded $5 billion.

The most extreme terrorist groups aspire to achieve this level of death and destruction. It therefore comes as no surprise that jihadist groups, such as the Islamic State and its affiliates, have touted these fires and others in their propaganda. A video released earlier this month by the Islamic State's Al-Hayat Media Center describes arson as a highly effective, low-skill attack with great potential for damage and psychological impact, highlighting the California wildfires as an example for how death tolls in large fires "sometimes exceed the number of those lost in major strikes by the mujahideen in which they used guns and explosives." Voice of Hind, an online magazine published by an Islamic State affiliate in India, has encouraged adherents to use fire as a comparatively simple means of attack to "annihilate the disbelievers." Jihadist publications and videos have touted the use of fire for years, from the Islamic State publication *al-Naba* (as well as their now-defunct magazine Rumiyah) to Al Qaeda's magazine *Inspire*. In 2019, the Islamic State claimed responsibility for widespread crop fires that caused a great deal of damage in Iraq and Syria.

The use of arson for terrorist purposes is not a new phenomenon, nor is it limited to jihadists. Extremists on the far right and the far left, as well as special interest extremists, have used arson to send political messages for years. In a recent example from April 2020, John Michael Rathbun was charged with attempted arson after trying to use gasoline to start a fire at a Jewish assisted living center in Massachusetts. Rathbun was active on white supremacist internet forums—so active, and so lax about what he was posting, that his attack was discovered after he posted his plans on a public calendar on Telegram.

Similarly, in 2019 far-right extremist Tristan Morgan accidentally set himself on fire while attempting to burn down the Exeter Synagogue in the United Kingdom. Despite the tactical errors in these cases, the threat of arson terrorism should be taken seriously. Arson has a long history of being used to terrorize black neighborhoods, businesses, and churches in the United States. Even when no lives are lost, the psychological and economic impact of these attacks can be severe.

Environmental and animal rights extremists also have a history of arson attacks. Arson was particularly appealing to their ideology because they wanted to destroy facilities or machinery that they felt were doing harm, but they did not necessarily want to harm humans or animals. For example, the Earth Liberation Front advocated a tactic called "monkeywrenching," which refers to sabotage and property destruction against industries that they perceive to be damaging the environment. Common monkeywrenching tactics include arson, sabotaging logging and construction equipment, and tree spiking. The Earth Liberation Front has claimed responsibility for a number of fires, the most destructive being the 1998 fire at a Colorado ski facility, which reportedly caused $12 million in damage. Other special interest groups that have a history of engaging in arson include the Animal Liberation Front (animal rights) and the Coalition to Save the Preserves (environmental protection). Anti-abortion extremists have also conducted arson attacks, though organizationally they would be considered lone wolf attacks rather than attacks affiliated with a specific group.

While these cases demonstrate clear interest and intent to weaponize fire by a wide range of terrorist groups, a more systematic look at arson as a terrorist tactic is possible by using the Global Terrorism Database developed by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland. This database, whose information is publicly available from 1970 through 2018, captures arson as a unique weapon type. The four charts (see here) show some interesting trends about arson use throughout history.

Arson is an attractive tactic for many types of terrorist groups. Fire can be incredibly destructive in terms of lives lost, property and economic damages, and psychological impact. Arson is a low-cost and low-skill tactic, and elements of nature (such as high winds) can be used as a force multiplier. Additionally, arson can function as just one element of a complex attack, with a potential for "ambushes (luring), intentional depletion of resources (diversion), and follow-on or secondary attacks." Large fires are also incredibly appealing to terrorist groups with apocalyptic or accelerationist ideologies, such as jihadist and extreme right-wing groups.

The COVID-19 pandemic has already had a significant impact on terrorism. Because of ongoing public safety measures and many people's discomfort with crowded areas at the moment, typical soft targets for terrorist attacks are not as plentiful as before the pandemic. Arson may become a more attractive method to terrorists during this time because fires can drive people out of their homes and, much like a virus, once started, fire can spread far and leave devastation in its path. Another worrying development that has accelerated during the pandemic is the rise and increased reach of conspiracy theories. These theories can be incredibly radicalizing, particularly when people are spending more time at home and online while suffering anxiety over the pandemic and the economy. One example of a conspiracy theory whose adherents have committed arson attacks: the theory that 5G cellphone towers are somehow responsible for the COVID-19 pandemic. This theory has led to more than 70 arson attacks on cell phone towers, which can put people's lives at risk if the towers are damaged and access to emergency services is disrupted. Such attacks on critical infrastructure have not gone unnoticed, particularly on white supremacist messaging boards. As COVID-19 forces terrorists to adapt, the potential for arson attacks should not be ignored.

Stevie Kiesel *is Biodefense Ph.D. student, GMU.*