Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

ICI
CBRNE-Terrorism Newsletter
April 2017

Nice/Paris

Berlin

Jerusalem

London

Stockholm

No More roses

St Petersburg

Berkeley develops quick blood test to ID people exposed to ionizing radiation

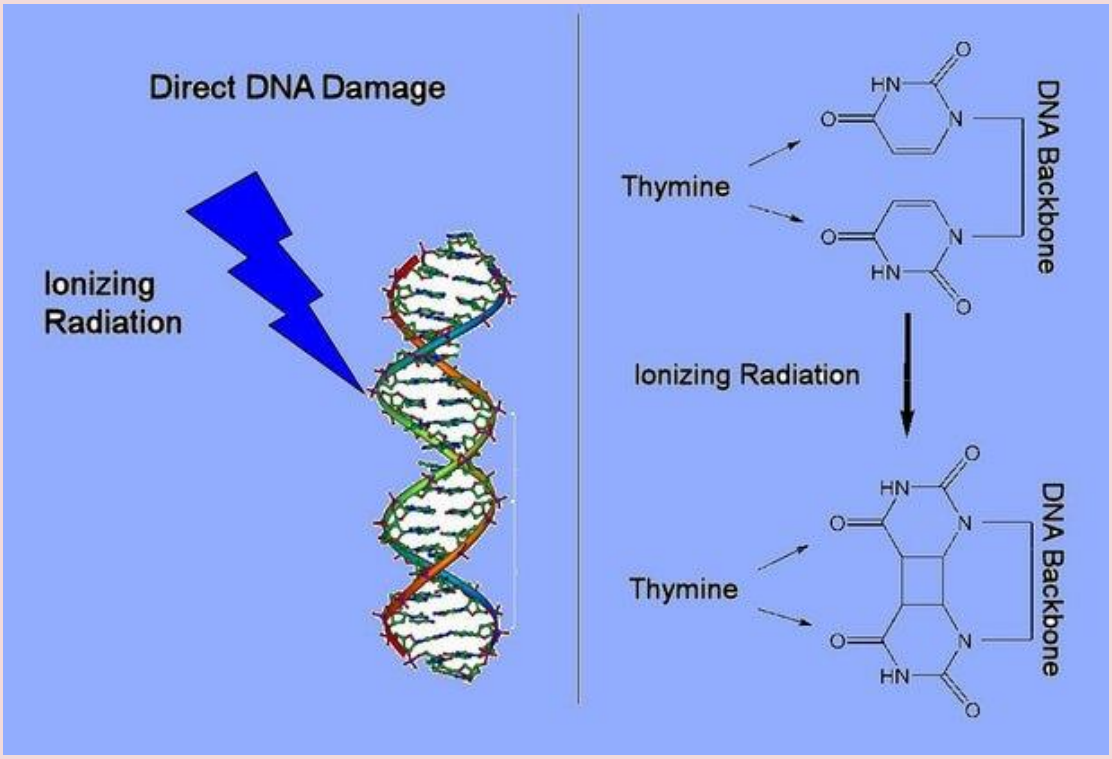
Source: http://newatlas.com/radiation-exposure-blood-test/25733/

January 2013 – Industrial and medical accidents have resulted in about 3,000 cases of acute radiation syndrome with over 100 deaths over the past 60 years. Far larger numbers are possible in the future from major reactor accidents or the use of dirty bombs. In the aftermath of a major incident, the radiation dosages of victims must be sorted out quickly, so that suitable treatment can begin as soon as possible. Medical researchers at the US Lawrence Berkeley National Laboratory have now developed a simple blood test to determine the exposure of a patient to ionizing radiation, that can be carried out in the field with a hand-held analyzer.

Acute radiation syndrome (radiation sickness) results from exposure to high levels of ionizing radiation. Immediate symptoms can include nausea and vomiting, headache, fever, and diarrhea. The problem is that all of these can be caused by shock or infection, which might also be the result of being involved in an industrial accident with an unknown amount of radiation.

As early treatment is the key to maximizing the odds of surviving a large dose of radiation, sorting out the radiological exposure of the victims is a high priority. Unfortunately, at present no quick medical screen exists to identify people exposed to dangerous levels of radiation. While there are early changes in white cell populations, these also can result from an infection due to an injury or chemical exposure.

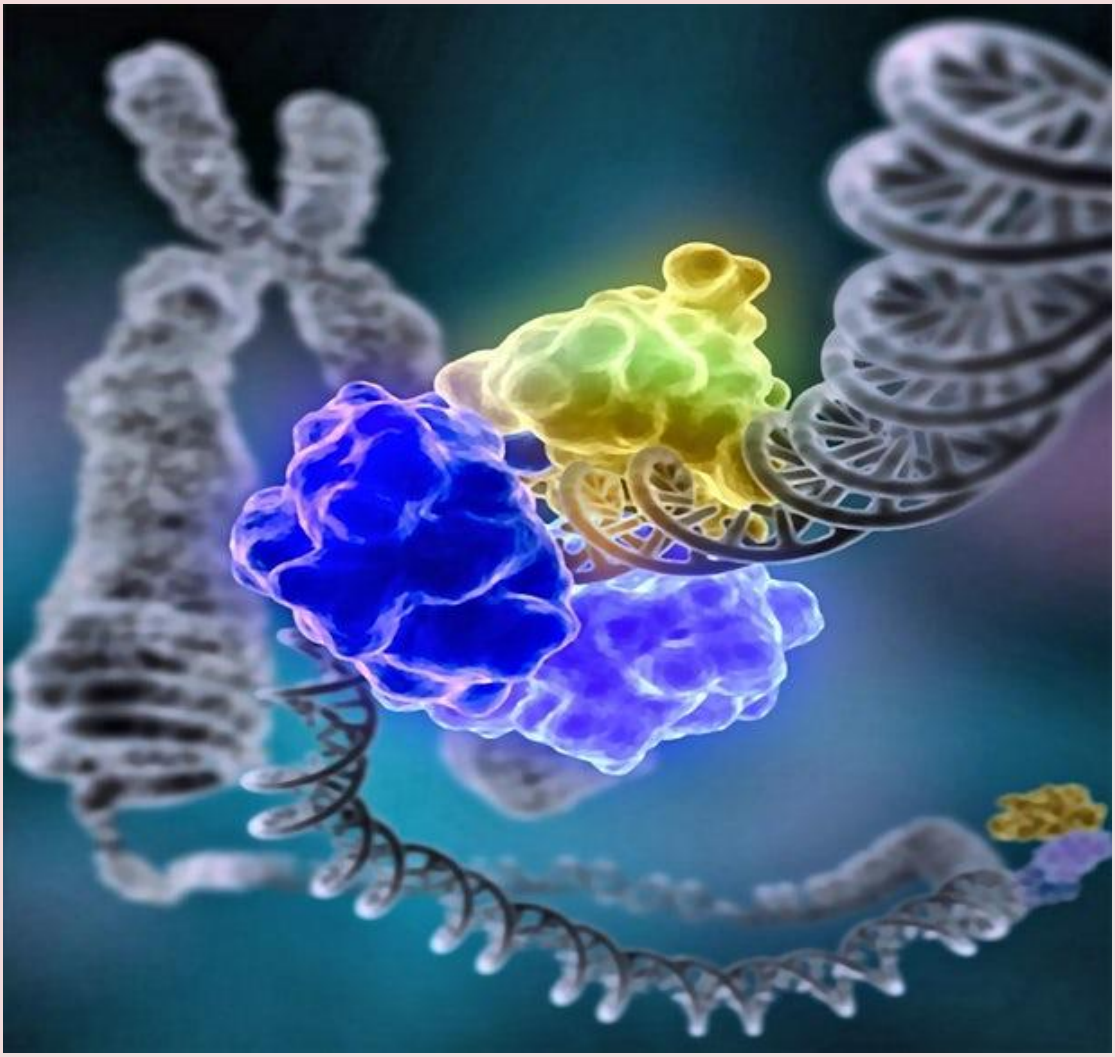
The whole-body absorbed dose is the amount of radiation that actually has produced ionization damage within the body. It is measure in Greys (Gy), which is a Joule of energy deposited within a kilogram of body tissue. One Gy is equal to 100 rads, although that unit is now obsolete. A Gy of radiation is sufficient to produce many millions of ions within each cell of the body.



DNA damage from exposure to ionizing radiation (Image: Gerriet41)

Roughly speaking, there are three broad levels of exposure to ionizing radiation in terms of their effects on people. If exposed to more than eight Gy, a person will die within a week or two. Doctors can only provide palliative treatment to make the patient more comfortable.

If a patient has been exposed to less than two Gy, she will usually live, unless sick or feeble before the radiation exposure. The aim here is to watch and treat individual symptoms as they arise.
The tricky area is for exposures between two and eight Gy. In the upper end of this range, patients will almost certainly die without treatment, but treatment can save perhaps half of the patients. In the lower end, a significant number will die without treatment, but nearly all can be saved. It is in this range where accurately determining the level of radiation exposure is most important.
Currently, it takes several days to determine the level of radiation exposure – far too slow for those who would benefit from immediate treatment. But the Berkeley scientists have now developed a blood test that quickly detects if a person has been exposed to radiation, measures their dose, and separates people suffering from inflammation injuries.



DNA damage is repaired by a special enzyme, DNA ligase, shown encircling the DNA double helix to repair a broken strand of DNA (Photo: Tom Ellenberger, Washington University School of Medicine in St. Louis)

Eight DNA-repair genes have been identified in human blood that respond in a characteristic way to large doses of radiation. These genes respond differently to simple inflammation, such as might be caused by an injury or infection. Inflammation can mimic the effects of radiation and lead to false diagnoses, but these genes change in a manner which allows inflammation to be easily distinguished from radiation exposure. These genes can be evaluated by a blood test that can be done in the field, and quickly identifies who requires immediate treatment for radiation sickness.
More work is needed, but the team leader envisions a blood test using their biochemical markers that could be administered via a handheld device similar to that which diabetes patients use to check their blood sugar. The test could help emergency personnel quickly identify people

exposed to high radiation doses who need immediate care, and people exposed to lower doses who only need long-term monitoring.

The Battle of Chernobyl

Source: http://topdocumentaryfilms.com/the-battle-of-chernobyl/

UK watchdog sounds alarm over doctored papers & security breaches at French nuclear parts supplier

Source: https://www.rt.com/news/382273-nuclear-france-failure-uk/

Mar 25 – Britain's Office for Nuclear Regulation (ONR) has questioned the adequacy of a French nuclear forge which had already supplied parts for UK nuclear sites. It follows revelations of doctored paperwork and security breaches by the French producer.

The ONR report, obtained under a Freedom of Information request and seen by Reuters, gives details on the December 16 visit by an international monitoring team to a French Creusot forge, operated by the country's state-owned nuclear supplier Areva.

Nuclear alert: 130 security breaches at UK atomic facilities in last 5 years

In the report, the UK watchdog warned that safety procedures at Creusot were far below the required standards for a key nuclear equipment supplier. That, they said, could lead to severe consequences for EDF's [the largest energy company in France] Hinkley Point nuclear project currently under construction in southwest Britain, which is set to receive forgings from Creusot.

"ONR should consider the adequacy of EDF's... oversight and assurance arrangements for Areva as a key supplier to Hinkley Point, given the performance shortfalls at Creusot Forge and the associated risks to [nuclear] components manufacture," the regulator said, as cited by Reuters.

Among the breaches was the continued use of correction fluid on documents at the foundry, despite an earlier ban.

The ONR report also inquired into why internal inspections and audits carried out in past decades at Creusor Forge had not discovered and dealt with any of the falsification activities.

Following the December findings, two EDF nuclear reactors were stopped for months, utilities worldwide started reviewing Areva-made parts, and Paris launched a probe into the suspected falsification of documents.

The inspection of the troubled facility was carried out last year by an international team from France, Canada, the US, China, Finland, and Britain.

ONR said that quality control significantly improved *"on the shop floor"* of Creusot, and most of the top management had been replaced.

The UK watchdog noted, however, that the international inspectors *"were not confident that the improvement programmes and associated remedial actions... were sufficiently resourced, prioritised and integrated"* to achieve sustained improvements.

On Friday, ONR said that more check-ups are expected to assure that the components for nuclear reactors are of high quality. Before the end of 2017, a regulatory review will be conducted by the UK watchdog to check the progress of the company which owns Areva, EDF.

EDF confirmed that the requirements will be observed. *"Steel forgings for Hinkley Point C will be manufactured to the most stringent nuclear standards which are reviewed and assessed by the independent UK regulator, the Office for Nuclear Regulation,"* a spokesman for EDF Energy in the UK told Reuters.

Also, its own *"inspection and quality assurance program"* will be used by EDF, to give the *"required confidence that the components manufactured by Areva for Hinkley Point C meet those exacting standards,"* the spokesman noted.

Survey into the radiological impact of the normal transport of radioactive material in the UK by road and rail

Ref: PHE publications gateway number: 2016706 PDF, 581KB, 40 pages

Details

The main objectives of this study were to:

- gather and analyse information on the types of radioactive materials transported by road and rail
- to assess the radiation exposure of transport workers and members of the public from the normal transport of radioactive material by road and rail

The scope covered all types of radioactive material categorised as Class 7 transported, including radioactive materials for medical and industrial use as well as materials associated with the civil nuclear fuel cycle and the transport of radioactive waste products.

The study considers separately the three main sectors that transport radioactive material (Class 7) in the UK:

- civil nuclear industry
- radiopharmaceutical industry
- general industry and research

Nuke Testing 101: How, And Why, North Korea Tests Its Bombs

By Eric Talmadge

Source: http://www.military.com/daily-news/2017/03/29/nuke-testing-101-how-and-why-north-korea-tests-its-bombs.html

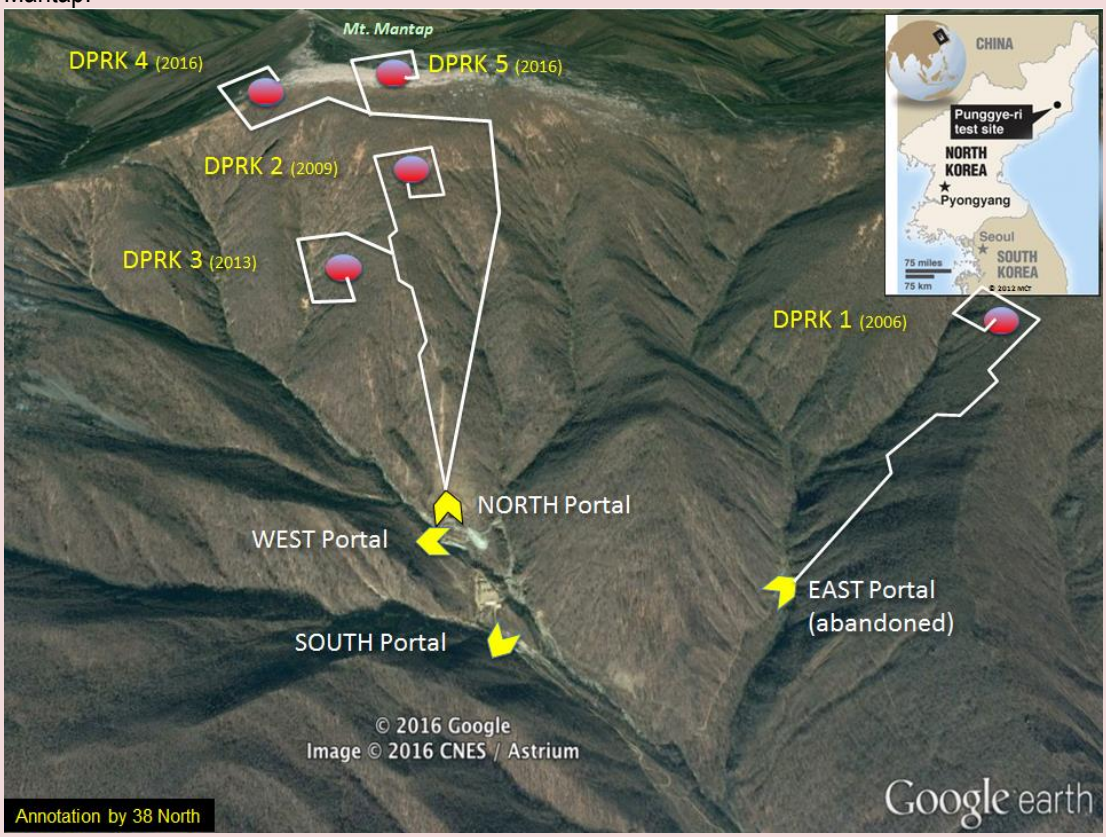
In this Sept. 9, 2016, file photo, a man watches a TV news program reporting a nuclear test by North Korea at Seoul Railway Station in Seoul, South Korea. Ahn Young-joon/AP

Mar 29 – Let's say you're North Korea and you have this nuclear device you really want to test. And let's say you'd rather some of the more sensitive details remain private.

Physicists, geologists, imagery analysts, some of the best militaries in the world, monitoring posts set up by non-proliferation organizations -- beating the technology arrayed against you will be no mean feat.
But, it turns out, they might not actually find very much.
North Korea has proven over the past 10 years it can be exceptionally difficult to determine from a properly set up nuclear test some of the most basic details an adversary would want to know.
Concern is growing another test may be looming because of heightened activity at the North's testing site, though activity can be staged to create a false alarm.
Here's a look at how the North does its testing, and why it keeps it up.

THE TUNNELS OF MOUNT MANTAP

North Korea has conducted five nuclear tests, all in the depths of a remote, granite peak called Mount Mantap.



▶▶ **Read also:** http://38north.org/2017/03/punggye031017/

The location of its testing site is no secret.
It's a favorite target of spy satellites. North Korea featured it in a 2010 propaganda film.
About halfway up the 2,205-meter (7,200-foot) mountain are three main entrances, or portals, into horizontal tunnels stretching a kilometer (about a mile) or more into the mountain. Studies of the tunnel used for the second test, which was conducted in 2009 and featured in the propaganda film, suggest it has the shape of a fishhook. Pakistan used a similar design.
The device was placed at the farthest end of the tunnel, which used the angles and corners of the "hook" section to deflect and absorb as much of the blast as possible. To further optimize absorption, the tunnel had nine or 10 sharp corners with bulkheads and dead-end "debris traps."
To prevent ejecta from escaping into the atmosphere -- and to further contain the explosion itself -- sand, gravel or other materials can be mixed with concrete to plug, or "stem," segments of the tunnels.
The most recent test was probably conducted below 700 meters (770 yards) of solid mountain.
The North has always held its tests between 8 and 10 in the morning.

KEEPING THE GENIE IN THE BOTTLE

North Korea didn't do an especially good job of obscuring its first test, in 2006.

Signature gases were detected in the atmosphere, making it possible for scientists to conclude Pyongyang had used a plutonium device. Seismic data suggested the test was more of a fizzle than a bang.
In 2009, North Korea used a new tunnel and no such gases were detected. In 2013 xenon isotopes were detected but well after the fact. They were too degraded to answer whether the device used plutonium or highly enriched uranium.
That's important because the North has only limited supplies of plutonium, but lots of natural uranium. Uranium enrichment would allow it to build a bigger stockpile, and uranium enrichment facilities are easier to conceal. It is widely believed the North has tested both.
North Korea says it tested an H-bomb in January last year. Last September it detonated its most powerful device to date. It claims that test proved it can put a nuclear warhead on a long-range ballistic missile.
David Albright, a physicist and founder of the nonprofit Institute for Science and International Security in Washington D.C., said that without better evidence, neither claim can be confirmed or denied.
"The evidence so far cannot determine the nature of the test," he said.

WEIGHING THE FALLOUT

A test would bring criticism and possibly tougher sanctions -- or at least tougher sanctions enforcement.
But Pyongyang has stated repeatedly that building a "nuclear deterrent" to counter what it sees as the threat of a U.S.-led invasion is the cornerstone of its national defense strategy. Showing off a little bit can be of tremendous benefit from the military perspective.
And it is showing clear signs of improvement.
Debates persist regarding the true yield of the blasts -- another detail that can be hard to pin down with precision -- but they are believed to have been on an upward trend, with the most recent coming in at somewhere between 10 and 30 kilotons. For comparison, the bomb dropped on Hiroshima had a 20-kiloton yield.
Albright said he is concerned the North is trying to master the use of thermonuclear bomb materials, such as weapons grade lithium-6, and suspects it is looking at new fission designs, including bombs with composite cores of plutonium and enriched uranium.
The payoff would be smaller, but deadlier and more missile-friendly, bombs.
In other words, expect more testing.

***Eric Talmadge** has been the AP's Pyongyang bureau chief since 2013.*

N.K. estimated to have some 1,000 drones: report

Source:http://english.yonhapnews.co.kr/news/2017/03/29/0200000000AEN20170329002100315.html

This photo taken on April 11, 2014, shows three drones which North Korea was presumed to send to South Korea for spying purposes. (Yonhap)

Mar 29 – A South Korean state-run think tank reported Wednesday North Korea is presumed to possess about 1,000 drones, raising concerns they could be used for airborne terror attacks.

North Korea is focusing on developing drones in a bid to make up for the inferiority of the country's air forces and better conduct reconnaissance, Chung Ku-youn, a research fellow at the Korea Institute for National Unification, said in a report.

Since the early 1990s, North Korea is estimated to have been developing various versions of drones, called Banghyun.

Given the level of technology, North Korean drones are projected to fly at an maximum speed of 162 kilometers per hour with an capacity to carry about 20-25 kilogram payloads, the report said.

North Korea has recently developed a large stealth drone **"Banghyun 5"** that can carry explosive devices and radioactive materials,

"North Korea's air forces are inferior to its South Korean counterpart and an absence of military satellites is making it difficult for Pyongyang to reconnoiter (the South)," the report said.

Chung expressed concerns about North Korea's possible use of drones for terrorist attacks or provocations.

North Korea may seek to put chemical or biological weapons on drones to carry out far-away attacks, the report said.

North Korea is presumed to possess about 25 chemical agents including six nerve agents such as sarin and VX, according to a 2016 report by the Korea Institute for Defense Analyses. The country is not a signatory to the Chemical Weapons Convention.

Pyongyang is estimated to also have 13 types of pathogens such as anthrax and clostridium botulinum that can be used as biologic weapons, it said. In 1987, the country became a signatory to the Biological Weapons Convention.

Kim Heung-Kwang, a defector and the head of a private think tank, said last year.

The Banghyun-5 drone, as it is supposedly called, is made of titanium and carbon composites and has a 900-liter fuel tank, allowing it to fly for up to 10 hours. The drone is designed to carry a payload of enriched uranium, which North Korea is believed to possess as a result of its nuclear weapons program.

Also known as a Radiological Dispersal Device (RDD), a dirty bomb is not to be confused with a nuclear weapon. Instead, it uses conventional explosives such as TNT or dynamite to spread radioactive material over a wide area. The more powerful the explosive, the wider the contaminated area. Other dispersal means include aerosol sprays and crop-dusting planes.

A wide variety of radioactive isotopes are candidates for dirty bombs, including Americium-241, Californium-252, Cesium-137, Cobalt-60, Plutonium-238, and Strontium-90. Dirty bombs rarely have enough radioactive material to kill.

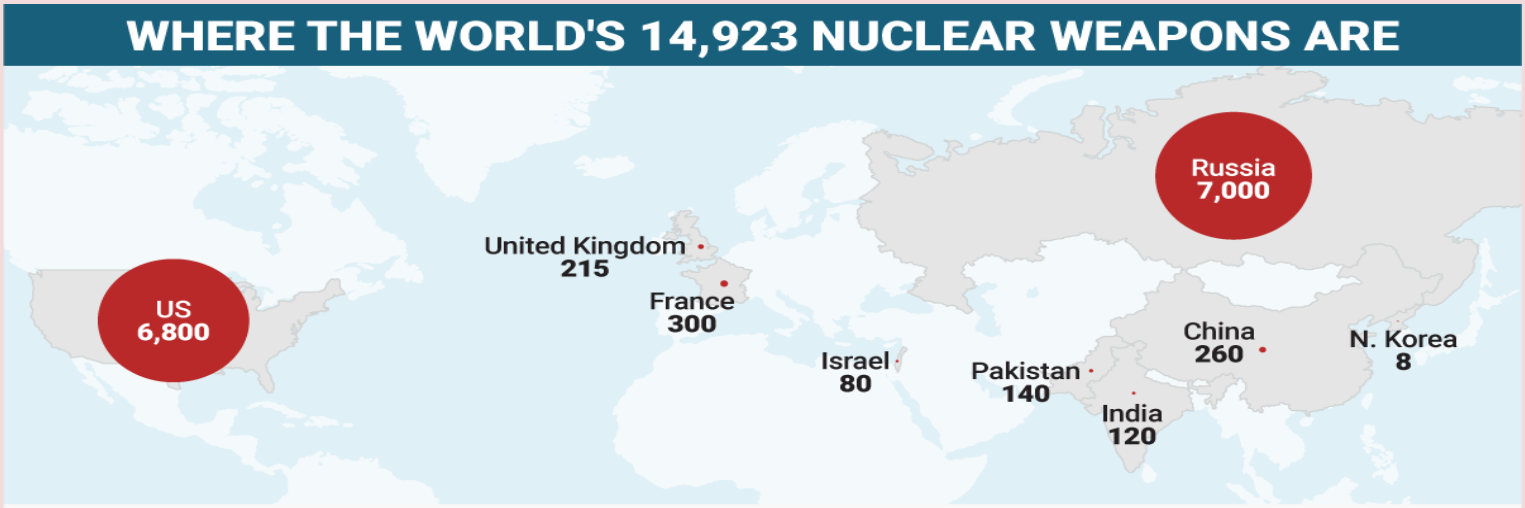
Prolonged exposure may cause radiation sickness and elevate a person's long term chances of developing cancer but are not instantly lethal. They mostly create fear and panic due to public perceptions of radiation dangers.

Another byproduct of an RDD attack is seeding an area with radioactive fallout, making it dangerously uninhabitable—but easily avoided. The half life of some isotopes is in the hundreds of years, making an expensive and tedious cleanup necessary.

Now, this report should be taken with a grain of salt. Such a program would be a closely held state secret in North Korea, a notoriously inaccessible country. Titanium and carbon composites are also hard to manufacture. On the other hand, North Korea is known to have a great deal of interest in drones, and has repeatedly flown them over South Korea. Several drones have crashed in South Korea, including drones with photographs of the capital, Seoul, and the Blue House, the official residence of the South Korean president.

A radiological dispersal device drone would be an ideal weapon for North Korea's provocative attacks. The country's leadership periodically orders provocations—such as shelling an inhabited island with artillery or starting a gun battle at sea—in order to appear unstable. Attacking a South Korean park, building, or landmark (such as the Blue House) with the drone probably wouldn't trigger a war with Seoul but certainly would grab the attention of the international community.

Nukes – who is having what



Country	Russia	US	France	China	UK	Pakistan	India	Israel	N. Korea
Deployed	1,910	1,800	290	?	120	0	0	0	?
Stockpiled/non-deployed/other	2,390	2,200	10	260	95	140[A]	120[B]	80	8
Retired/waiting to be dismantled	2,700	2,800	0	0	0	0	0	0	0
Total	7,000	6,800	300	260	215	140	120	80	8[C]

A. Some data suggest Pakistan has 120-130 nuclear weapons, which are left unassembled until launch. (FAS)

B. Similarly, some data suggest India has 110-120 unassembled nuclear weapons. (FAS)

C. Estimate based on bomb-grade material North Korea has likely made. It's not publicly known if the nation has warheads capable of launch.

SOURCES: Bulletin of the Atomic Scientists; Federation of American Scientists; SIPRI

BUSINESS INSIDER

Radioactive parcel intercepted at Moscow airport

Source: https://www.rt.com/news/383744-radioactive-parcel-moscow-airport/

Employees of Moscow's Vnukovo airport work in the customs control zone. © Alexey Filippov / Sputnik

Apr 06 – The Russian Postal and Federal Customs Services intercepted a radioactive parcel at a logistics center at Moscow's Vnukovo Airport and sent it to a special facility for disposal on Thursday.

The discovery was made *"during a check of mail to be delivered outside Russia,"* the Russian Post's press-service told TASS news agency.

As the **Yantar radiation control system** was scanning one of the parcels, it registered *"gamma rays exceeding the maximum permissible radiation background by dozens of times,"* it said.

READ MORE: Radioactive boars found in Czech forests 31yrs after Chernobyl disaster

The source of dangerous emissions was immediately removed from the rest of the packages and placed in a protective container.

The parcel contained *"an aeronautic measuring device with a built-in dial piece,"* the press service said, adding that the radioactive cargo had been sent to a specialized facility for disposal.

"The radiation level of the remaining postal items was at standard level," it stressed.

The radioactive parcel had been sent by a female Muscovite to an addressee in the UK, according to TASS's police source.

Here are the missiles North Korea just showed off, one by one

Source: https://www.washingtonpost.com/news/worldviews/wp/2017/04/15/here-are-the-missiles-north-korea-just-showed-off-one-by-one/

The Pukkuksong-1 submarine-launched ballistic missile on a truck.

Apr 16 – North Korea put on a jaw-dropping military display Saturday, when the regime celebrated its most important day of the year: "the Day of the Sun," the anniversary of its founder, Kim Il Sung.
Kim Jong Un, the founder's grandson and the current leader of North Korea, has made it very clear that he wants nuclear warheads and the means to deliver them to the United States. In his New Year's Day address, Kim said that North Korea was entering the "final stage" of preparations to launch an intercontinental ballistic missile capable of reaching the American mainland.
So experts were anticipating a big show Saturday, but even they were stunned by the range of apparently new missiles on display, and the sheer number of them.
We talked to Jeffrey Lewis, head of the East Asia program at the James Martin Center for Nonproliferation Studies in California and a self-described "arms control wonk," about the missiles on display Saturday.

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

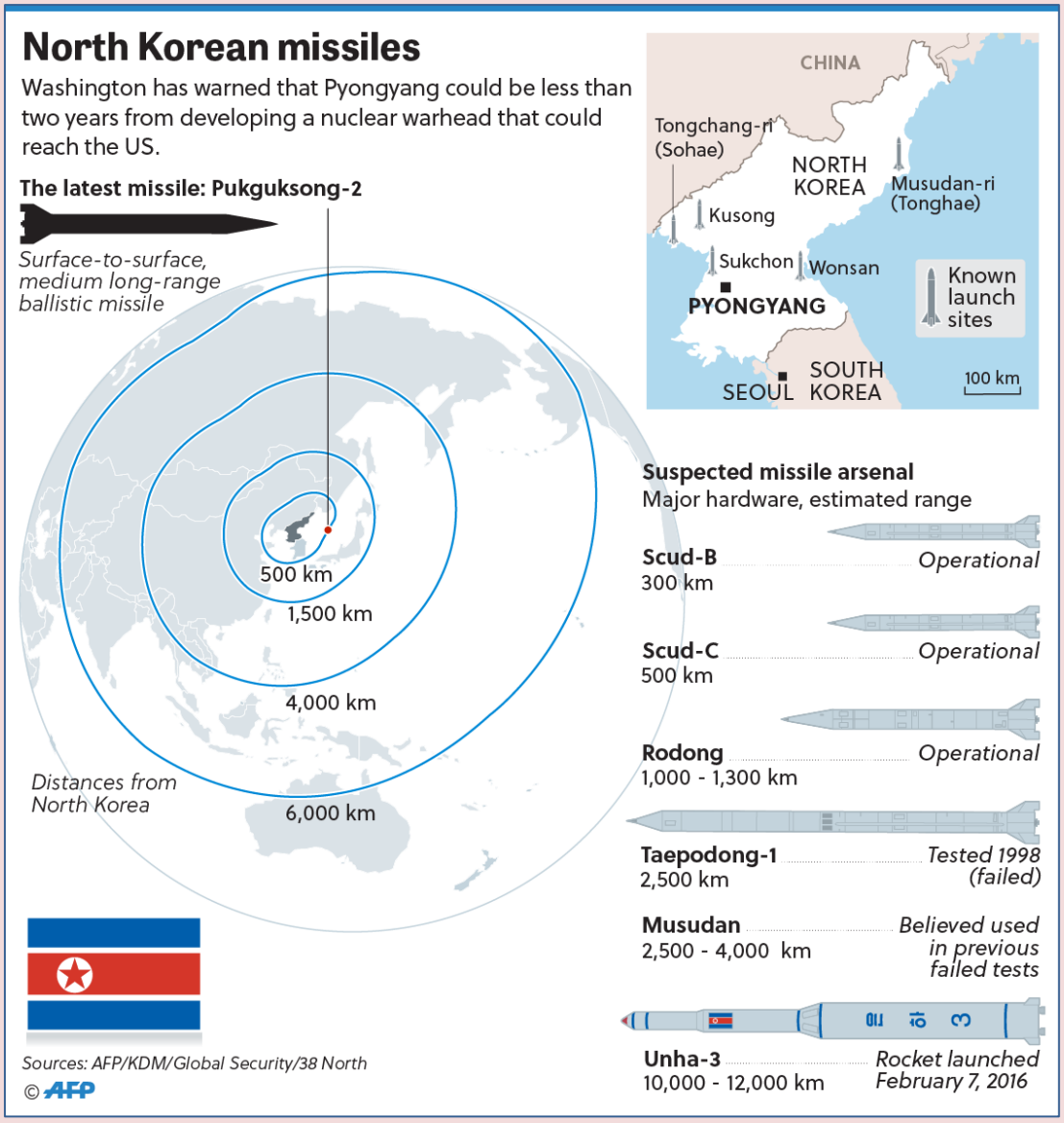
North Korean missiles officially banned and widely available

By Bertil Lintner
Source: http://www.atimes.com/article/north-korean-missiles-officially-banned-widely-available/

Apr 19 – North Korea's failed missile launch on April 16, only a day after the reclusive regime rolled out its big guns in a huge parade in the capital Pyongyang, may have come as a sigh of relief to many Western observers worried about the increasingly belligerent behavior of one of the world's last pariah regimes.
It is still not clear what type of missile malfunctioned, but it exploded within seconds of being launched from a test site on the northeastern coast of the Korean peninsula. The relief may be short-lived, though, as the missile arsenal displayed the day before showed that Pyongyang has developed a wide range of new missiles beyond the one that sputtered and exploded.
The most advanced of those missiles, known as the Taepodong 2, has a potential range of 6,700-9,000 kilometers that could conceivably reach the west coast of the United States if fully developed. North Korea's expanding missile reach is known to be a driving force behind US President Donald Trump administration's rising strategic threats against Pyongyang.

Years of international trade sanctions, near-economic collapse and even widespread famine have failed to hamper the country's missile development programs, which are geared for both preemptive defense and export.

Despite United Nations-imposed bans on military equipment exports, North Korea has earned and is still earning substantial revenue from the sale of missile components and related technology overseas.



It is widely believed that those exports have kept Kim Jong-un's regime afloat and are the financial source of his more menacing nuclear program. Pyongyang's military equipment and missile customers over the years have included Iran, Egypt, Pakistan, Libya, Syria, the United Arab Emirates (UAE), Angola, Vietnam and Myanmar.

In more recent times, however, North Korea has lost some of its most important missile customers, including Pakistan, which moved closer to the United States after the invasion of Afghanistan in 2001, Libya, whose long-time leader Muammar Gadhafi was ousted in 2011, and Syria, which is being torn apart by civil war.

The UAE was apparently not satisfied with the quality of North Korea's Hwasong missiles, which they reportedly left to rust in a warehouse after replacing them with US-made missiles. Earlier missile development cooperation with Angola and Vietnam has also ceased as those two countries have also distanced themselves diplomatically from North Korea.

Submarine-launched ballistic missiles and what appeared to be land-based medium to long range Pukguksong-2, or KN-15, missiles were shown for the first time during the April 15

parade in Pyongyang. A variant of the latter was fired in February when Trump was meeting with Japanese prime minister Shinzo Abe at his golf resort in Florida.

That successfully launched missile reached a height of 550 kilometers before falling into the sea, 500 kilometers east of the Korean coast.

North Korea began producing surface-to-air missiles more than 50 years ago with the help of Soviet technicians. But those were quite rudimentary and it was not until Pyongyang signed a defense agreement with China in 1971 that the industry really took off.

North Korea gradually became capable of developing and fine-tuning its growing arsenal of missiles with the help of some rather unexpected non-communist partners.

Egypt was first to provide assistance. Pyongyang first helped Cairo in the war against Israel in 1973 by providing pilots to its air force. In return, Egypt transferred a small number of Soviet-supplied FROG-7B missiles and launchers to North Korea.

In the early 1980s, Egypt provided North Korea with Soviet-made SCUD B missiles, which were not test-fired but rather used as models for reverse-engineering in a string of new defense factories that Pyongyang had established.

Pakistan was next. In the early 1970s, Islamabad approached Pyongyang to buy conventional weapons at a time when tension was escalating with India as East Pakistan was breaking away and eventually became Bangladesh.

More sophisticated weaponry soon appeared on Pakistan's shopping list, and the modified version of North Korea's Rodong missile known as Gauri was first tested in April 1998. Cooperation with Iran led to the development of its Shehab missile system, which was based on similar designs.

More recently, North Korea and **Myanmar**'s then military junta signed a defense agreement in Pyongyang in November 2008, which included missile development programs. The status of that cooperation is unclear, however. In January 2012, then president Thein Sein — a former military general — declared that allegations of a such a relationship with North Korea were "unfounded."

In July 2013, the US Treasury Department sanctioned Lieutenant General Thein Htay, the head of Myanmar's Directorate of Defense Industries, for his alleged involvement in the illicit trade of North Korean armaments to Myanmar.

The sanctions order said: "The international community has repeatedly condemned North Korea's nuclear and ballistic missile proliferation activity, most recently in UN Security Council Resolutions 2087 and 2094. North Korea's arms trade provides it with an important source of revenue to expand and enhance its proscribed nuclear and missile programs, which are a threat to international peace and security."

The US government, which at the time was restoring relations with Myanmar's new quasi-civilian government in Naypyidaw, added diplomatically that there was no evidence to suggest that this was official Myanmar policy.

Diplomats and analysts remain skeptical, however. According to well-placed military sources, KOMID, or the Korea Mining and Development Trading Corporation – a state-owned entity that is the main exporter of equipment related to ballistic missiles as well as conventional weapons – appointed Kim Chol-nam as its new representative in Myanmar in late 2016.

Previously based in Beijing, he has been blacklisted by the US and mentioned in UN Security Council reports for his involvement in weapons trading, including the sale of missile parts and technology.

Whatever the current status of North Korea and Myanmar's missile development program, the loss of old customers in the Middle East has prompted Pyongyang to focus on Southeast Asia, and apparently Naypyidaw in particular, for new sales.

Myanmar is also believed to owe Pyongyang substantial funds for previous military assistance, which means that relations with North Korea, despite assurances to the contrary made by Naypyidaw authorities to the US and others, are likely still alive and well.

Even if the April 16 missile test was a spectacular failure, the public display of old and new missiles at this month's Pyongyang parade shows that North Korea still possesses some of the most developed missile systems in the world.

Kim Jong-un clearly sees such advanced weaponry as life insurance for his regime, as well as its most important source of foreign exchange.

The hard truth is that North Korea has only limited export commodities other than weapons that its foreign trading partners are interested in buying.

Bertil Lintner *has reported on North Korea's weapons of mass destruction for Jane's Defense, the Far Eastern Economic Review and Wall Street Journal, and is the author of Dear Leader, Great Leader: Demystifying North Korea under the Kim Clan*

North Korean missile launch possibly sabotaged

Source: http://www.debka.com/

An unidentified North Korean ballistic missile exploded seconds after it was launched Sunday, April 16, from a site near the port city of Sinpo, just as US Vice President Mike Pence arrived in Seoul for talks with the South Korean government on how to deal with Pyongyang's belligerence. The medium-range missile failure occurred the day after a spectacular military parade rolled through central Pyongyang to mark the 105th anniversary of North Korea's founder Kim Il-sung. It showcased 50 missiles, including the first display of a submarine-launched missile.

The responses of US officials and the concurrence of the failed detonation with the arrival of the US vice president suggest that North Korea's missile and nuclear programs are closely monitored by US intelligence, electronic and cyber tools. A previous North missile launch on April 5 suffered an in-flight failure before the weapon crashed into the Sea of Japan. There was also an unsuccessful missile launch in late March.

Out of a basketful of aggressive options, DEBKAfile's military and intelligence experts pick the four most likely methods the Americans may have applied to thwart the latest North missile launch:

1. Sabotage of the missile's fuel, guidance, or communications systems, or of its exterior or the launch pad.
2. Sabotage of the missile's command and control system, such as changing its flight commands, ignition system, or ordering it to self-destruct, as is done to avoid landing in an unintended location or falling into enemy hands.
3. Electronic warfare against the command and control systems in the mission control center by sending powerful electromagnetic pulses to disrupt communications with the missile.
4. A cyberattack against the missile's control system that changes the electronic commands and downs the missile.

Are Governments Sufficiently Prepared for Nuclear Incidents?

By Arik Eisenkraft

Source: http://www.hstoday.us/single-article/exclusive-are-governments-sufficiently-prepared-for-nuclear-incidents/6ad5dfd5ffca3c2af992fa325a728a62.html

Apr 20 – As more and more countries move away from fossil fuels and towards alternative energy sources, many are reexamining their approach towards nuclear energy.

Six years after the Fukushima nuclear incident, three decades after the Chernobyl nuclear disaster and nearly four decades after the Three Mile Island nuclear accident, governments are still grappling with the public safety implications of nuclear energy. All three episodes prove that the risks are far from theoretical.

One thing is clear: whatever the cause – whether a natural disaster such as an earthquake followed by a tsunami, a set of human errors or a flawed nuclear facility combined with human error -- there are countless sets of circumstances which have the potential of spiraling into a nuclear disaster. History has taught us that no nuclear system is nature-proof, or foolproof.

An analysis of radio-nuclear disasters from the past, such as the 1986 Chernobyl accident in the Ukraine or the 1978 Goiânia incident in Brazil, provides us with some insight about how to begin planning for similar inevitabilities in the future.

What can we expect in any future radio-nuclear accident?

Hundreds if not thousands of people would likely be exposed to

radiation levels that will have some effects on their health. Many will develop Acute Radiation Syndrome (ARS), while some will suffer combined injuries of trauma and radiation. Others involved will be left to wonder for the rest of their lives how the effects of the exposure to ionizing radiation will affect them. This may well

lead to acute psychological stress, influencing their everyday lives – as we see now in the Fukushima Prefecture six years after that 2011 disaster.

These types of analyses of past incidents have led to renewed emphasis on public safety, especially the need for advanced preparations in case of a radio-nuclear crisis.

Though it would be advantageous to establish a doctrine that fits all possible scenarios (and despite the fact that mass casualty scenarios resulting from different causes do share some similarities), there are still profound differences and distinct preparedness gaps between a radio-nuclear event and other types of catastrophes, whether conventional or non-conventional, which warrant unique approaches in preparedness.

Hence, in parallel to risk assessment analyses and meticulous planning of nuclear facilities, decision makers must continue to upgrade response plans for possible nuclear incidents of all types, looking at major and minor components of rescue and relief efforts.

Emergency response plans are prepared on various levels. Federal and state decision makers begin at the strategic level, looking mainly at national consequences and gaps. The different response organizations and agencies typically prepare lower-levels plans, intended to enhance emergency responses in the event of such a disaster, with relevant adaptations to scenarios such as mass casualty events, a fire-related disaster, Chemical, Biological, Radiological and Nuclear (CBRN) defense incidents (with differences between each of the components), or any other natural or man-made disaster.

As with other mass casualty scenarios, these preparations include medical preparedness, such as the stockpiling of approved medical countermeasures (MCMs), ensuring they are kept in a way that will enable prompt handling, shipping and distribution to prevent the effects of radiation on exposed individuals in relevant timeframes.

Governments must also supply funding for research and development efforts to allow for novel, safer and more effective MCMs than what are currently being stockpiled for use by the entire population, including children and pregnant women, which are defined as higher-risk populations.

Medical preparedness also includes defined guidelines and doctrines for first responders, medical personnel and anyone else who is expected to be involved in response efforts. This includes educating and training first responders and hospital staff, purchasing personal protection equipment for first responders, preparing hospitals to cope with such a radio-nuclear disaster, defining relevant medical countermeasures, as well as long-term follow-up plans.

Preparedness efforts should also include evacuation plans for residents living close by to such facilities. Civilian education programs dealing with basic issues of how to react in case of a radio-nuclear catastrophe must also be put in place.

Two major gaps in such preparedness need to be considered by governments assessing their readiness to deal with such disasters.

The **first** is lack of field dosimetry – meaning that we are currently unable to measure precise levels of exposure to radiation. Without field dosimetry, we cannot define who is in danger of developing ARS and needs to be closely monitored in order to receive early medical intervention.

The **second** gap regards currently accepted MCMs for ARS. Those MCMs currently stockpiled are helpful, but have limited efficacy, focusing mainly on one subpopulation of blood cells that are relevant in the Hematopoietic Syndrome of Acute Radiation Syndrome (H-ARS). These drugs

do help in preventing life-threatening infections, which is one of the hallmarks of ARS.

However, other hematological effects like severe anemia and low numbers of platelets, and effects on other physiological systems and organs may also cause life threatening complications, and the drugs currently available hardly address any of these issues.

In addition, these drugs require large teams of trained personnel and are extremely complex to distribute, likely leading to a less than optimal response.

Several countries throughout the world have completed or are in the process of completing critical preparations for these types of nuclear scenarios. That said, there continue to be remarkable differences in preparedness between such countries, mainly due to differences in their definitions of the risks involved and in the basic approach towards these scenarios (resulting mainly from cultural and economic differences).

For those countries which do see nuclear energy as part of their ongoing national energy strategy, formulating precise and detailed preparedness plans must be an integral part of their programs, for the benefit of all their citizens.

Dr. Arik Eisenkraft *is Director of Homeland Defense Projects at Pluristem Therapeutics Inc. and involved in several Israeli start-ups in the field of military medicine. From 2008-2016 he served as Head of the Medicine Branch at the CBRN Protection Division of the Israeli Ministry of Defense where he led the national research and development efforts as well as procurement of MCMs against all CBRN threats, working together with national and foreign governmental departments and agencies, the IDF the Home-Front Command and the Israeli Ministry of Health. His efforts focused on the seeding of new research programs, aimed at developing new MCMs, as well as re-purposing and broadening clinical indications of currently available compounds, and testing cutting-edge technologies for drug delivery methods. From 2000-2008 he served in the CBRN Medicine Branch of the IDF. He's currently a member of several national professional teams in the field of CBRN Medicine. He has an MD degree from the Sackler Faculty of Medicine, Tel-Aviv University, Israel; a residency in Pediatrics from the Sheba Medical Center, Tel-Hashomer, Israel; and a MHA degree from the Ben-Gurion University of the Negev.*

New nuclear forensics signature discovery capability to help trace origins of plutonium

Source: http://www.homelandsecuritynewswire.com/dr20170421-new-nuclear-forensics-signature-discovery-capability-to-help-trace-origins-of-plutonium

Apr 21 – Two weeks ago the Department of Homeland Security's Domestic Nuclear Detection Office (DNDO) joined with partners at the Pacific Northwest National Laboratory (PNNL) to launch the Plutonium Processing Signatures Discovery capability. The new capability, the result of a four-year effort, represents a significant technological advancement in nuclear forensics that will improve our ability to trace the origins of plutonium. Nuclear forensics involves determining where illicit or smuggled radioactive material came from. In the event of a nuclear weapon detonation, knowing where radioactive material came from can help investigators determine who's responsible.

DHS notes that there are different ways to process plutonium. These varied processes can produce slightly different characteristics in plutonium, such as the color and density. These unique characteristics found in nuclear materials are referred to as "nuclear forensics

signatures." This new capability will significantly improve our ability to trace the origins of plutonium, because it allows us to replicate individual nations' processes. This not only helps us identify where the radioactive material came from, but also allows us to predict forensic signatures of plutonium from a given process without having actual samples of those materials.

"The new **Plutonium Processing Signatures Discovery** capability, along with other nuclear forensics clues and law enforcement and intelligence information, will help in identifying the origin of interdicted nuclear materials and the perpetrators responsible," DHS says.

As Dr. Steven Ashby, Director of PNNL, said, "The development of the Plutonium Processing Signatures Discovery capability is four years in the making and the result of a great partnership and close collaboration between PNNL, DNDO, and the nuclear forensics community."

William Powell, 'Anarchist Cookbook' Writer, Dies at 66

Source: https://www.nytimes.com/2017/03/29/arts/william-powell-anarchist-cookbook-writer-dies.html

William Powell, as seen in the documentary "American Anarchist." Credit Gravitas Venture

Mar 29 – William Powell was a teenager, angry at the government and the Vietnam War, when he walked into the main branch of the New York Public Library in Manhattan in 1969 to begin research for a handbook on causing violent mayhem.

Over the next months, he studied military manuals and other publications that taught him the essentials of do-it-yourself warfare, including how to make dynamite, how to convert a shotgun into a grenade launcher and how to blow up a bridge.

What emerged was "The Anarchist Cookbook," a diagram- and recipe-filled manifesto that is believed to have been used as a source in heinous acts of violence since its publication in 1971, most notably the killings of 12 students and one teacher in 1999 at Columbine High School in Littleton, Colo.

Throughout his manual, Mr. Powell fashioned a knowing voice that suggested broad experience in warfare, sabotage or black ops, mixed with an extremist's anti-establishment worldview.

"As almost everyone knows, silencers are illegal in virtually all the countries of the world," he wrote before describing how to build a silencer for a handgun, "but then a true revolutionary

believes that the government in power is illegal, so, following that logic, I see no reason that he should feel restricted by laws made by an illegal body."

He declared that his book was an educational service for the silent majority — not the one identified by President Richard M. Nixon as his middle-American constituency, but the disciplined anarchists who were seeking dignity in a world gone wrong. To them, he offered how-to plans for weaponry and explosives as well as drugs, electronic surveillance, guerrilla training and hand-to-hand combat — a potent mix that attracted the attention of the Federal Bureau of Investigation.

The book found a big audience. More than two million copies have reportedly been sold, and still more have been downloaded on the internet.

"It was inevitable that he did it," James J. F. Forest, a professor of security studies at the University of Massachusetts, Lowell, said in a phone interview. "If he hadn't done it, somebody else would have. It's human behavior to tap into a dangerous stream of knowledge, and in his case he was inspired to make that dangerous information available to anyone else who was interested."

Mr. Powell never revised the book or wrote a sequel, but his original stayed in print, through Lyle Stuart and its successor company, Barricade Books, and most recently by Delta Press. Eventually, he renounced the book. In 2000, he posted a statement to that effect on Amazon.com. And later, in 2013, he expressed his regret in an article he wrote for The Guardian.

He chose a career as a teacher, not a revolutionary, specializing in working on behalf of children with special needs.

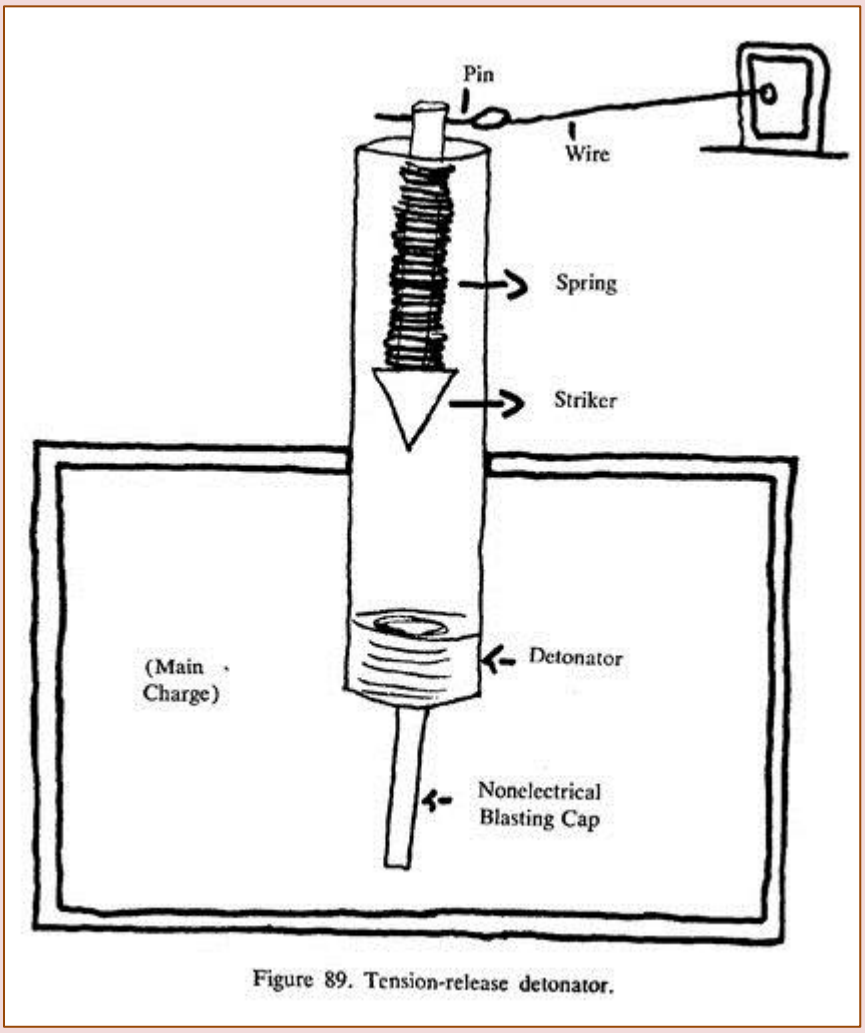


Figure 89. Tension-release detonator.

And then, on July 11 of last year, he died of a heart attack while vacationing with his family near Halifax, Nova Scotia. He was 66 and had lived part-time in Massat, France, when he was not working with his wife, Ochan Powell, on educational projects in other countries.

A sketch from "The Anarchist Cookbook." Credit Barricade Books Inc.

His family reported the death on Facebook, but few if any obituaries followed. His son Sean said that the people who needed to know had been told, and that the family had not thought of reaching out to newspapers.

It was not until last week that his death became more widely known, with the theatrical release of "American Anarchist," a documentary about Mr. Powell. His death was noted in the closing credits.

The director, Charlie Siskel, said he had interviewed Mr. Powell over a week in 2015.

"What interested me was: How do you go through 40 years of your life with his dark chapter in the background?" Mr. Siskel said on Monday. "How does one sleep at night or get through the day?"

On camera, Mr. Powell seemed to struggle to absorb the idea that his book had apparently had an influence on a number of notorious criminals.

One was Zvonko Busic, a Croatian nationalist who hijacked a TWA flight in 1976 while carrying phony bombs after leaving a real one at Grand Central Terminal that killed a police officer who tried to deactivate it.

Others included Thomas Spinks, who was part of a group that bombed abortion clinics in the 1980s; Timothy McVeigh, who bombed the Alfred P. Murrah Federal Building in Oklahoma City in 1995; Eric Harris, one of the Columbine attackers; and Jared Loughner, who killed six people during his attempted assassination of Representative Gabrielle Giffords in Arizona in 2011.

"When 'The Cookbook' has been associated with Columbine and the later characters and killing, I did feel responsible, but I didn't do it," Mr. Powell told Mr. Siskel, adding: "Somebody else with a perverted, distorted sense of reality did something awful. I didn't."

William Ralph Powell was born on Long Island, in Roslyn, on Dec. 6, 1949. His father, William Charles Powell, was a press officer at the United Nations; his mother, the former Doreen Newman, ran a phobia clinic at a hospital in White Plains.

Mr. Powell told Mr. Siskel that after his father was transferred to Britain, he attended a school where bullying was commonplace and where the headmaster had caned him. When the family returned to the United States, he said, he felt alienated as an outsider. His fifth-grade teacher mocked his British accent. At a prep school in Westchester County, N.Y., he said, he was molested by the dorm master.

He was working at a bookstore in Greenwich Village in late 1969 when he decided to quit his job to research and write "The Anarchist Cookbook."

"My motivation at the time was simple," he wrote in The Guardian. "I was being actively pursued by the military, who seemed single-mindedly determined to send me to fight, and possibly die, in Vietnam. I wanted to publish something that would express my anger."

The book, a precursor to more recent publications like "The Mujahideen Poisons Handbook" and "Minimanual of the Urban Guerrilla," was at times angry, but it also came with cautionary notes ("This book is not for children or morons") and common-sense tips, like one he appended to the 14 steps for manufacturing TNT.

"The temperatures used in the preparation of TNT are exact," he wrote, "and must be used as such. Do not estimate or use approximations. Buy a good centigrade thermometer."

In an interview at the time of the book's publication, Mr. Powell told The Bennington Banner in Vermont, "I don't see myself as crazed or bomb-throwing, though I could be if driven into a corner."

By 1971, when Lyle Stuart — considered a renegade for his belief that the American people had a right to read anything — published "The Anarchist Cookbook," Mr. Powell was attending Windham College in Putney, Vt. After graduation, he received a master's degree in English from Manhattanville College in Purchase, N.Y.

His early teaching focused on children with emotional and learning needs. He moved overseas in 1979 and worked in Saudi Arabia, Tanzania, Indonesia and Malaysia, teaching marginalized children and training teachers in how to better include them in the classroom.

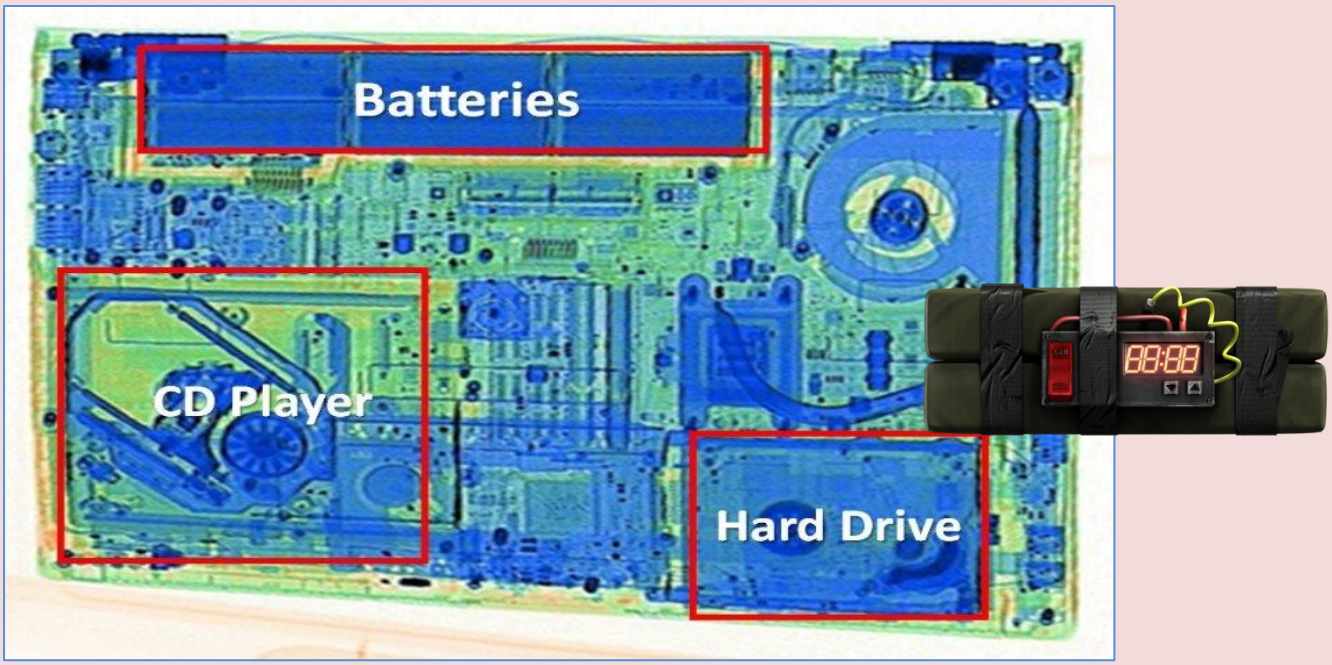
Sean Powell said in an interview that his father did not exile himself from the United States because of "The Anarchist Cookbook."

"The book came out in 1971," he said, "and he went to Saudi Arabia in 1979. Why would he take eight years to go into exile?"
In addition to his wife, the former Ochan Kusuma, and his son Sean, Mr. Powell is survived by another son, Colin; four grandchildren; a brother, Christopher; and his mother. His first marriage ended in divorce.
When "The Anarchist Cookbook" drew the attention of the F.B.I., agents were assigned to track which stores sold the book and to find out if William Powell was a pseudonym, according to the bureau's file on Mr. Powell. It noted a request by John W. Dean III, counsel to President Nixon, for a copy of the book.
But agents could find no reason to take action against Mr. Powell. Though he did, as the F.B.I. wrote, "submit for consideration recipes for nearly every type of explosive" whose manufacturer and distribution violated federal law, there was no evidence that he had been guilty of either.

Special Report – Laptops: Control, Alt or Delete?

By Philip Baum
Source: http://www.avsec.com/

Mar 27 - I have no doubt that there is sufficient intelligence out there to warrant concern over laptop computers or iPads concealing, and/or their lithium batteries being adapted to initiate, improvised explosive devices. Actually, we didn't even need the intel. It has long been public knowledge that the device that detonated on board Daallo Airlines flight 159 in February 2016 was concealed within a laptop and was probably activated by a passenger who had been given the device after he had gone through the screening checkpoint at Mogadishu Airport...by an airport insider.



Meanwhile, the intelligence community is worthy of praise for the number of plots that they have identified and for safeguarding the societies we live in. The aviation industry owes a debt of thanks to those individuals who interrupted the liquid explosive plot of 2006 and, in 2010, provided the very specific information that printers had been shipped from Yemen to the United States, via UPS and FedEx consignments, containing IEDs (concealed, as we later discovered, within the printer toner cartridges). These are just a few examples of the endeavours which have made aviation safer; there are plenty more 'finds' rightly hidden from the public.
When governments, or their security services, receive threat information, they have a duty to put in place measures that better protect us. It is often a thankless task where measures are implemented without those who design them being able to explain their rationale in any detail. All they can say is that, based on the information available, additional safeguards - often described as being proportionate in nature - are a necessity.

The restrictions introduced by the United States and United Kingdom governments on the carriage of laptops, and other devices, on flights from certain states (the list of items and countries varying either side of the Atlantic) must, one would hope, be based on increasing concern that additional modified devices are in circulation. That, I fear, is where the 'intelligence' process ends. The actual measures themselves defy common sense.

The best lesson the past has taught us is that next time it will be different. Each major bombing - or attempted bombing - this century has utilised a different way of infiltrating the device on board: shoes, underpants, liquids, printer toner cartridges, and, of course, laptops. Our aviation security system must be designed in such a way as to identify future attack scenarios.

There are numerous reasons why flights might be safer from a modified laptop, containing an IED, if it is in checked luggage rather than carry-on:

- the passenger is not able to initiate the device using a traditional control mechanism; the device is less likely to find itself next to the aircraft's fuselage and, therefore, any blast may be absorbed by the surrounding baggage and cargo (the Daallo bomb did not, due to the aircraft's low altitude at the time of detonation, cause the destruction of the airliner even though it was activated in a window seat near the fuel tanks);
- checked luggage screening systems around the world are more likely to be equipped with explosive detection technology that is not yet commonplace in cabin baggage inspection systems (frustratingly, the new measures have also served to highlight these shortcomings, which can now be exploited by those with terroristic intent); and,
- the screening process of checked luggage is much faster than that of cabin baggage, especially if greater focus is going to be placed on specific hand-carried electronic devices. Yet surely we need a response which ensures that no such device makes it onto the aircraft at all?

Let's consider the **Daallo Airlines incident** - and, indeed, the Metrojet bombing of 2015. Both tragedies were the result of insider threats. With Daallo, an airport employee literally handed over the device to the passenger thereby circumventing the passenger screening system. Were there to be direct flights from Somalia to the UK or the US, the latest restrictions would have had no effect whatsoever; the only people to be inconvenienced would have been those law-abiding passengers who checked their laptops into the hold. Now it may well be the case that it is partly because of concerns over 'insiders' that the US and UK do not operate flights to Somalia in the first place, but that does not answer the question as to why these latest restrictions only apply to certain routes.

Many of the departure points impacted by the latest restrictions are transportation hubs for onward connections to (and, more pertinently, from) places such as Somalia. Indeed, the intended target of the Daallo Airlines bomb was a Turkish Airlines flight. The likes of Emirates and Qatar Airways (impacted by the US regulations) certainly operate to locations where security concerns are considerable. Understandable, therefore, that overseas governments should want to address any loopholes resulting from suicidal passengers transferring onto flights at the seemingly safer Jordans, Turkeys and Moroccos of this world. But there are numerous other routes to the US and UK and, if the supposed device can be initiated by a suicide bomber, then they can also travel from Istanbul, Doha, or wherever, via other European, African or Middle Eastern cities not on the list.

There are a number of disturbing suppositions. Firstly that IEDs can always be detected in checked luggage - which they cannot - and secondly that our concern should be restricted to the electronic items listed. X-ray examination can yield positive results. In an incident almost beneath the media's radar on 2nd March, an improvised explosive device (or grenade) was detected at Egypt's Borg al-Arab Airport (Alexandria) in the luggage of a

Russian passenger bound, on Turkish Airlines, for Istanbul. Equally, sophisticated bombs can remain undetected; the printer toner cartridge bombs were not detected in the UK by a multitude of screening technologies, including explosive trace detection, and it was only a diligent Emirati security officer who, when screening the device sent via Dubai, opted not to rely on technology and to take the printer apart that resulted in the devices being identified. I obviously will not go into detail regarding the quantities and types of explosives governments are 'certifying' technologies to detect; suffice to say the presence of explosive detection technology does not necessarily equate with the guaranteed detection of real improvised explosive devices.

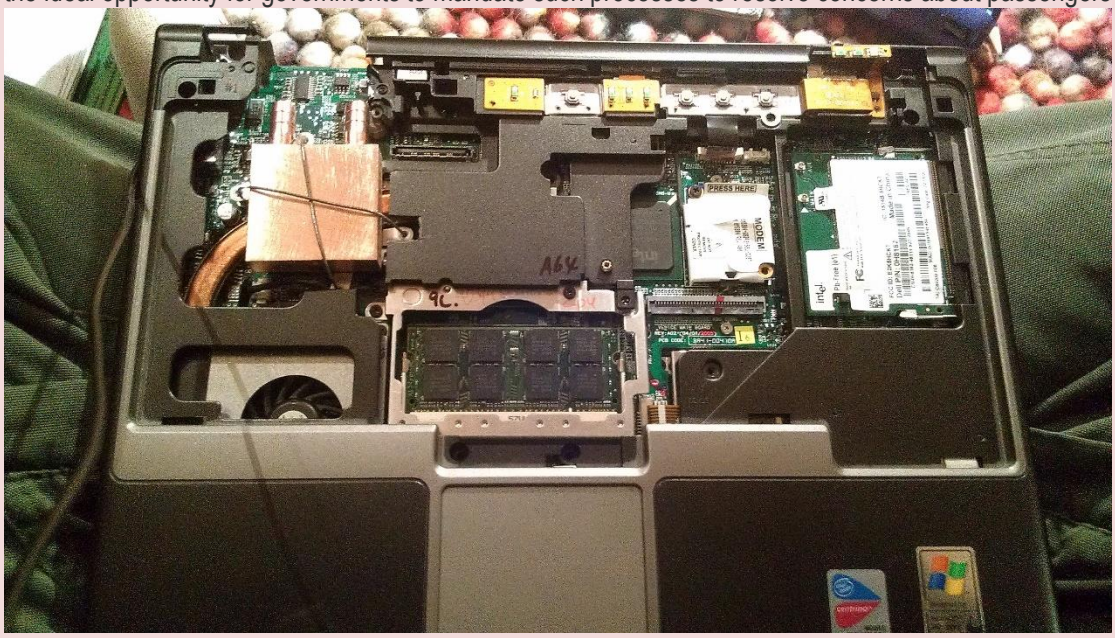
Above all of this, however, is the fact that the restrictions really are saying that bombs can only be detected by technology and not by humans. Global aviation security is really in a very sorry state of affairs if our checkpoint screeners cannot distinguish between a laptop-IED and a genuine laptop, or between an individual who is suicidal and one who is not. If the concerns are about electronic or electrical items, question passengers who are carrying them about their fidelity. If the concerns are only over laptops originating in certain countries, then don't implement restrictions on passengers who are not starting their journeys in those locations. Take, for example, a British business traveller heading to Istanbul on a city-break or an American family heading to Dubai, the former carrying a laptop, the latter a camera - why should they be inconvenienced? To ensure a level playing field? No, there's nothing 'level' about the new restrictions, or the airlines impacted. Regardless, in both examples it would be feasible to record the make and model number of the items as they leave the UK and US and, therefore, to permit those same items to be carried in cabin baggage on return flights. But we shouldn't even have to embark on such an arduous process...

There would be greater logic in restricting all cabin baggage on all routes (and I sincerely hope that does not happen), or even ceasing operations to all airports of concern; after all, the **restrictions do not address the insider threat at these airports, nor the potential for homegrown terrorists manufacturing similar devices in the US or UK and boarding flights with them,** as the liquid plot bombers would have done. The suicidal attack on Westminster, carried out on the first anniversary of the Zaventem bombings, clearly demonstrated that we cannot effectively monitor all those who may wish to attack us even if they live in Birmingham, let alone Mogadishu.

The restrictions actually enable terrorists to achieve their intended goal of disrupting our daily lives. This is not only bad news for travellers, who do need to be able to work on flights (a long-haul flight is, for me, the perfect office day; free to work, uninterrupted, on presentations, emails, spreadsheets and articles - including this one) and who rightly fear that their laptop, checked into the hold, might either not reach its destination or do so but no longer function (note how laptops are packaged for carriage when opening one fresh from the computer store). Consider also that the business traveller preferring to fly with carry-on baggage only now has to wait for their luggage at the reclaim belt, even if they are only a day trip to Istanbul! It is also bad news for airlines as yet another trigger for unruly passenger behaviour is introduced into the system. The restrictions on liquids, aerosols and gels, introduced nearly 11 years ago, were seen to be a cause for people becoming aggressive inflight. The electronics restrictions are far worse - one might bemoan the confiscation of a bottle of water, deodorant aerosol, premium quality perfume or avocado foot lotion, but the value of a laptop, which cannot be confiscated, is far greater and passengers are going to be spending hours worrying about their valuables concealed, out of sight, in the aircraft hold. That's to say nothing of the concern of being separated from the priceless data, which may be commercially or security sensitive in nature, contained on laptop hard drives. Many, of course, now unable to work, and feeling frustrated, will simply drink instead!

There are also practical considerations, especially if the restrictions are not global in nature. Take a passenger who checks in for a flight online, expecting only to carry hand-luggage, and who goes through a centralised screening checkpoint at one of the 'targeted' departure airports. Screeners are not going to be trying to identify these restricted items as they will be permitted on most routes, yet at the gate, where the destination becomes clear and secondary checks are performed, perhaps only 30 minutes before departure, the passenger suddenly finds that they cannot carry their laptop on board. What then? Too late to return to check-in. Are we just going to have even more bags checked-in at the gate? Sure, the passenger should have known, but just look at the number of them who are still having their LAGs confiscated at checkpoints 11 years after they were restricted. Regardless, the potential for flight delays and disgruntled passengers is significant and many

may opt not to fly at all. It would all be worth it if we were enhancing security as a result, but we are not! The laptop et al restrictions could yet become another LAGs debacle, whereby obviously genuine passengers are having to discard (or now check-in) harmless products in the name of tick-box security and screeners looking for restricted items rather than passengers and employees with negative intent. With the latest amendment to Annex 17 (to the Chicago Convention) set to recommend (sadly, not yet standardise) the introduction of behavioural analysis into the screening process, this would have been the ideal opportunity for governments to mandate such processes to resolve concerns about passengers



carrying specific items. Yet bizarrely we have opted to disconnect the passenger from their electronic items, making hand-search all the more difficult and the analysis of such items in the presence of their owner (comparing the item to the appearance and behaviour of the passenger) nigh on impossible. Illustrative of the abject failure to adopt a risk-based approach to screening, the US Department of Homeland Security seemingly can't even guarantee the integrity of its own employees, or their computers, and eliminate them from concern! On Its own website it states that, "The limits on the size of electronics in carry-on bags apply to all passengers, including U.S. government employees with U.S. government-issued laptops."

My original intention, for this [April] issue [of Aviation Security International], was to write more expansively about the assassination of Kim Jong-nam at Kuala Lumpur International Airport on 13 February when, allegedly in a North Korean-sponsored plot, two women attacked him in the check-in hall, one with a cloth laced with VX nerve gas. **It is a reminder that the chemical/biological weapons threat is one which requires our greater attention.** The global terrorist has, after all, previously copied Pyongyang-designed attacks and devices; it is now 30 years since KAL 858 was brought down by an IED. The perpetrators used liquid explosives (almost 20 years before the 'new' threat of liquid explosives) as part of the main charge and the IED was infiltrated on board on the flight by two people who had travelled a circuitous route to avoid detection. Clearly governments today are not concerned about terrorists travelling circuitous routes with laptop IEDs!

We must, of course, react to intel. There is concern that IEDs designed by the infamous bombmaker Ibrahim al-Asiri, such as on Daallo Airlines, might be used to target aviation again. But let's not forget that al-Asiri also developed the undetected printer toner cartridge bombs...and the body cavity device secreted inside his brother's body in an assassination attempt on Saudi Arabia's Deputy Minister of Interior in 2009. Perhaps we should also respond to the threat of the body bomb now if al-Asiri's inventions are of concern?

Then we could all become checked luggage!

Philip Baum *is Editor,* ***Aviation Security International****, and Author,* ***Violence in the Skies: A History of Aircraft Hijacking and Bombing*** *(Summersdale, 2016, and available in the USA on Amazon from 1 April 2017).*

ISIS car bomb factory discovered in Mosul where 'jihadis pack vehicles with deadly CHLORINE and paint trucks bright colours to fool US spy drones'

Source: http://www.dailymail.co.uk/news/article-4296488/ISIS-car-bomb-factory-jihadis-drones.html#ixzz4d1JBwGMm

Apr 02 – An ISIS car bomb factory with vehicles and explosives to cause mass destruction has been discovered in the Iraqi city of Mosul.

Iraqi soldiers found two cars and an armoured plated garbage truck destined to be used in suicide missions.

The truck had been spray-painted with bright red paint while the bodywork had been rendered in white - a new ISIS tactic to confuse US surveillance drones into thinking suicide car bombs are ordinary civilian vehicles.

During the offensive in east Mosul, most ISIS car bombs were either painted black or their steel bullet-proof metal sheets were left unpainted.

The truck's bodywork had been reinforced with thick steel sheets, designed to act as bullet-proofing to protect the driver traveling at high speed towards enemy positions.

Government troops made the terrifying discovery in the Josah district as they advanced into the western half of the city, where hundreds of thousands are still trapped under the terror group's control.

'These two car bombs were under construction and were almost ready to be loaded with explosives to be used against us, but Daesh didn't have time to deploy them before we liberated the area,' Heider, a soldier with Iraq's elite Rapid Response Division (ERD), told MailOnline.

'If it had been used, the rubbish truck would have created a massive explosion, easily destroying three houses,' he added.

Soldiers say this new strategy of painting lethal vehicle-borne improvised explosive device (VBIEDs) is designed to confuse aerial surveillance operations being carried out near the front-lines by US spy drones to delay the military response against car bombs.

'The US military are here with us on the front lines but not fighting, they are using drones to monitor Daesh activities, especially suicide car bombs,' said Iraqi soldier Mohammed.

'They have a big technologically-advanced drone which they constantly fly over areas we are advancing into, to check for incoming Daesh suicide car bombs.'

He explained that, when a car bomb is identified, co-ordinates are given to Iraqi and coalition warplanes, which then target them with airstrikes.

Since the Iraqi military started its operation to liberate West Mosul from ISIS in February, militants have continued to use car bombs and snipers as their main defence.

'Four suicide car bombs came at us yesterday, just on this one frontline,' said Mohammed. 'Three of them were stopped by airstrikes and our RPGs, but one of them blew up with a massive explosion when we hit it.

'Daesh have hidden suicide car bombs in covered areas in residential homes and garages so they can't be seen from the air,' he said. 'We fully expect that there will be a lot more suicide cars waiting for us, hidden in civilian homes.'

Weapon: The bullet proof car bombs are made with a small slit in the windscreen to prevent an ISIS suicide bomber being shot dead before completing their mission

A few streets away the driver of a a crumpled Honda VBIED was killed before he could detonate the vehicle. His car bomb stood by the side of the road, painted light blue to appear like a civilian car to drones flying overhead.

Fake windows and wheels had been painted on the side of the vehicle. A tiny slit had been cut into the windscreen to prevent the ISIS suicide bomber driver from being shot before completing his mission.

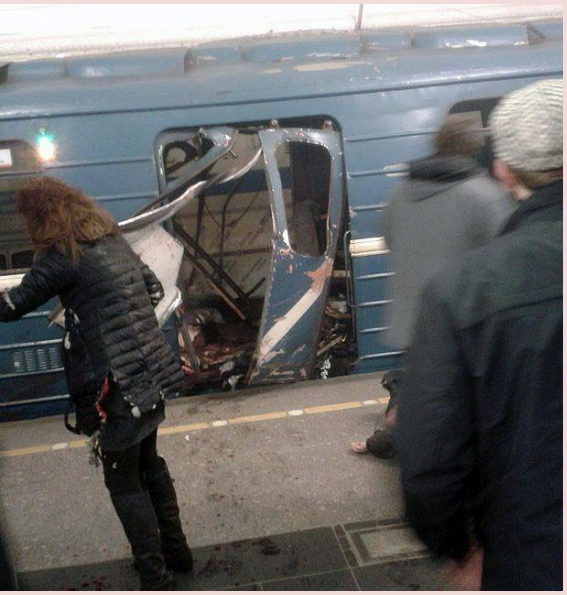
In the afternoon sunshine, the body of the militant driver, shot through the head, laid prostrate on the ground nearby. 'They are not people, they are just animals,' said Iraqi soldier Ahmed. 'They sent four car bombs for us yesterday. The day before there were ten, and we have already destroyed two today.'
In the bomb factory warehouse, officers from Iraq's Federal Police busily stripped the rubbish truck of its red and white metal panels.

One worker said they planned to use the parts on their own military vehicles, which are under constant threat from ISIS IEDs, suicide bombs and RPGs.
Engineers also found two chlorine canisters that ISIS reportedly use as a makeshift chemical weapon in their defence of Mosul, formerly their Iraq stronghold.
An ISIS car bomb painted in the same bright red shade as the rubbish truck recently seized by Iraqi forces was found fitted with chlorine canisters. Chlorine, first used as a chemical weapon by Germany in WWI causes instant death when inhaled.
'These are mortar rounds and plastic canisters containing diluted black oil, which ignite when the vehicle blows up and creates a huge fire,' soldier Heider explained.
Former CIA director John Brennan last year warned that ISIS had already used chemical weapons and have the capacity to make small quantities of deadly chlorine and mustard gas.
At a nearby public swimming pool commandeered by ISIS, several large chlorine tanks were discovered.
'These were meant for cleaning the swimming pool but ISIS have started using them as chemical weapons on their suicide vehicles,' said ERD lieutenant Walid.
'They fit these canisters onto the back of large suicide bomb cars and the chlorine canisters blow up, releasing a very dangerous gas when they detonate the vehicle,' he added.

11 killed in explosion on Saint Petersburg subway

Source: http://www.timesofisrael.com/at-least-10-dead-in-explosion-on-saint-petersburg-subway/

Apr 04/05 – Some 11 people were killed Monday in an explosion on the subway in Saint Petersburg, Russian authorities said.

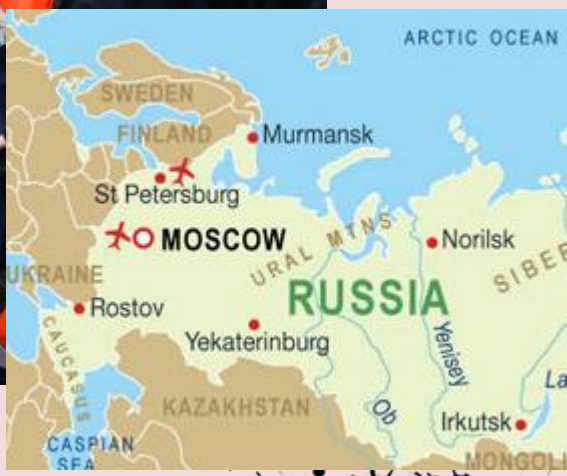


President Vladimir Putin, who was visiting the city on an unrelated trip Monday, said investigators were looking into whether the explosion was a terror attack or if there might have been some other cause. He offered his condolences to the families of those killed. Russia's National Anti-Terrorist Committee, which said "several" people were killed and injured, said an unidentified explosive device went off on a train that was traveling between two stations.

Andrei Kibitov, spokesman for the St. Petersburg governor, told Russian television 11 people were killed and over 50 injured in the subway explosion.

The blast occurred at the Technological Institute metro station's platform, a busy hub of the underground network in the center of Russia's second-largest city.

The subway's administration said several stations in the city were closed and that an evacuation was underway. Reports indicated that all stations in the city had been shut.



The Russian anti-terrorism committee said it had found and deactivated a bomb at another Saint Petersburg subway station.

Social media users posted photographs from the scene of the blast, showing people lying on the floor and a train with a mangled door nearby.

Russian Senator Viktor Ozerov told the Interfax agency that the explosion looked like a terrorist attack. Following the reports, the Moscow metro also announced that it was "taking additional security measures" as required by law in such situations, according to the network's official Twitter account.

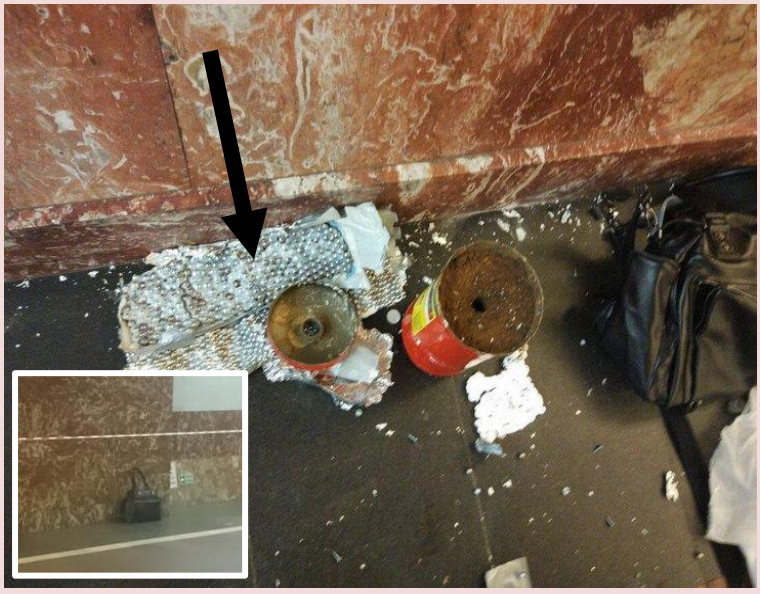
While there was no immediate indication as to what caused the blast, Russia's security services have previously said they had foiled "terrorist attacks" on Moscow's public transport system by militants, some of whom were trained by Islamic State jihadists in Syria.

And Russia's public transportation systems have been targeted by attacks in the past.

In 2013, Russia was hit by twin suicide strikes that claimed 34 lives and raised alarm over security at the Sochi Winter Olympic Games.

A bombing at the main railway station of the southern city of Volgograd killed 18 people on while a second strike hit a trolleybus and claimed 16 lives.

Is he the terrorist (CCTV capture) – 22 yo from Kazakstan?



◀ The second IED

A suicide raid on Moscow's Domodedovo airport that was claimed by Islamic insurgents from the North Caucasus killed 37 people in January 2011. That strike was claimed by the Caucasus Emirate movement of Islamist warlord Doku Umarov.

Russia beefed up its security over the holiday period

in the wake of the attack on the Berlin Christmas market that killed 12. Authorities placed heavy trucks at road intersections to block off areas where public festivities were taking place after the attack in the German capital that was claimed by the Islamic State group.

Russia has intervened militarily to bolster Syrian President Bashar al-Assad's forces in September 2015, turning the tables on the battlefield just as rebel forces were strengthening their hold on key areas.

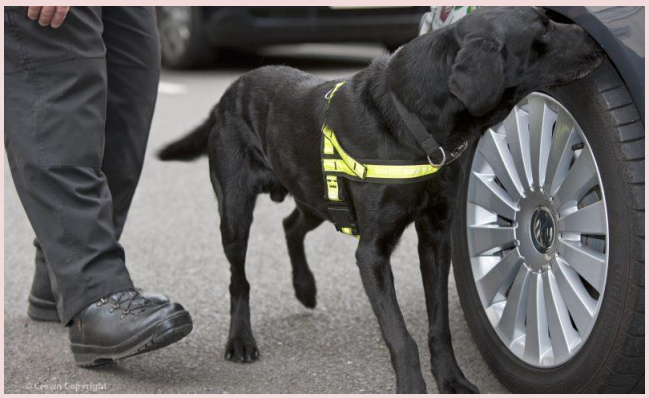
Russian bombardments helped the regime retake rebel areas in the east of the northern city of Aleppo after four years of fighting.

More than 310,000 people have been killed in Syria since the conflict broke out in March 2011 with protests against Assad's rule.

IED Detection – Have Trained K9 Finished their Role?

Source: http://i-hls.com/archives/75879

Apr 08 – The current threat environment of improvised explosive devices (IEDs) concealed on persons, in vehicles, and in the mail poses challenges for traditional explosive detection measures.



Around the world, security forces have depended on dogs to protect critical infrastructure, supply chains, and transportation assets. Specialised teams consisting of a trained K9 and a skilled handler are deployed to search for and detect explosives at static checkpoints and roving patrols. An article in army-technology.com tries to answer the question whether k9 dog detection squads are still the best option in an evolving frontline environment.

While these teams have been effective, they have significant limitations as dogs require intense training, expensive kennel facilities, quarantine for international travel, specialised food, and water. In certain environments, such as extreme heat and humidity, a K9's attention span and effectiveness may be reduced.

Explosive detection technologies such as X-ray and bulk visualisation equipment can fill a variety roles by using screening and minimally invasive processes The same devices may

also be equipped to identify the specific material. And new technologies now allow for the detection of trace amounts of explosives.

In general, K9s can only be trained to detect approximately ten different odors effectively, while some detection technologies, on the other hand, can detect a much wider range of threats including numerous types of explosives, toxic industrial chemicals, and even narcotics.

Some technologies, such as Raman spectroscopy devices, are equipped with threat libraries allowing them to identify hundreds or even thousands of hazardous substances and are modifiable and expandable with simple software updates.

Today, IEDs are a common and prevalent threat worldwide. They can be composed of commercial, military, or homemade explosives, or military ordnance and ordnance components concealed within various spaces.

As terrorist elements around the world continue to deploy IEDs as their most deadly weapon of choice in today's battlespace, numerous explosive detection solutions are increasingly fielded in transport hubs such as airport and seaports, and by security forces, to detect explosives threats at high-value locations.

Handheld and desktop Explosive Thread Detection (ETD) systems have proven to be the most operationally valuable equipment for modern security forces in detecting and defeating IEDs. The latest generation of ETD solutions offer an attractive solution to augment K9 assets, and in certain situations replace their use entirely.

Using particulate and vapour ETD in concert is a valuable capability, and many security forces are acquiring ETD technologies which such dual functionality, allowing them to field both solutions in one handheld toolbox.

ETD devices require minimal consumable resources to operate, have a lower operating cost and lower total cost of ownership, require little operator training, have no break-in period, and can be easily transported and replaced. In certain parts of the world, ETD screening may be less culturally disruptive than the introduction of K9 assets.

Oslo police detonate 'bomb-like device'; suspect in custody

Source: http://www.reuters.com/article/us-norway-police-idUSKBN17A0TS

Apr 09 – **Norwegian police set off a controlled explosion of a "bomb-like device" in central Oslo early on Sunday and were holding a suspect in custody in an investigation led by security police.**

A Reuters reporter described a loud bang shortly after Oslo's bomb squad arrived with a remote-controlled robot once the area was cordoned off by police late on Saturday night.

"The noise from the blast was louder than our explosives themselves would cause," a police spokesman said, adding that further investigation was needed to find out if the device had contained explosives.
The device, about 30 cm (1 ft) across, had appeared to be capable of causing only a limited amount of damage. Forensics experts will examine fragments to figure out what it was.
Police across the Nordic region have been on heightened alert after a truck ploughed into a crowd in Stockholm on Friday. Four people were killed and 15 injured in what police called an apparent terror attack.
Norwegian police detained a suspect but declined to give information about his identity. Norway's police security service, PST, said in a tweet it had taken over the investigation from local police.
"We're in a very early phase of the investigation," PST spokesman Martin Bernsen said. More details were likely later on Sunday, he added.
Police took away cordons put up overnight in the Groenland area and residents resumed normal Sunday activities, with shops and cafes open. There was no sign of police at the site.
The **Groenland area** (photo), a multi-ethnic neighbourhood that is home to popular bars and restaurants,

several mosques, and the city's main police station. The police station is less than a kilometre away from where the device was found.
In 2011, right-wing extremist Anders Behring Breivik set off a car bomb in Oslo that killed eight people and destroyed Norway's government headquarters, before going on a shooting rampage that killed 69 people at nearby Utoeya island.

Egypt: Isis claims responsibility for Coptic church bombings

Source: https://www.theguardian.com/world/2017/apr/09/egypt-coptic-church-bombing-death-toll-rises-tanta-cairo

Apr 09 – **Isis has claimed responsibility for two bomb blasts that struck Coptic churches in Egypt, killing at least 47 people as members of the country's largest religious minority celebrated Palm Sunday.**

An explosion in the city of Tanta, about 56 miles (90km) north of Cairo killed 29 and injured 71 as they prayed at the Mar Girgis church according to the Egyptian health ministry. A second blast struck the Egyptian port city of

Alexandria three hours later, killing 18 and wounding 35.

The bombings were the latest in a series of attacks on Egypt's Christian minority, who account for about 10% of the population and have been repeatedly targeted by Islamic extremists. The attacks come weeks before Pope Francis is due to visit Egypt.

Egypt's president Abdel Fattah el-Sisi announced a three-month state of emergency on Sunday night in response to the bombings after meeting his national security chiefs.

Video from the moment the blast struck the Mar Girgis church in Tanta just before 10am on Sunday showed the sounds of a choir gathered to sing hymns celebrating the Christian holy day, rapidly turning to screams of anguish and panic.

Egypt's state television later reported that a bomb planted under one of the pews ripped through the church.

"As I was passing by the church, I heard a huge blast – I'd never heard a sound like this," said Salah el Arby, a taxi driver in the town of Tanta. "People began running out of the church – shouting and afraid."

"I believe this attack was the fault of the security forces," he continued, citing a bomb previously diffused by police at Mar Girgis church in the town on the 29 March. "The police didn't protect the church on an important day like today."

Gruesome images circulated on social media in the aftermath of the blast, showing blood-stained woven palm branches, of the kind traditionally carried to celebrate Palm Sunday. Churches across Egypt had anticipated a higher than average attendance to celebrate the holiday.

The second blast in the Egyptian port city of Alexandria struck St Marks Coptic Orthodox church came three hours later. Egyptian state media reported that Coptic Pope Tawadros II was inside the church when the explosion struck, after leading worshippers in Palm Sunday prayers.

Three policeman were killed as they tried to prevent the suicide bomber from entering St Marks Cathedral in Alexandria, including one who embraced the suicide bomber just 100 metres from the Cathedral, preventing him from entering.

"Although there was a police constable who hugged the person holding the explosive belt to stop him entering the church, at the same time we cannot ignore the

fatal mistakes by the security authorities that let this many attacks happen in a short time," said Haitham al Hariri, a member of parliament with the Socialist Popular Alliance.

"If a bomb had been placed under the seat in Alexandria while the Pope was speaking as it was in Tanta, this would have been an even bigger disaster."

Speaking to the Guardian from the Amiri public hospital where victims of the blast had been taken, he said: "I'm here in the hospital and people are angry at me - and angry at every official in this country. Families here are disappointed, frustrated and angry at everyone with no exception – from the head to lowest in the state."

Despite the efforts of Egyptian security forces on the ground at the site of each attack, a day of intense violence left Coptic Christians asking whether they are safe in Egypt despite the government's pledge to protect them.

The twin attacks, timed for a day of Christian worship, come following months of attacks on Egypt's Coptic minority. St Peter and St Paul's church in the St Marks Cathedral compound in Cairo witnessed a similar attack in December 2016, in which a suicide bomber was able to enter the church, killing 29 people as they worshipped there by placing a bomb under a pew. When claiming responsibility for the attack in February this year, Isis vowed to "liberate" Cairo and threatened Christians across Egypt.

News of the bombings came as Francis was marking Palm Sunday in St Peter's Square.

The pontiff asked God "to convert the hearts of those who spread terror, violence and death, and also the hearts of those who make and traffic in weapons".

The Egyptian president Abdel-Fatah al Sisi said in a statement that the blasts "will not undermine the resolve and true will of the Egyptian people to counter the forces of evil, but will only harden their determination to move forward on their trajectory to realise security, stability and comprehensive development."

Christians have been increasingly targeted in Egypt following the overthrow of former Islamist president Mohammed Morsi in 2013. December's attack was followed by increasing attacks on Coptic Christians in the Sinai Peninsula, causing some 250 Christians to flee the northern Sinai town of Arish.

"The problem is that there is a virulently anti-Christian sentiment among radical Islamists and there is unfortunately no failsafe way to protect everyone all the time. This is unfortunately true in countries around the world," said H.A Hellyer of the Royal United Services Institute.

"It's not the first time Christians in Egypt have witnessed attacks like this," said Mina Thabet, a specialist in religious minorities at the Cairo-based Egyptian Commission for Rights and Freedoms. "They feel that no one is providing them with the necessary protection."

"The government is responsible for their security," he said. "Combating terrorism isn't just about force, it needs a new strategy – and Christians are paying the price."

"Two explosions in the same day are organised," he continued, saying that the close timing of the attacks suggests that the attackers coordinated with one another to plan the attacks. "It happened today and it could happen tomorrow," he said.

Egypt bombing: Tributes pour in for hijabi police officer who died trying to protect Christians

Source: http://www.independent.co.uk/news/world/middle-east/egypt-bombing-hijab-police-officer-nagwa-abdel-aleem-church-protect-christians-killed-explosions-a7676606.html

Apr 09 – Egyptians have been paying their respects to a woman police officer who died when she stopped an Isis suicide bomber from entering a Coptic Church in Alexandria.

At least 44 people were killed in two bombings targeting Egypt's Christian minority on Sunday - the first at St George's Church in Tanta, about 60 miles (100 kilometres) north of Cairo, followed by the explosion during Mass at Alexandria's Saint Mark's Cathedral.

Nagwa Abdel-Aleem, 55, was guarding the entrance to the church when the suicide bomber attempted to pass her security check. Unable to proceed any further, he detonated the bomb at the main gate. It is thought the attacker's primary target was Pope Tawadros II, who had left the site a few minutes earlier.

Ms Abdel-Aleem is the first woman to die in the line of duty in Egypt's police force. Egyptian media reported that one of Ms Abdel-Aleem's two sons, also a police officer, also died in the incident (small photo – right).

Pictures of her alongside her husband, an army lieutenant, have been widely circulated on social media, along with messages of thanks and blessings.

Egypt's Christian minority - around 10 per cent of the 90 million strong population - is the frequent targets of Islamist groups around the country as well as Isis-affiliated militants in the Sinai, which have flourished in the chaos that has engulfed Egypt since the 2011 revolution.

Letter Found After Borussia Dortmund Bus Attack Demands Pullback in Syria

Source: https://www.nytimes.com/2017/04/12/world/europe/borussia-dortmund-explosion-bus-germany.html

Apr 12 – A letter that was found after explosions damaged the team bus of one of Germany's premier soccer teams called for the country to scale back its involvement in the Western military coalition in Syria, the authorities said on Wednesday.

Frauke Köhler, a spokeswoman for the Federal Prosecutor's Office of Germany, also said that two people with an "Islamist background" had been taken into custody after an attack on the Borussia Dortmund bus Tuesday evening when the team was traveling to its stadium for a Champions League match against A.S. Monaco.

The game was postponed and kicked off Wednesday night at a packed stadium in Dortmund under tightened security.

Ms. Köhler said the letter demanded that Germany withdraw its Tornado aircraft from the campaign in Syria, where they are used for reconnaissance and where the Islamic State is under attack from a multinational coalition trying to push it from its strongholds.

The letter also demanded what it termed "the closure of the Ramstein Air Base," Ms. Köhler said, a reference to the main airport for American and NATO military forces in Germany.

The letter, which the German news media said was written in slightly awkward, nonnative German, blamed Chancellor Angela Merkel for taking part in actions against Islamists and demanded an end to attacks.

"From this point on," it said, "all nonbelieving actors, singers, sports people and other prominent people in Germany and other crusader nations are on the death list of the Islamic

State. And that as long as the following demands are not met: Tornados out of Syria. Ramstein Air Base must be closed."

The unusually specific set of demands came with no claim of responsibility, but it was being examined by experts, Ms. Köhler said. The Federal Prosecutor's Office has taken charge of the investigation.

She provided no details about the two people who had been taken into custody beyond saying they were "from the Islamist spectrum," and she said the prosecutor would decide whether to apply for a warrant to keep at least one of them in detention.

The German news media described that suspect as a 25-year-old Iraqi man who was detained in the town of Wuppertal, about 40 miles southwest of Dortmund. The other suspect is 28 and from Unna, just east of Dortmund, the German news agency DPA reported. Investigators searched the homes of both men, Ms. Köhler said.

She also said a second document had turned up on the website linksunten.indymedia.org hinting that a far-left group might be responsible for the attack. However, she said, "There are considerable doubts about this claim."

Investigators have not determined exactly what type of detonator or what explosive was used, she said.

The Interpreter Newsletter

Understand the world with sharp insight and commentary on the major news stories of the week.

The bus was "heavily damaged" in the explosion on Tuesday, Ms. Köhler said, and a more serious outcome was narrowly avoided. A piece of metal said to be part of the explosive devices had lodged in the headrest of a seat on the bus, she said, but she did not specify whether that seat had been occupied.

Her statements suggested a carefully planned attack on Europe's most popular sport and a match between two of the Continent's best teams, which would attract attention in its two biggest countries, Germany and France.

"Football has a big fascination, and that is why it also exerts a temptation on terrorists, to abuse that effect," Thomas de Maizière, Germany's interior minister and the country's most senior security official, told reporters at the stadium.

"People will have to get used to discomforts," he added, "but not to the abolition of the freedom we would relinquish if we call off everything."

One player was injured in Tuesday's explosion, the Spanish defender Marc Bartra. He has had surgery on his right wrist, and team officials said he was recovering.

Ms. Merkel, an avid soccer fan, condemned what she called the "repulsive act." Balanced against that, she said, was the good will of supporters from both Dortmund and Monaco — Germans welcomed Monaco fans into their homes with the hashtag #bedforawayfans on Twitter — which she called "a clear signal against every sort of violence."

The authorities in North Rhine-Westphalia, which is Germany's biggest state and includes Dortmund, promised tight security Wednesday night. Soccer fans were advised not to bring

backpacks to the stadium, which is Germany's largest with a capacity of more than 80,000 people, and to arrive early because of strict security checks.
Wednesday's match began less than 24 hours after the explosion — a tight reshuffle dictated by a crowded soccer calendar at this time of year. Dortmund's fans, known for their boisterous singing and extreme devotion to the team, welcomed their squad to the field with a rousing version of the song "You'll Never Walk Alone." Politicians filled the V.I.P. stands to highlight the message that terrorism will not get the better of ordinary Germans.
After a tentative start, Dortmund ended the first half behind by a score of 2-0. The home team was especially spirited in the second half, but failed to close the gap, finally losing, 3-2, to Monaco.
Security was also tightened significantly at two other Champions League matches on Wednesday: in Munich, where Bayern Munich played Real Madrid, and in Madrid, where Atlético Madrid hosted Leicester City.

EDITOR'S COMMENT: Bus triple glasses saved lives – perhaps coated with an anti-vandal film? There is also a report about two holes on bus body – bombing + shooting? Another report indicates that explosives in the pipe-bombs were similar to those used by German Armed Forces (?) Who did it? Jihadists? Anti-nazi group? Huligans? Roadside IEDs require certin knowledge and field experience that ordinary criminals lack. It would be interesting to know more about this unique incident – the first of its kind in Europe but always there is a first for terrorist actions. **UPDATE:** It was a bomb-fo-profit incident (stock market gabling) – another first (read more in following pages)!

Iraqi, German suspects held over team bus attack in Germany

Source: http://www.thebaghdadpost.com/en/story/9276/Iraqi-German-suspects-held-over-team-bus-attack-in-Germany

Apr 12 – German police have detained a suspect with "Islamist links" following a bomb attack on the bus of the Borussia Dortmund football team, the BBC reported on Wednesday.
Prosecutors also said the three explosive devices contained metal pieces.
Two letters claiming the attack on Tuesday evening were being investigated, they said.
Prosecutors are treating the blasts as a terrorist attack but say the precise motive is unclear at present.

Glowing bacteria detect buried landmines, unexploded ordnance

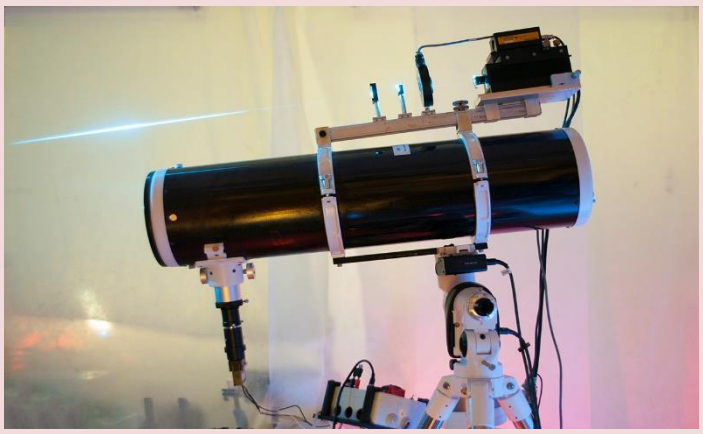
Source: http://www.homelandsecuritynewswire.com/dr20170412-glowing-bacteria-detect-buried-landmines-unexploded-ordnance

Apr 12 – The need for safe and efficient technologies for detecting buried landmines and unexploded ordnance is a humanitarian issue of immense global proportions. **About half a million people around the world are suffering from mine-inflicted injuries, and each year an additional 15 to 20 thousand more people are injured or killed by these devices. More than 100 million such devices are still buried in over seventy countries.**

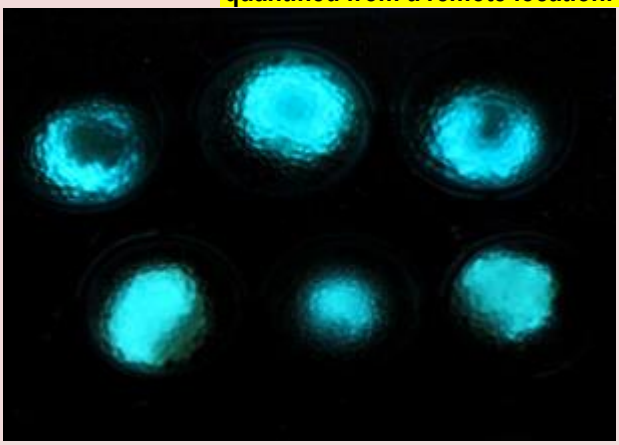
The major technical challenge in clearing minefields is detecting the mines. The technologies used today are not much different from those used in the Second World War, requiring detection teams to risk life and limb by physically entering the minefields. Clearly,

there is a critical need for an efficient solution for the remote detection of buried landmines and unexploded ordnance.

HUJI says that researchers from the Hebrew University of Jerusalem now report a potential answer to this need. Writing in the journal *Nature Biotechnology*, they present a novel, functional system combining lasers and bacteria to remotely map the location of buried landmines and unexploded ordnance.



The system is based on the observation that all landmines leak minute quantities of explosive vapors, which accumulate in the soil above them and serve as markers for their presence. The researchers molecularly engineered live bacteria that emit a fluorescent signal when they come into contact with these vapors. This signal can be recorded and quantified from a remote location.



The bacteria were encapsulated in small polymeric beads, which were scattered across the surface of a test field in which real antipersonnel landmines were buried. Using a laser-based scanning system, the test field was remotely scanned and the location of the buried landmines was determined. This appear to be the first demonstration of a functional standoff landmine detection system.

"Our field data show that engineered biosensors may be useful in a landmine detection system. For this to be possible, several challenges need to be overcome, such as enhancing the sensitivity and stability of the sensor bacteria, improving scanning speeds to cover large areas, and making the scanning apparatus more compact so it can be used on board a light unmanned aircraft or drone," said Prof. Shimshon Belkin, from the Hebrew University's Alexander Silberman Institute of Life Sciences, who was responsible for genetically engineering the bacterial sensors.

— Read more in Shimshon Belkin et al., "Remote detection of buried landmines using a bacterial sensor," Nature Biotechnology 35, no. 4 (11 April 2017): 308-10 (DOI: 10.1038/nbt.3791).

US drops largest non-nuclear bomb in Afghanistan

Source: http://edition.cnn.com/2017/04/13/politics/afghanistan-isis-moab-bomb/index.html

Apr 14 – The US military dropped America's most powerful non-nuclear bomb on ISIS targets in Afghanistan Thursday, the first time this type of weapon has been used in battle, according to US officials. **A GBU-43/B Massive Ordnance Air Blast Bomb (MOAB), nicknamed the "mother of all bombs," was dropped at 7:32 p.m. local time, according to four US military officials with direct knowledge of the mission. A MOAB is a 30-foot-long, 21,600-pound, GPS-guided munition.**

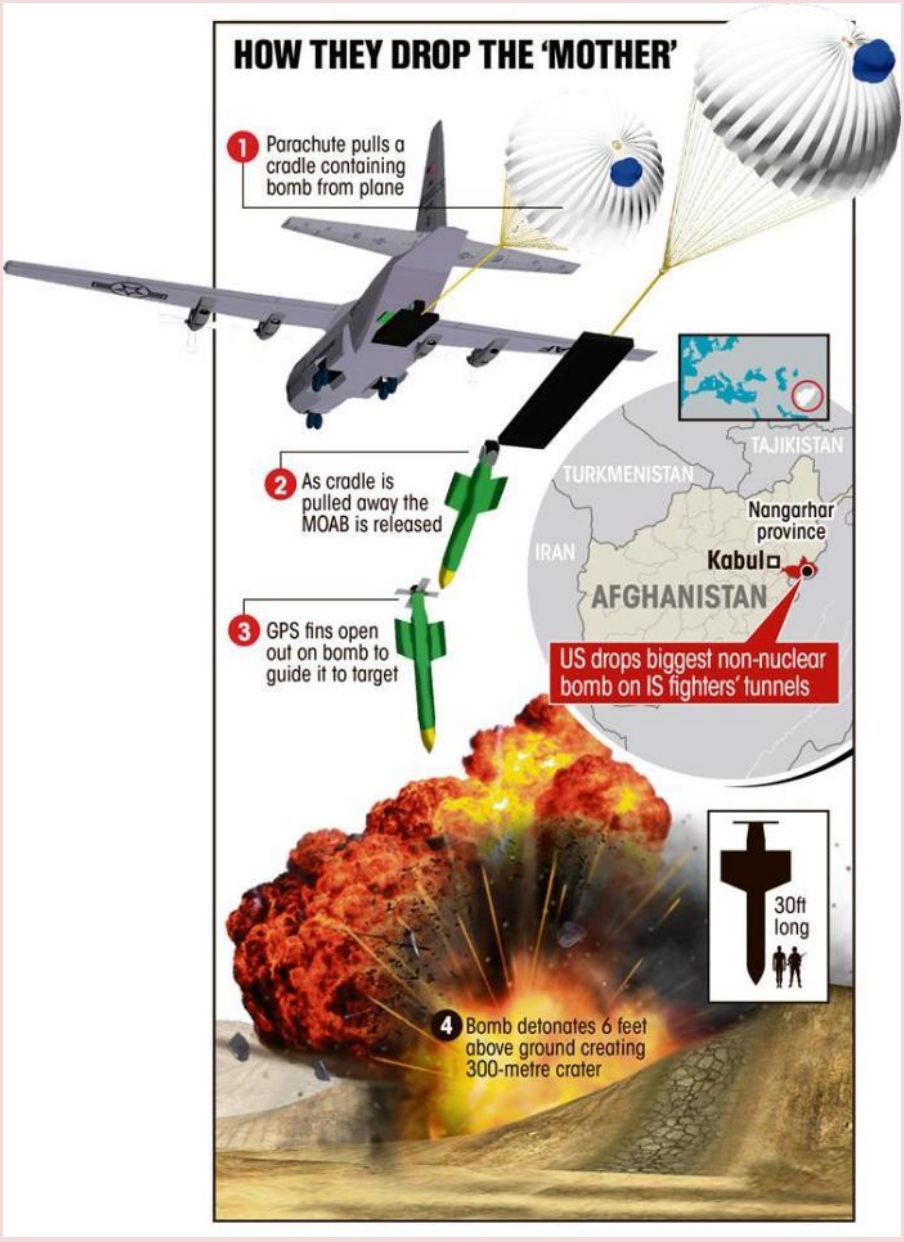
The bomb was dropped by an **MC-130 aircraft**, stationed in Afghanistan and operated by Air Force Special Operations Command, Pentagon spokesman Adam Stump told CNN.

Officials said the target was an ISIS cave and tunnel complex and personnel in the Achin district of the Nangarhar province, a remote area in the country's east which borders Pakistan.

"The United States takes the fight against ISIS very seriously and in order to defeat the group we must deny them operational space, which we did," White House press secretary Sean Spicer said later Thursday. The strike "targeted a system of tunnels and cave that ISIS fighters use to move around freely."
Afghanistan's ambassador to the US, Hamdullah Mohib, told CNN's Brooke Baldwin that the bomb was dropped after fighting had intensified over the last week between US Special Forces and Afghan troops against ISIS.

The US and Afghan forces were unable to advance because ISIS had mined the area with explosives, so the bomb was dropped to clear the tunnels, Mohib said.
Trump declined to say whether he personally signed off on the strike, but did comment, "Everybody knows exactly what happens. So, what I do is I authorize our military."
He continued, "We have given them total authorization and that's what they're doing."
Asked about Trump's "total authorization" comments, a senior administration official declined to specify whether the President indeed ordered the strike in Afghanistan.
But the official said that in general, "We don't approve every strike," adding that, "This administration has moved further away" from dictating military strategy from the White House.
It's a change both Trump and Defense Secretary James Mattis wanted, the official said.
The President has granted military commanders broader latitude to act independently on several battlefields where US forces are involved, which Trump touted as making a "tremendous difference" in the fight against ISIS.
During the campaign, Trump vowed to eradicate ISIS, saying he would "bomb the s**t" out of the terror group, also known as ISIL.
Republican hawks were quick to voice their support for the strike Thursday.
"I hope America's adversaries are watching & now understand there's a new sheriff in town," tweeted Sen. Lindsey Graham, a South Carolina Republican. "Pleased Air Force dropped MOAB against ISIL in Afghanistan. Must be more aggressive against ISIL everywhere - including Afghanistan."
But California Democrat Rep. Jackie Speier voiced concerns about potentially increasing US military involvement in Afghanistan.
"We are escalating in an area I think we should be deescalating in," she told CNN's Wolf Blitzer. "Coupled with what happened in Yemen, what happened in Syria, these are efforts

that are made to suggest that we will be engaging in wars in three different countries simultaneously."
Gen. John Nicholson, commander of US forces in Afghanistan, signed off on the use of the bomb, according to the sources. The authority to deploy the weapon was granted to Nicholson by the commander of US Central Command, Gen. Joseph Votel, Stump said.
This is the first time a MOAB has been used in the battlefield, according to the US officials. This munition was developed during the Iraq war and is an air blast-type warhead that explodes before hitting the ground in order to project a a massive blast to all sides.
During the final stages of testing in 2003, military officials told CNN that the MOAB was mainly conceived as a weapon employed for "psychological operations." Military officials said they hoped the MOAB would create such a huge blast that it would rattle Iraqi troops and pressure them into surrendering or not even fighting.



As originally conceived, the MOAB was to be used against large formations of troops and equipment or hardened above-ground bunkers. The target set has also been expanded to include targets buried under softer surfaces, like caves or tunnels.
But while the MOAB bomb detonates with the power of 18,000 pounds of tritonal explosives, the size of its explosion pales in comparison to that of a nuclear bomb.
Former Defense Secretary William Perry described the stark difference in power between a MOAB and nuclear bomb.
"The #MOAB explosive yield is 0.011 kilotons, typical nuclear yield is 10-180 kilotons - the US alone possesses over 7000 nuclear weapons," he tweeted.
"As ISIS-K's losses have mounted, they are using IEDs, bunkers and tunnels to thicken their defense," Nicholson said in a statement following the strike.
"This is the right munition to reduce these obstacles and maintain the momentum of our offensive against ISIS-K," Nicholson added.
"US forces took every precaution to avoid civilian casualties with this strike. US Forces will continue offensive operations until ISIS-K is destroyed in Afghanistan," read the statement from US Forces Afghanistan.
The extent of the damage and whether anyone was killed is not yet clear. The military is currently conducting an assessment. (**UPDATE** DEBKAfile: 90 Talibans were killed)
The Pentagon is currently reviewing whether to deploy additional trainers to Afghanistan to help bolster US allies there.
The Achin district is the primary center of ISIS activity in Afghanistan. A US Army Special Forces soldier was killed fighting the terror group there Saturday.

There are about 8,400 US troops in Afghanistan and they regularly perform counterterrorism operations against ISIS in the Nangarhar Province.
The US counterterrorism mission is separate from the NATO-led effort to train, advise and assist the Afghan army and police force.
While ISIS is identified primarily with its presence in Iraq and Syria, US and coalition officials have long expressed concern about a growing presence in Afghanistan.
ISIS first emerged in the summer of 2015 in the country's east, fast gaining ground and support, often among disaffected Taliban or Afghan youth.
US military officials have said the ISIS branch is largely comprised of former members of regional terror groups, including the Pakistani Taliban and Islamic Movement of Uzbekistan.
A US official told CNN that the military estimates are that the Afghan affiliate of ISIS has about 600 to 800 fighters, primarily based in two to three districts in southern Nangarhar. There are also a small number of ISIS operatives in Kunar province as well, the official added.
The Afghan offshoot's link to the organization's Syria-based leadership has been questioned. Many say in fact the Afghan ISIS fighters came from Pakistan and adopted the group's branding in order to get financing.

But every bomb has a FATHER as well!

Putin's monster explosive is known officially as the Aviation Thermobaric Bomb of Increased Power and is reportedly four times bigger than MOAB.

Father Of All Bombs	Mother Of All Bombs
Mass: 7.1 tons	Mass: 8.2 tons
TNT equivalent: 44 tons (88,000lbs)	TNT equivalent: 11 tons (21,600lbs)
Blast radius: 300 metres (984ft)	Blast radius: 150 metres (492ft)
Guidance: INS/GPS	Guidance: GLONASS

It carries 44 tons of TNT and explodes in the same way as its American counterpart, obliterating anything within the blast zone, collapsing buildings and producing huge blasts and aftershocks.
Although - like the MOAB - it is not nuclear, the aftermath of the bomb could be comparable to a nuke being deployed.

NOTE: B61-12 gravity nuclear bomb was tested (March 14, 2017) at Tonopah Test Range, Nevada

(USA) dropped from an F-16 aircraft.

Bombing of Syrian bus convoy kills dozens outside Aleppo

Source: http://www.reuters.com/article/us-mideast-crisis-syria-idUSKBN17H04Y

Apr 15 – A bomb blast hit a bus convoy waiting to cross into government-held Aleppo in Syria on Saturday, killing dozens of people evacuated from two Shi'ite villages the day before in a deal between warring sides.

The agreement had stalled, leaving thousands of people from both government-besieged and rebel-besieged areas stranded at two transit points on the city's outskirts, before the explosion occurred.

Late on Saturday buses began crossing into both government-held and rebel-held territory from the two transit points as the deal resumed, pro-Damascus media and the Syrian Observatory for Human Rights monitoring group reported.

But the incident underscored the difficulty carrying out any agreement between warring sides in a volatile and complex Syrian conflict which, in its seventh year, shows no signs of easing.

A media unit run by Damascus ally Hezbollah said the attack was carried out by a suicide car bomb and killed at least 40 people. The Observatory said more than 24 were killed and scores more wounded. (**Latest updates** speak about 126 dead – 68 children).

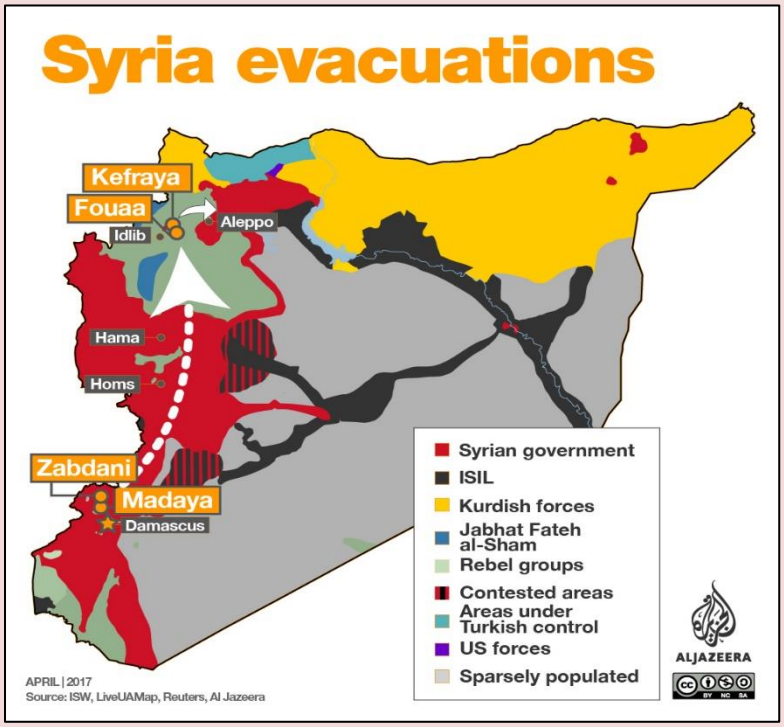
Footage on state TV showed bodies lying next to charred buses with their windows blown out, and vehicles in flames.

The blast hit buses in the Rashidin area on Aleppo's outskirts. The vehicles had been waiting since Friday to cross from rebel-held territory into the government-controlled city itself. Ambulances later took the wounded to hospital in Aleppo.

The convoy was carrying residents and pro-government fighters from the Shi'ite villages of al-Foua and Kefraya, which are besieged by

rebels in nearby Idlib province, an insurgent stronghold.

They had left under a deal where, in exchange, hundreds of Sunni insurgents and their families were granted safe passage from Madaya, a government-besieged town near Damascus.
But a delay in the agreement had left all those evacuated stuck at transit points on Aleppo's outskirts since late on Friday.



Residents of al-Foua and Kefraya waited in the Rashidin area.
Rebels and residents of Madaya meanwhile waited at the government-held Ramousah bus garage, a few miles away. They were to be transported to Idlib.

People waiting in the Ramousah garage heard the blast, and said they feared revenge attacks by pro-government forces. They circulated a statement on social media imploring "international organizations" to intervene so the situation did not escalate.
The evacuation deal is one of several over recent months that has seen President Bashar al-Assad's government take back control of areas long besieged by his forces and their allies.
The deals are unpopular with the Syrian opposition, who say they amount to forced displacement of Assad's opponents from Syria's main urban centers in the west of the country.
They are also causing demographic changes because those who are displaced are usually Sunni Muslims, like most of the opposition. Assad is from the minority Alawite sect and is supported by Shi'ite regional allies.
It was unclear who carried out Saturday's bombing attack.
The exact reasons for the delay in completing the evacuation deal were also unclear.

Forced displacement

The Observatory said the delay was caused by the fact that rebels from Zabadani, another town near Damascus included in the deal, had not yet been granted safe passage out.
A pro-opposition activist said insurgents blamed the delay partly on the fact that a smaller number of

pro-government fighters had left the Shi'ite villages than was agreed.

Earlier on Saturday, at the transit point where the buses from al-Foua and Kefraya were waiting, one resident said he was not yet sure where he would live.

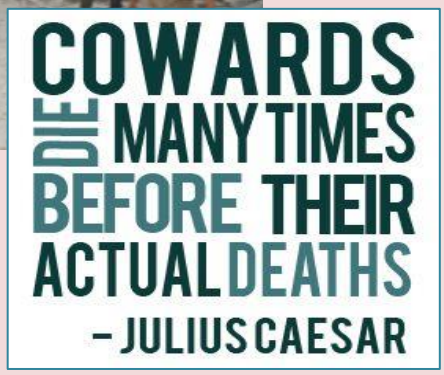
"After Aleppo I'll see what the rest of the group is doing, if there are any preparations. My house, land and belongings are all in al-Foua," Mehdi Tahhan said.

A Madaya resident, speaking from the bus garage inside Aleppo, said people had been waiting there since late on Friday, and were not being allowed to leave.

"There's no drinking water or food. The bus garage is small so there's not much space to move around," Ahmed, 24, said.

"We're sad and angry about what has happened," he said. Many people felt that they had been forced to leave," he said.

"There was no other choice in the end - we were besieged inside a small area in Madaya."



Other evacuation deals in recent months have included areas of Aleppo and a district in the city of Homs.

Syria's population is mostly Sunni. Assad's Alawite religious minority is often considered an offshoot of Shi'ite Islam.

He has been backed militarily by Russia, and by Shi'ite fighters from Iran and the Lebanese Hezbollah group in Syria's six-year-old conflict.

Assad has the military advantage over rebels in the west thanks to Russia's intervention in 2015, although the insurgents are still fighting back and have made gains in some areas.

Mine-sweeping equipment to be donated to fight IS

Source: http://www.taipeitimes.com/News/taiwan/archives/2017/04/18/2003668939

Apr 18 – **Taiwan is preparing to donate US$500,000 in mine-weeping equipment to the coalition fighting the Islamic State (IS) group,** Deputy Minister of National Defense Cheng De-mei (鄭德美) said yesterday at a legislative hearing that highlighted the challenges posed by the nation's continued exclusion from international terrorist intelligence databases.

Cheng made the remarks in response to questions by Democratic Progressive Party (DPP) Legislator Tsai Shih-ying (蔡適應) at a hearing of the legislature's Foreign and National Defense Committee on anti-terrorism measures as Taipei prepares to host the Summer Universiade in August.

The mine-sweeping equipment has been prepared, Cheng said, adding that the Ministry of Foreign Affairs is in the process of coordinating the donation.

Several legislators expressed concern over whether the government is receiving adequate intelligence to prevent a possible terrorist attack during the Universiade.

"There is no way for us to access information on lost or missing passports and travel documents, except indirectly through other governments," DPP Legislator Lo Chih-cheng (羅致政) said, adding that the nation's exclusion from Interpol denied it access to key crime and terrorism databases.

Deputy Minister of Foreign Affairs Francois Wu (吳志忠) said while the Interpol has rejected Taiwan's requests to access the databases, the European Police Office (Europol) has given a more positive response and individual governments have shared information from their databases.

However, the nation continues to lack real-time access to Interpol databases, he said.

National Police Agency Deputy Director-General Chou Wen-ke (周文科) said that Tokyo has supplied Taipei with information from its Interpol databases.

In response to a question by Chinese Nationalist Party (KMT) Legislator Johnny Chiang (江啟臣), National Security Bureau Director-General Peng Sheng-chu (彭勝竹) said that the US has provided anti-terrorism training to Taiwanese law enforcement units to prevent a possible attack during the Universiade and will send observers to monitor drills.

Bomb outside Athens bank causes minor damage, no injuries

Source: http://abcnews.go.com/International/wireStory/bomb-athens-bank-minor-damage-injuries-46896349

Apr 19 – A bomb exploded outside a bank in central Athens late Wednesday, causing minor damage to the building but no injuries, authorities said.
Officials said the explosion followed an anonymous warning call to a private Greek television station and police were able to evacuate the area before the bomb detonated.
A police statement said the device was left in a bag outside the entrance to the bank, which is close to two busy avenues.
No group claimed responsibility for the attack. Similar bombings in the past have been claimed by extreme left or anarchist groups.

EDITOR'S COMMENTS: (1) The bank mentioned was Eurobank S.A.; (2) Damages were quite extensive: (3) IEDs timer worked perfectly (waring call at 22:05 giving an evacuation time of 35min; bomb exploded on 22:40); (4) The bank is located in the very center of Athens downtown where police presence is extensive; (5) Banks' counter-IED protection need serious reform instead of being sittin ducks. Damages in both the bank and surrounding buildings were quite extensive.

German prosecutors: Soccer bombing a stock fraud rather than Islamist terror

Source: http://hotair.com/archives/2017/04/21/german-prosecutors-soccer-bombing-stock-fraud-rather-islamist-terror/

Apr 21 – We say it pays to wait for all the facts to emerge on breaking news stories, and not to jump to conclusions. The saga of the attack on a German soccer team proves the wisdom of that advice, and the value of skepticism along the way. The attack had all the hallmarks

of a radical Islamist terror attack, right down to the purposeful shrapnel and the political statement that accompanied it, and German prosecutors even arrested a known Islamist radical — at first.

Today, however, **German police have arrested a man who shorted Borussia Dortmund stock on the morning of the attack, and allege that financial gain was the real motive behind the bombing:**

A **28-year-old German-Russian citizen** took out a five-figure loan to bet that Borussia Dortmund shares would drop, then bombed the soccer team's bus in an attack he tried to disguise as Islamic terrorism in a scheme to net millions, German officials said Friday. …

She said the man came to the attention of investigators because he had made "suspicious options purchases" for shares in Borussia Dortmund, the only top-league German club listed on the stock exchange, on the same day as the April 11 attack.

W. had taken out a loan of "several tens of thousands of euros" days before the attack and bought a large number of so-called put options, betting on a drop in Dortmund's share price, she said.

"A significant share price drop could have been expected if a player had been seriously injured or even killed as a result of the attack," according to prosecutors, though Koehler said the precise profit W. might have expected was still being calculated.

According to the Associated Press, stock prices *did* dip after the attack, but rose again quickly afterward. The suspect — identified only as "Sergei W" at the moment — would have had to act quickly to profit off the short, but prosecutors allege he wanted a much bigger payday. Had players been killed or more of them seriously wounded, the stock price would have fallen farther and remained depressed, giving him more opportunity to act quietly. As it turned out, though, only one player was seriously wounded, and the injury is not expected to keep him from missing significant playing time.

Nevertheless, the bombing had its impact on the team's field play. Midfielder Nuri Sahin told an interviewer that he couldn't get his mind on their first game after the attack, saying that "there is so much more than football in this world."

So it was greed rather than religion that was the motivator — not exactly an unknown force in crime, of course, and especially not attempted murder. It's not as if the initial story didn't have its holes, either. The first clue was probably the clumsy attempt to shift blame to two very different groups at the same time by leaving letters from both a supposed Islamist terrorist and an imaginary anti-fa radical, which made German investigators suspicious from the start. **A real terrorist from either faction wouldn't have tried to blame the other while claiming credit for an attack.** It didn't take long for investigators to unravel that, either; the AP report says that police had Sergei W under surveillance for a week before the arrest, which would have meant it started the day after the attack.

This makes for a rather memorable lesson in checking assumptions. If German prosecutors have this right, this suspect exploited (very reasonable) fears of terrorism in order to cash in at the expense of athletes, sports fans, and investors. Not all evil springs from radical ideology, a fact to keep in mind when trying to make sense of horrid attacks such as these.

EDITOR'S COMMENT: Absolutely agree that we do not have to jump to conclusions despite any "clear" indications. On the other hand, is it normal for a "gambler" to make roadside IEDs with nails? What is his military background/experience (if any)? What type of explosives were used (chemical signature)? What is his religion and educational background? Is the case over for the public or we need to know more (even after some time)?

New ISIS VBIED Tactic Has Vehicle Firing Rockets At Troops And Armor Before Impact

Source + Video: https://www.funker530.com/new-isis-vbied-tactic-vehicle-firing-rockets-troops-armor-impact/

Apr 21- A quick update for everyone that has been following the Islamic State's tactics in order to ensure their troops are well prepared in the event we find ourselves boots on the deck. The Islamic State is now rigging up their SVBIEDs with rockets and rudimentary launching systems. In the latest release, the Islamic State fighters showcase their new vehicle, both in the garage and in action against the Iraqi Army on the ground in Mosul.

It is important that we monitor our enemy, and keep track of new developments in their tactics. This new

style of SVBIED could prove very dangerous on the battlefields, as the vehicle can essentially provide suppression for itself as it barrels towards its intended target. Show this video to your troops, start planning for ways to defeat this now.

1 child killed, 11 injured as teen brings grenade into computer lab in Dagestan, Russia

Source: https://www.rt.com/news/385940-school-blast-dagestan-russia/

Apr 24 – At least one teenager was killed and 11 others injured in a blast in Russia's Republic of Dagestan, where an explosion went off at a local computer room. The incident was caused by a grenade brought into the building by one of the teenagers.

At least three of the injured teenagers are in a critical condition, RIA Novosti reported, citing a local hospital.

Dagestan's Interior Ministry spokesman confirmed the numbers of the dead and injured to RT.

Investigators are now working at the scene, the official said, adding that anti-terrorist committee is not involved in the case. According to preliminary data, the incident happened due to "*careless handling of a weapon*," he told RT.

The incident happened in the village of Agvali, Dagestan, in Russia's North Caucasus region.
A grenade exploded in a computer room, RIA Novosti cited the principal of a local school, Shamil Abakarov, as saying.
The weapon was allegedly brought into the building by an eighth-grade student, he said.

Did Russia Shoot Down US Missiles in Syria?

Source + **video**: http://www.riskhedge.com/post/exclusivedid-russia-shoot-down-us-missiles-syria

Apr 21 – In an exclusive video interview with RiskHedge, a long-time geopolitical expert says there is an alternate story making the rounds about the United States' April 7 missile strike on Syria's Shayrat Airbase in response to the Syrian regime's alleged use of sarin gas on its own people.

"Not all missiles made their target," says Dr. Theodore Karasik, a senior advisor to Gulf State Analytics. **"There were supposed to be 60. One malfunctioned on one of the ships. 36 made target, the remainder did not. And, there's a question of where did they go?"**
Dr. Karasik, a former senior political scientist in the International Policy and Security Group at RAND Corporation, spent the last decade in the Middle East and retains an extensive network in the region.

"The missing [missiles] were either brought down by S-300 battery or were taken over by Russian electronic jamming and were plunged into the sea," explains Dr. Karasik. "Now, this alternative theory means that the US and Russia have already clashed if you will—technically—with the use of the TLAMs

(Tomahawk missiles) and then being intercepted or taken over by Russian control."

If true, this means the US and Russia have had a *direct military confrontation* for the first time in decades. "This is very important," says Dr. Karasik, "because it illustrates that we've had our first encounter with the Russians, and that sets the stage for potentially future encounters between Washington and Russia on the Syrian battlefield."

In addition, the rationale for the missile strike in the first place—Bashar al-Assad's sarin gas attack on his own people—may be based on faulty intelligence.

"Apparently, the location of the attack itself is in an industrial area where there are a lot of toxic industrial chemicals located," says Dr. Karasik. "The attack on this location produced a toxic cloud that was deadly enough, obviously, to kill and maim hundreds. The issue here is that in this particular attack, where this industrial gas was released, this is not in any way related to a sarin-type attack."

Dr. Karasik says sarin is an odorless agent while victims complained they smelled an odor. He also explains that medics who were treating the victims were not properly dressed to handle sarin gas.

"Yes, there was an industrial toxic agent that killed and maimed people," says Dr. Karasik. "But, whether or not it was sarin still has not been proven."

This alternative theory is coming from a number of different places, according to Dr. Karasik, including sources in Washington, the Gulf region, and Russia.

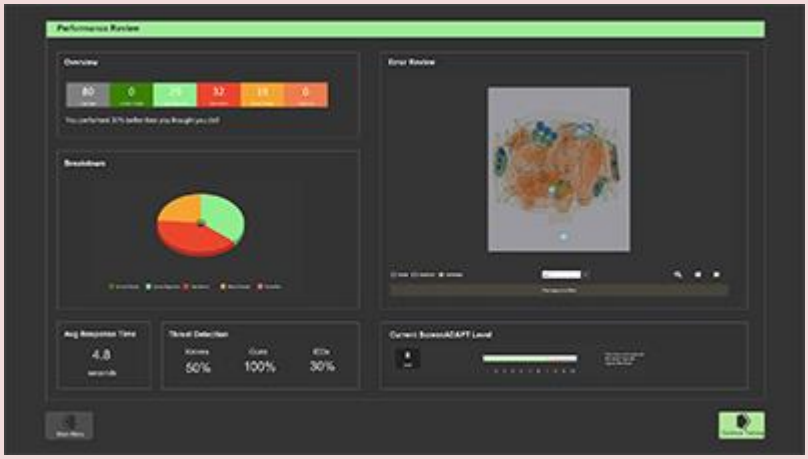
RiskHedge reached out to the White House, Pentagon, and Russian Embassy in Washington, DC to comment on this story. As of press time, the White House and Russian Embassy have yet to respond. Pentagon spokesman Major Adrian Rankine-Galloway referred back to the press conference held by Secretary of Defense Jim Mattis and General Joseph Votel immediately following the Syrian missile strikes. During the briefing on April 11, General Votel said the United States "targeted 59 locations on the airfield and struck 57 of those."

New training system improves airport screening efficiency, accuracy

Source: http://www.homelandsecuritynewswire.com/dr20170323-new-training-system-improves-airport-screening-efficiency-accuracy

Mar 23 – Among the many tasks assigned to Transportation Security Administration (TSA) Transportation Security Officers (TSOs), they must screen every bag boarding commercial aircraft within the United States.

The contents of bags are displayed on a screen as the scanned items pass through an X-ray machine. TSOs must identify threats, while minimizing unnecessary manual secondary bag searches that slow checkpoint throughput when they mistakenly flag a benign item. Interpreting X-ray images and understanding what threat and non-threat items look like in innumerable orientations is a daunting visual task.



Visual search of X-ray images is a repetitive task for the approximately 50,000 screeners employed by TSA, with an often low probability of encountering a threat. TSOs are trained to use perceptual cues such as color, orientation and spatial location of individual items to identify potential threats and differentiate them from non-threat items in the X-ray images of scanned bags.

The huge volume of items scanned every day must be cleared as quickly and efficiently as possible to facilitate air travel. However, missing a threat could be catastrophic. Lives depend on TSO accuracy. TSOs battle competing demands for safety and speed daily.

S&T says that the Department of Homeland Security Science and Technology Directorate's Office for Public Safety Research (OPS-R) developed a training system that not only makes TSOs more efficient, but also maintains their accuracy.

Existing training software is limited and uses only exposure training to elicit improvements in threat detection. Current training uses example after example until a TSO becomes more proficient. This training method is not adaptive to an individual's needs, does not leverage the latest training methods or technology, and does not identify the root causes of a TSO's deficiencies.

With these needs in mind, OPS-R sought to develop TSO training methods and tools that not only leveraged innovative emerging technology, but would also be relevant, challenging, intuitive and engaging. Enter ScreenADAPT, an advanced X-ray image analysis training system that examines TSO performance based on the latest in visual search research and uses eye-tracking technology to examine visual search performance.

ScreenADAPT has two main advantages over traditional training methods.

First, the program has an eye-tracking capability. Right now, trainers and trainees do not have any objective measure of where they are looking on the screen, for how long and in what pattern. This can all be determined using ScreenADAPT. This critical information allows trainers and trainees to analyze why an error was made. It can now be determined if a threat was missed because a trainee did not look at that area of an image, or if they looked at that area and did not recognize the item was a threat.

Second, ScreenADAPT provides diagnostic metrics on TSO performance and automatically adapts to the trainee's needs. ScreenADAPT dynamically addresses the trainee's needs by varying the type of training, type of threats, level of bag clutter and difficulty.

"You make this type of error, you get this type of corresponding training. If they are missing guns, they will see more guns; if they are missing IEDs they will see more IEDs," said Darren Wilson, OPS-R's ScreenADAPT program manager. "If a TSO makes a scanning error, they will get more exposure training. But if they make a recognition error, they will receive a different type of training to combat that, called discrimination training. The different types of training address the corresponding root causes of the errors and assist in building each TSO's mental threat image library."

The initial effectiveness evaluation indicated that using ScreenADAPT in initial training not only resulted in TSOs identifying threats faster, but also clearing bags faster. They were able to make faster decisions with more confidence.

Customization at the airport level is also a major advantage of ScreenADAPT. The items passengers pack in their bags in Portland, Oregon, at any given time of year can be very different than the items people pack in Orlando, Florida. ScreenADAPT allows individual airports to upload their own images that reflect the threat environment and items most often seen in that locality, as well as be responsive to emerging threats.

ScreenADAPT can be configured with a single or dual screens, and includes a small camera located just below each monitor to unobtrusively track eye movements.

The ScreenADAPT software calculates all of a TSO's hits, misses and false alarms, and it can compare their performance metrics to those of their peers. The feedback ScreenADAPT produces helps improve all scanners' performances.

"The whole premise is to maximize visual search performance," said Wilson. "What this enables you to do is to train the core visual search skills necessary to efficiently and effectively conduct X-ray image analysis. Even if there are advancements in technology, it's always going to come back to these basic visual search skills."

TSA has recently deployed fifty ScreenADAPT systems for an even larger training effectiveness evaluation at airports in New York City, Pittsburgh, Portland (Oregon), Houston, Las Vegas and Raleigh. Some of these locations volunteered to be research airports, while others were chosen to vary the size of airports and types of passengers in data collection.

Initial data indicates that ScreenADAPT results in a 45 percent improvement in efficiency, with no loss in threat detection effectiveness.

Google working with UK on counter-extremism

Source http://www.middleeasteye.net/news/google-home-office-prevent-counter-extremism-1186558071

Mar 29 – Google has been providing "digital and communications support" to counter-extremism campaigners backed by the Home Office, even as it faces a backlash from ministers over extremist content online, Middle East Eye can reveal.

The internet search giant's work with the Office for Security and Counter-Terrorism (OSCT), which is based in the Home Office and is responsible for the government's Prevent counter-extremism strategy, has included social media and video training for Muslim civil society organisations that dates back at least five years.

MEE has seen an invitation to one such session, a "workshop on YouTube and online video optimisation, to be delivered by Google." It was sent out by the OSCT's Research, Information and Communications Unit (RICU).

"As you know, we at RICU are supporting a network of civil society groups such as yours to build your communications capabilities," the invitation said.

A source who attended the session, which took place in 2012 and included a visit to Google's YouTube studio in central London, told MEE that the invitation had arrived "out of the blue".

"There is no open process. You don't apply, you are invited and the people who were invited to attend those seminars would be drawn from a list of organisations that had been pulled together for a good number of years," said the source, who

agreed to speak on condition of anonymity.
Google's low-profile counter-extremism work with government agencies is ongoing. A company representative told a parliamentary inquiry last year that the company had a "long history of working with government and with law enforcement authorities".

'Profiting from hatred'
Details about Google's relationship with the OSCT can be revealed as it comes under growing pressure from senior ministers and prominent advertisers over its perceived failure to tackle extremist content online.
Sarah Newton, the Home Office minister responsible for counter-extremism, said last week that Google had been called into Downing Street and "read the riot act" after it emerged that advertisements paid for by the government had appeared on the website of Hizb ut-Tahrir and a website linked to Hezbollah.
Yvette Cooper, the chair of parliament's home affairs committee, also wrote to the company to accuse it of "profiting from hatred".
"Google is the second richest company on the planet. The lack of effort and social responsibility it is showing towards hate crime on YouTube is extremely troubling," wrote Cooper.
Following last week's London attack, Home Secretary Amber Rudd said that she would be meeting representatives of Google and other social media companies again on Thursday to urge them to "take a more proactive and leading role tackling the terrorist abuse of their platforms" and told Sky News "they're going to get a lot more than a ticking off".
Foreign Secretary Boris Johnson and Prime Minister Theresa May's office have also both called for technology companies to do more to remove extremist material from their platforms.
But details of the workshop delivered by Google suggest that it has links to the government that are closer than either has publicly indicated.
The invitation described it as "an opportunity to learn how to drive audiences to your online videos through effective titles, tagging, descriptions, cross promotion, and how to exploit insight tools". But MEE's source said that RICU had also used the session as an opportunity to promote its own work.
"There is a unit within RICU that deals with creating and helping voluntary sector organisations, Muslim ones in particular, to produce better quality content for social media purposes. I remember having conversations with them about whether we'd be interested in working with them to produce some content that we would then put on our website."

'Challenge extremist propaganda'
Other government departments and other social media companies also have working relationships.
MEE has seen another invitation sent by the Department for Communities and Local Government for an event earlier this year at Twitter's headquarters aimed at interfaith organisations.
"We aim the workshop to be a practical faith-sensitive workshop with the Twitter experts on maximising and crafting your social media impact and understanding tools and reporting," the invitation said.
In response to a Freedom of Information (FOI) query, the OSCT confirmed that it held information requested about its relationship with Google.
But it declined to release further details on the grounds that doing so would compromise national security, prejudice the prevention or detection of crime, and prejudice commercial interests.
The OSCT also said that releasing the names of individuals and organisations with which it worked would constitute a breach of confidence and would undermine the Prevent strategy, which aims to stop people being drawn into terrorism.
But it said that it did bring together civil society groups and industry experts to enable them to "confront and challenge extremist views and propaganda".
"The Research, Information and Communications Unit connects them with industry experts to provide them with the digital and communications support they need to deliver their own campaigns, including creative advice, production capabilities, website build, media training and public relations support," it said.
RICU has previously been revealed to have orchestrated a number of ostensibly grassroots counter-extremism campaigns fronted by community groups and campaigners.
Google earlier this year hosted a digital summit at its London headquarters organised by Imams Online, a website alleged to have close links to RICU. Imams Online

maintains that its content is "independent of any external influence".

MEE's source said the opaque nature of the government's work with Google and other technology companies raised concerns about the "encroachment of the security agenda into all aspects of our lives".

"The YouTube session was all about appraising the NGOs who don't normally get that level of exposure or opportunity and when you are thrown the opportunity of meeting with Google or YouTube and you are a fledging voluntary sector organisation that has struggled to get any kind of grant funding then of course you are going to jump at it. People were interested," the source said.

'Fundamentally dishonest'

But, the source said, the government risked undermining civil society organisations' credibility and effectiveness by linking funding and training opportunities to the Prevent agenda, which is widely distrusted and considered discriminatory in Muslim communities.

"You need those authentic organisations that have legitimate currency in the sectors they work in to build up resilience and that shouldn't be compromised by any money or training that has that indelible link to Prevent and the security agenda because then their own constituency just switches off. And it is fundamentally dishonest as well," the source said.

Google declined to comment for this story but it has stated publicly that it works with governments and community groups to combat extremism.

Anthony House, the head of public policy strategy for Google Europe, Middle East and Africa, last year told a parliamentary inquiry that the company had a "long history of working with government and with law enforcement authorities".

It has also set up pilot programme offering "Google grants" to charities and NGOs "dedicated to preventing radicalisation" which allowed them to place adverts for free against terrorism-related search terms of their choosing.

Google's parent company, Alphabet, has prioritised making the world "safer from violent extremism" and "disrupting online radicalisation and propaganda" as key challenges for which it provides funding for projects via its Jigsaw technology incubator company.

Projects backed by Jigsaw, previously known as Google Ideas, include Abdullah-X, a YouTube cartoon "that aims to steer young minds away from extremism", and Moonshot CVE, a company that describes itself as "applying start-up thinking to the field of countering violent extremism".

'Big and powerful companies'

Speaking to BBC radio on Tuesday, David Wells, a former British intelligence officer, said that big technology companies already had relationships with intelligence agencies in the UK and the US.

"There is the existing relationships that go on and work quite well behind the scenes. We saw quite a lot come out of the [Edward] Snowden revelations which revealed quite a lot how big tech companies are working with governments on a case by case basis," said Wells. "The government is looking to the private sector to solve big problems which they can't solve on their own."

Luc Delany, a former European policy associate at Google, also said that technology companies were working hard to make sure that governments "understand what they do and why they do it".

"We are talking about some very big and powerful companies but we are also talking about very new companies," said Delany.

"No one wants to have criminals behaving on their platforms and networks and they want to work with government to identify potential problems and solve them and they do that with public policy teams, with meetings, with developments, they hire legal experts, they hire former intelligence officers to try and identify these problems."

The Home Office also declined to offer any further comment to its response to MEE's FOI request. Asked whether it had paid Google for its services, or whether these had been provided in kind, it suggested MEE could submit a further FOI request for clarification.

National Cyber Center to be established in Latin America by Israeli Consortium

Source: http://i-hls.com/2017/03/national-cyber-center-established-latin-america-israeli-consortium/

Mar 29 – **The Israeli Cyber Companies Consortium (IC3) was recently awarded a contract worth tens of millions of dollars to establish a national cyber center in a country in Latin America.**

The IC3, led by Israel Aerospace Industries (IAI), will supply a strategic national level cyber defense center to a Latin American country. This will include risk evaluation, establishment of an advanced monitor and defense center against cyber-attacks, an information-sharing infrastructure, and a cyber-training program.

ELTA Systems' Ltd., a Group and Subsidiary of IAI (IAI/ELTA) will oversee the project's implementation; supply a national-grade solution for the **identification, investigation and early detection of cyber-attacks; accompany and train cyber personnel; and establish a public information-sharing platform in the cyber domain.**

Israeli Cyber Companies Consortium

According to IAI's announcement, Verint Systems Ltd. will deploy its Threat Protection System (TPS) solution, an essential multi-vector detection, automated investigation and response platform focused on advanced cyber-attacks at the national level. Check Point Software Technologies Ltd. will supply solutions for Next Generation Threat Prevention, Advanced Access Control and forensic lab tools, fused with real-time actionable intelligence at a national scale, providing protection against cyber-attacks. ClearSky will provide cyber intelligence solutions, strategic planning, and cyber defense methodologies for national cyber protection and collaboration. CyberX will deal with the detection of cyber threats in SCADA and ICS systems.

The IC3 was established in 2016 under the endorsement of the Israeli government to provide holistic, end-to-end, cyber solutions at the national level, working with leading Israeli cyber companies having complementary areas of expertise, to address technological-cyber needs at a national and governmental level. The Consortium includes IAI/ELTA, Check Point, Verint, Bynet, ECI, CyberX, and ClearSky, and most recently, BGProtect, CyberArk, and Safebreach.

"Combining technological cyber solutions from an assortment of leading Israeli companies allows us from both the international and technological level to offer a comprehensive and integrated solution – this is a case when the whole is greater than the sum of its parts" said Esti Peshin, General Manager of IAI's Cyber Division. "The endorsement of the Israeli government is critical to the success of the consortium, and we are confident that the model applied in Latin America will continue to prove itself in the future".

ISIS-linked cyber group releases "kill list" of 8,786 US targets for lone wolf attacks

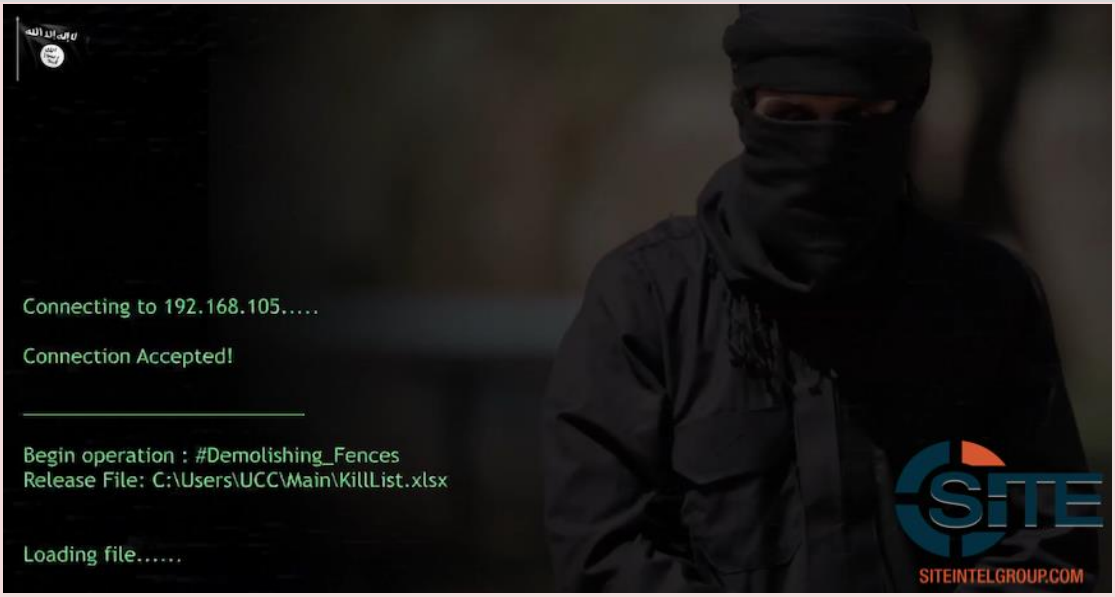
Source: http://www.newsweek.com/isis-linked-cyber-group-releases-kill-list-8786-us-targets-lone-wolf-attacks-578765

Apr 09 – A group of hackers supporting the Islamic State militant group (ISIS) have released a list of thousands of individuals in the U.S. and their addresses, calling for lone wolf attacks on the targets.

The list, which includes 8,786 names, was released by the pro-ISIS hacking group the United Cyber Caliphate (UCC) and verified by the terror monitor SITE. The six-minute-long video, which includes a threat against President Donald Trump, instructed would-be attackers to: "Kill them wherever you find them."

The phrase is regularly used by ISIS and its supporters on social media channels when trying to incite lone killers to carry out attacks on their own initiative.

On 16 March UCC released a video saying its leader Osed Agha had been killed in a U.S. airstrike. The footage promised retaliation for the killing. The group "vowed to continue its work" and included scenes of an American flag on fire.



In July 2016 the hacking group released another list of targets calling for lone wolf attacks. SITE said the list included 1,700 individuals including members of Christian churches and Jewish synagogues in the United States.

The FBI has said in the past that making contact with those included on such lists was a routine procedure "in order to sensitize potential victims to the observed threat."

The inclusion of churchgoers and members of synagogues is not surprising given the radical Islamist group's treatment of anyone who doesn't subscribe to their radical interpretation of Islam.

Stopping Attacks That Disrupt Voice Communications

Source: https://www.dhs.gov/science-and-technology/news/2017/04/10/snapshot-stopping-attacks-disrupt-voice-communications

Apr 10 – **Imagine if your call to 911, your financial institution, a hospital or even your child's school doesn't get through**.

In the past few years, 911 emergency call centers, financial services companies and a host of other critical service providers and essential organizations have been victims of telephony denial of service (TDoS) attacks. These attacks are a type of denial of service (DoS) attack in which a voice service is flooded with so many malicious calls valid callers can't get through.

The DHS Science and Technology Directorate (S&T) is working to make sure TDoS attacks cannot disrupt critical phone systems, explained TDoS Program Manager Daniel Massey. The program is part of S&T's Homeland Security Advanced Research Projects Agency's Cyber Security Division (CSD) portfolio.

A TDoS attack can be an 'old-school' attack, in which the victim is flooded with calls from a group of people using mobile or landline phones. These type of attacks often are coordinated through social networking. This TDoS attack approach most often is used to harass a victim or disrupt its operations.

In a high-tech twist, attackers are using technology such as automated dialing software, Voice over Internet Protocol (VoIP) and compromised mobile phones to send thousands of automated calls to tie up a target's phone system, rendering it unusable for legitimate incoming and outgoing calls.

These attacks are relatively easy and inexpensive and can be launched from anywhere in the world. In many cases, the objective of these attacks is to extort money. Victims range from government agencies to private companies and even individuals.

A typical extortion-type TDoS attack unfolds this way:

A person calls a company claiming to be a debt collector seeking repayment of a past-due loan. The caller threatens to lock up the

company's phone lines with repeated calls unless immediate payment is received. Sometimes the TDoS attack threat prompts victims to pay the ransom because they are either unsure whether they owe the money the attackers demand or they want to avert public embarrassment to the company's image.

If the payment is not provided, the attack is launched. The ensuing steady stream of calls can last several hours, stop for a while and then resume. Some attacks have continued over an extended period of weeks or even months.

But not all TDoS attacks seek a payment. For instance, last October an Arizona teenager was charged with sending thousands of calls to 911 emergency call centers and law enforcement agencies in multiple states. The teen had exploited a flaw in a leading mobile operating system to initiate the TDoS attack through compromised cell phones.

To stop these insidious attacks, CSD is funding two research projects designed to harden defenses against TDoS attacks.

The **first project** addresses the growing attack sophistication, frequency, call volume and complexity of call-number spoofing, says Massey.

Led by SecureLogix, a VoIP security specialist, the team is developing a prototype solution for complex TDoS attacks that will use a multi-level filter approach to analyze and assign a threat score to each incoming call in real time. That score will help distinguish legitimate from malicious calls and help mitigate an influx of malicious calls by terminating or redirecting them to a lower priority queue, to a partner service that could manage the calls or to an additional service that could verify each call's legitimacy.

The prototype is based on an existing voice-security solution, which provides a base to build upon so it can be deployed in complex voice networks. It also has an integrated business rules management system and machine-learning engine that can be extended easily with limited software modifications.

SecureLogix will deploy the prototype at a customer location, within the cloud and at a service provider network. The company also is working with multiple pilot partners including a 911 emergency call center, other emergency responders and large financial organizations, to deploy and validate the prototype in operational practice.

In the **second project**, a research team led by the University of Houston is addressing the vulnerability of Emergency 911 and Next-Generation (NG) 911 systems to TDoS, Distributed Denial of Service (DDoS), and robocall attacks, all of which pose significant threats to public safety.

The research team includes SecureLogix, FirstWatch, the Industry Council for Emergency Response Technologies, and cybersecurity analysts who specialize in penetration tests of telephony systems.

The team has assessed and modeled threats to the emergency response and public-safety communication network posed by DoS attacks. It is developing an integrated defense mechanism that is cost-effective, easy-to-manage, TDoS-defense capable, and customizable for the unique characteristics of varying 911 infrastructures.

The platform monitors each incoming call's signaling messages, metadata and voice contents to determine if it is suspicious. It then prioritizes the call according to an analysis of its content and audio to ensure real emergency calls are routed to 911 operators for immediate action. Additionally, the team developed a novel approach to check for synthetic voice to identify and address potential TDoS calls generated by phone bots.

In the not-too-distant future, these new defenses will help bring an end to TDoS attacks, thereby denying malicious actors a potent tool.

Cyber Security Review – Spring 2017

Source:https://issuu.com/deltabusinessmedialimited/docs/cyber_security_review_spring_2017?e=6269486/46614880

'Hybrid threat' centre to be built in Finland to counter fake news

Source: https://eandt.theiet.org/content/articles/2017/04/hybrid-threat-centre-to-be-built-in-finland-to-counter-fake-news/

Apr 12 – **A centre to combat disinformation and fake news is to be built in Finland, following an agreement between eight European countries, the US, and NATO.** The

centre, which will be named the European Centre of Excellence for Countering Hybrid Threats, will serve as a platform to pool resources and expertise between the countries involved.

In recent years, the Nordic and Baltic countries have been increasingly concerned over what have been described as **'hybrid threats'** - disinformation campaigns and systematic spreading of fake news, including by the Russian government.

In October 2015, Finnish President Sauli Niinistö warned of the "information warfare" that was already affecting Finns, and last year, the EU and NATO pledged at a summit in Warsaw to increase cooperation in the areas of cyber defence and countering hybrid threats.

Finland, the UK, France, Germany, Latvia, Lithuania, Poland, Sweden and the US signed a memorandum with NATO agreeing to establish the centre. It will be based in Helsinki, and will begin its work later this year.

Timo Soini, the Finnish foreign minister, said that Finland had become a target for hybrid threats through disinformation campaigns and malicious cyber activities. He added that countering hybrid threats was a European priority, and that the EU and NATO will face "the challenge of hybrid threats hand in hand".

The centre is being supported by the Finnish government, with an initial budget of €1.5 million, and will be staffed by a team of experts and researchers from the centre's founding countries.

The head of NATO's civil preparedness unit, Lorenz Meyer-Minnemann, said that the European Centre of Excellence for Countering Hybrid Threats would serve as a platform for the EU and NATO to pool resources and share their expertise.

"Working together is essential in building resilience to hybrid threats," he commented.

The centre is expected to collaborate closely with NATO's existing cyber defence centre in Estonia, and its strategic communications centre in Latvia.

The spread of fake news through social media – which some commentators suggest contributed towards the election of US President Donald Trump last year – has prompted more research focusing on how we use, understand and consume social media. A study from Penn State University and King's College London, for instance, recently reported that social media users often adopt different personas, or '(social) hats' unique to each different social network.

Facebook targets 30,000 fake-news accounts ahead of French election

Source: http://www.homelandsecuritynewswire.com/dr20170418-facebook-targets-30-000-fakenews-accounts-ahead-of-french-election

Apr 18 – Facebook was the subject of harsh criticism for allowing itself to be used by two Russian intelligence services – the GRU and the FSB – in their broad campaign of fake news in the summer and fall 2016, undertaken to help Donald Trump win the November election.

The company has taken action to prevent Russia and other actors from engaging in a similar campaign in France, where the first round of the presidential election is to be held on Sunday, 23 April.

The second round will be held 7 May.
Facebook said it has targeted 30,000 fake accounts linked to France as part of a global effort against misinformation.
The company said Thursday it's trying to "reduce the spread of material generated through inauthentic activity, including spam, misinformation, or other deceptive content that is often shared by creators of fake accounts."
It said its efforts "enabled us to take action" against the French accounts and that it is removing sites with the highest traffic.
NPR reports that Facebook and French media are also running fact-checking programs in France to combat misleading information, especially around the presidential campaign.
The company's action against fake news follows pressure by European authorities on another front: both Facebook and Twitter have been urged to remove extremist propaganda and other postings which violate European hate speech regulations.
In December, as the scope of Russia's false news campaign on behalf of Trump became more apparent, Facebook said it would ramp up its efforts against the spread of false news and misinformation on its service. The company said it will focus on the "worst of the worst" offenders and partner with outside fact-checkers and news organizations to sort honest news reports from made-up stories.
Since December, the company has extended its efforts beyond the United States.
Last week, Facebook it launched a resource to help users in fourteen countries, including the United States, France, and Germany ,spot false news. The resource is a notification, available for a few days, which leads users to a list of tips for spotting fake news. Information is also offered on how to report false news.
Facebook's notes that it is participating with other companies and tech industry leaders to establish a "news integrity" nonprofit organization to promote news literacy and increase the public's trust in journalism.

Israeli tech prevents ads from funding terror websites

Source: http://www.jpost.com/Business-and-Innovation/Tech/Israeli-technology-prevents-ads-from-financing-terrorist-websites-488287

April 19 – Internet advertisers are inadvertently financing sites that support terrorism and host inappropriate content – a phenomenon that one Israeli startup is aiming to eliminate.
The Herzliya-based **Taykey**, a company that analyzes the web to understand trends for audiences, has developed a tool that it says will enable advertisers to prevent their ads from appearing on such websites. With the help of this feature, advertisers can now be confident that they are not accidentally funding terrorist activity or inappropriate content distribution.
"Terrorism-supporting websites have access to a $160 billion online advertising market annually when they undergo an automatic approval process that large companies are unable to limit," said Amit Avner, founder and CEO of Taykey.
"In this manner, sites with offensive content generated hundreds of millions of dollars last year – among them, sites operated by terrorists who are included on the black lists of the United States."
All too often, advertisers who make use of large advertising networks on the Internet are entirely unaware that they are funding terrorism-supporting websites that display ads in exchange for a share of the profits, a statement from the company explained. While filters operate in real time in order to block such exchanges from occurring, terrorist sites are often able to evade such barriers due to the constant flood of content on the Internet.
Taykey's technology aims to take an entirely different route – by pre-screening trusted homes for ads, rather than trying to eliminate malicious content.
"Our solution will always route the advertisement to safe sites with quality content in order to reduce the income of terrorist sites, which will decrease their activities," Avner said. "As a result, fewer people will be exposed to them."
Taykey's technology works by scanning various news sites and social networks to cross-check information within them, the company explained. By identifying content that is gaining popularity among different audiences, the analysis works on the assumption that popular content within a "safe audience" – such as mothers, youth or sports

fans – would not include terrorism-supporting sites or inappropriate material.

"What we do is package all the things they like and tell advertisers – you want to be on this content," Avner told *The Jerusalem Post* on Tuesday.

"We don't look at pages and block unsafe content – we mark safe content. Think of us as primetime television. We basically find what's hot and relevant all the time, at scale, and help [advertisers] do that repeatedly hundreds of times a day."

Although not an advertising firm on its own, Taykey is now providing both trend insights and security tools to advertisers by integrating its technology into the interfaces of large online advertising networks like TheTradeDesk and AppNexus.

"The ads never go next to unsafe stuff," he said. "We always tell you, 'Here are the things that are safe,' versus, 'Here are the things you don't want to be on.'" In addition to the company's Herzliya headquarters, Taykey, founded in 2009, also has offices in New York, San Francisco, Chicago and Los Angeles.

While it does face some competition, Avner said that the other top companies in the field focus on checking whether or not an individual website is safe rather than following his firm's more proactive approach.

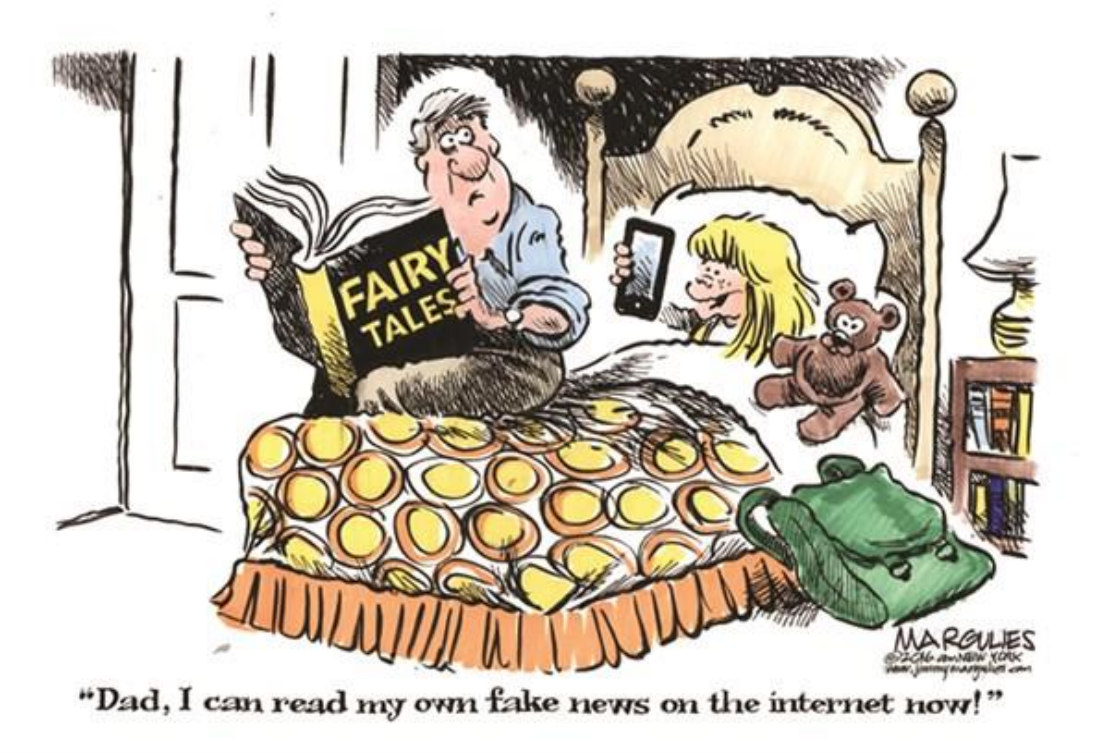
"We are, in a way, trying to make the world a bit of a better place," he continued.

Internet users may value their access to free news websites and social networks like Facebook, but the ad world is fueling these entities, Avner explained.

"Through advertising, the Internet is free," he said.

Yet, as is true in any industry associated with money, advertising can also attract plenty of bad people, Avner acknowledged. His company is therefore aiming to route ad money to high-quality content rather than into the hands of malicious operators.

"What we're trying to do as a data company is identify, analyze and understand through artificial intelligence what content is actually great, high quality and useful for any audience – for the target audience and for the advertiser," he said. "We hope that bad people make less money and high-quality people make more money."



Refillable vest offers last-mile wearable transport for clean water

Source (+video): http://newatlas.com/watervest-clean-water-transport/48589/

Mar 24 – While water scarcity gets a lot of attention, simply transporting this vital resource is in itself a huge dilemma. Women spend around 200 million hours a day hauling clean water around, and just 16 percent of the population in Sub-Saharan Africa have access to it in their homes. WaterVest is a wearable bladder designed to lighten the load, allowing users to carry several days' worth of water for a family in a single trip.

The reusable WaterVest costs around the same as a heavy-duty plastic bag to produce, and is made from recyclable plastics. It is designed to evenly distribute the load across the user's body and comes as a one-size-fits-all vest, with the idea being that it can be filled to match the wearer's comfort, be they big or small.

At full capacity, the WaterVest can transport 40 liters (10.5 US gal) at a time, which the developers say is enough for a family of four for four days. It self-seals to prevent contaminants entering the supply, and can be filled and emptied without the use of utensils. This prevents "double-dipping" and therefore, the spread of germs and infectious diseases.

The team says that the idea of WaterVest is not to replace the provision of clean water, but to augment it. The trips saved using the bladder in place of water bottles, buckets or jerry cans could prevent injury and add up to millions of hours, the team says – valuable time that could instead be used for more productive pursuits like education.

With several prototypes already developed, the team is looking to raise funds on Indiegogo to produce a small batch to test in the field. From there, it will refine the design and use the money to analyze the data collected from users in order to optimize the design. Pledges for a WaterVest prototype start at US$50.

The How and the Why of Crowd Management

By Stephen Maloney

On a Saturday night in 2013, a fire broke out in a nightclub in Sao Paulo, Brazil. More than 240 people, mostly college students, were killed. Two years later, two people were killed and more than 70 injured in a stampede to exit a club in Malta, due to a possible gas leak. Although the immediate causes of the two incidents were different, a common factor that led to so many dead and injured was poor management of large groups.

Source:https://www.domesticpreparedness.com/journals/march-2017/

Stephen Maloney, *CEM, is an emergency manager with the U.S. Federal Reserve Board. He has a B.S. in geology from the University of Maryland, an M.S. in environmental science and policy from Johns Hopkins University, and is a graduate of the National Emergency Management Executive Academy and Harvard University's National Preparedness Leadership Initiative.*

The IMPRESS Greek-Bulgarian cross-border tabletop exercise

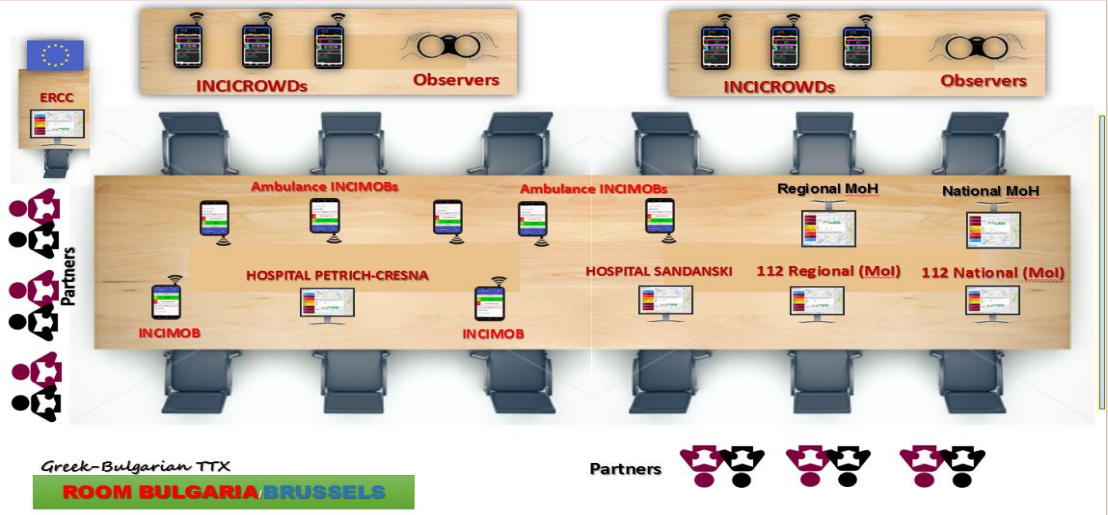
The final system of the EU-funded IMPRESS Project was successfully tested and validated in context of a cross-border Table Top Exercise (TTX) organized between Greece and Bulgaria in Sofia (16/3/2017)

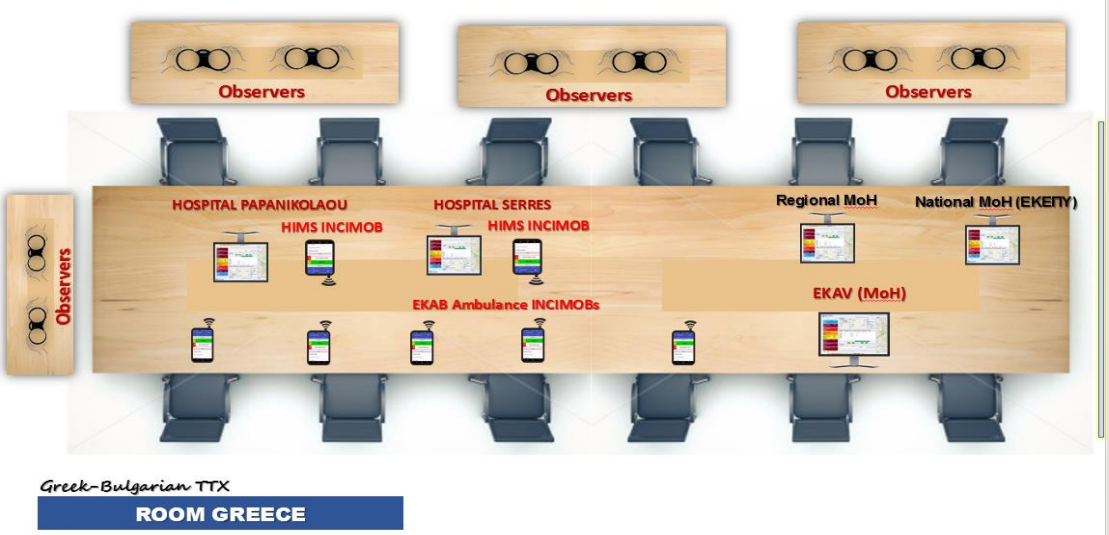
In the frame of the EU-funded R&D project IMPRESS: "Improving Preparedness and Response of Health Services in Major Crises" (No. 608078), coordinated by INTRASOFT International, the final system was tested and validated through a Table Top Exercise (TTX), that was successfully conducted in Sofia, Bulgaria on 16th of March 2017. The exercise was organized by IICT-BAS, KEMEA, EKEPY and INTRASOFT and hosted by NATO CMDR Center of Excellence in Shipka Hotel, Sofia. The IMPRESS system was operated by Greek and Bulgarian actors representing public services and hospitals, following a one day training that took place on March 15, 2017.

The scenario of the exercise was based on a combination of heavy rainfall and a strong earthquake that stroke Southern Bulgaria. As a result, extended damages to buildings and infrastructures along with a landslide damaging the roadside pavement in Strimon River and overflow of the river over part of the E79 Highway, were recorded. These incidents were coupled by multiple car accidents due to rockfalls along the respective segment of the E79 near the Greek-Bulgarian border. All the above caused a large number of fatalities and injuries requiring immediate response, pre-hospital medical intervention and transportation of casualties to nearby hospitals. Since transportation of victims via the damaged E79 connecting the southern part of Bulgaria with the rest of the country, the Bulgarian authorities requested international medical assistance, activating standard procedures via the European Emergency Response Centre (EERC) in Brussels.

IMPRESS system's components have been used in different configurations aiming to simulate field data gathering from multiple incident scenes and prove the capability of the system to strengthen coordination between the response organizations and the involved emergency medical services, including the international support request.

For the needs of the table top exercise, the IMPRESS infrastructure was arranged in two adjacent rooms simulating the respective system implementation in the Greek and Bulgarian operational realm.





The following organizations were actively participated in the GB TTX:

Bulgarian stakeholders and actors

The Regional Emergency Medical Center of Blagoevgrad, the Emergency Departments of the Hospital of Sandanski and Petrich, the EMS branch of the Blagoevgrad Hospital Unit located in Kresna and the Bulgarian Red Cross headquarter in Sofia as well as representatives of organizations of the Ministry of Interior.

Greek stakeholders and actors

National Center for Health Operations (EKEPY) under Ministry of Health; General Secretariat of Civil Protection; National Emergency Center (EKAV) both Athens HQ and Northern Greece Branch; Hellenic Center for Disease Control & Prevention (KELPNO); General Secretariat of Civil Protection (GSCP); two large hospitals in Thessaloniki ("Papanikolaou" General Hospital and "Ippokratio" General Hospital) along with the General Hospital of Serres (backup hospital).

Observers of the TTX

Bulgaria: Bulgarian Ministry of Health; Bulgarian Ministry of Interior; NATO CMDR Officers.
Greece: Ministry of Health; Post-Graduate Program on "Health Crises", Athens Medical School; Athens Assistance Medical Air Transport Co.
Italy: Italian Civil Protection – Palermo, Sicily.

Exercise lifecycle involving the IMPRESS system solution

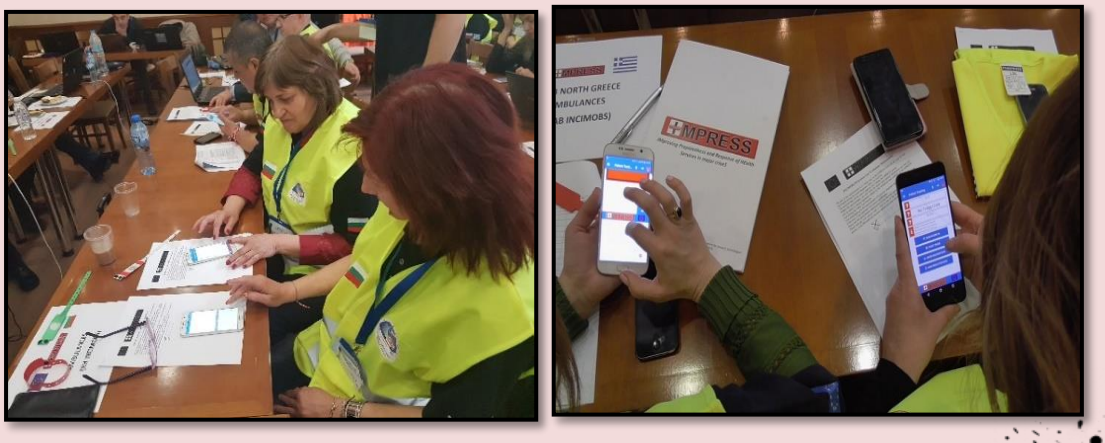
The TTX addressed the needs of the scenario using the IMPRESS resources deployed in Shipka Hotel, Sofia. According to the scenario, due to very heavy rainfall and snow melting in the upper regions of the watershed of Strimon River, the National Institute of Meteorology and Hydrology-BAS released a warning for increased risk of rapid rising of the river water level in the lower parts of Kresna Gorge, where the river bed tapers between the mountain cliffs. A red alert was issued for the international E-79 Highway, which runs parallel to the river bed and which is extremely narrow in this segment of the road due to the mountainous nature of the area. All alerts were broadcasted through radio and TV.

Later on, an earthquake sized 6.7R was registered by the IGGG-BAS, 10 km. northeast of Kresna town. Information was sent to the National and Regional Civil Protection Authorities by fax/email.

Due to the above alerts, IMPRESS modules have been activated in National and Regional Emergency Services and Health Departments. At the same time, dedicated volunteers using the **INCICrowd** mobile application send observations, comments and photos/videos from the affected areas.

Bulgarian actors, separated in various operational IMPRESS operating teams representing different public organizations

The call-centers of the Fire Brigades and the Regional EMS were overwhelmed by calls, received via the 112 Service, asking for S&R teams and traffic policemen in the affected area. In addition, the National Health Organization Center checked for hospitals' availabilities (through WARSYS and Data Harmonization Component) and dispatched available ambulances. Ambulances arrived at the incident area, made an initial triage and transferred the most critical cases into local hospitals (Kresna, Sandanski, Petrich). Due to the earthquake, hundreds of buildings have been collapsed and people were trapped into elevators. Power lines were also damaged and some health facilities activated their backup generators. More ambulances were requested to arrive at Kresna railway area crossing the city.



Regional Health Services (Ambulance crew) conducting triage using INCIMOB

IMPRESS tools and functionalities supported on-scene medical teams, first responders and agencies involved in the exercise, during the overall procedure, aiming to optimize the response and deployment of resources and timely dispatching the victims to hospitals. Following the triage and recommendation for dispatching, the receiving hospitals were informed to be prepared to receive fatalities, using their relevant INCIMAG and INCIMOB versions.

Due to the size of the disaster, the Bulgarian Ministry of Defense supported the Ministry of Interior to implement the National Plan for Disaster Protection and participated in the National Crisis Management Joint Committee formed. Furthermore, and due to the need for additional medical assistance, an advanced medical post was set up in the area of Kresna and secondary transport by air ambulances was organized toards nearby hospitals.

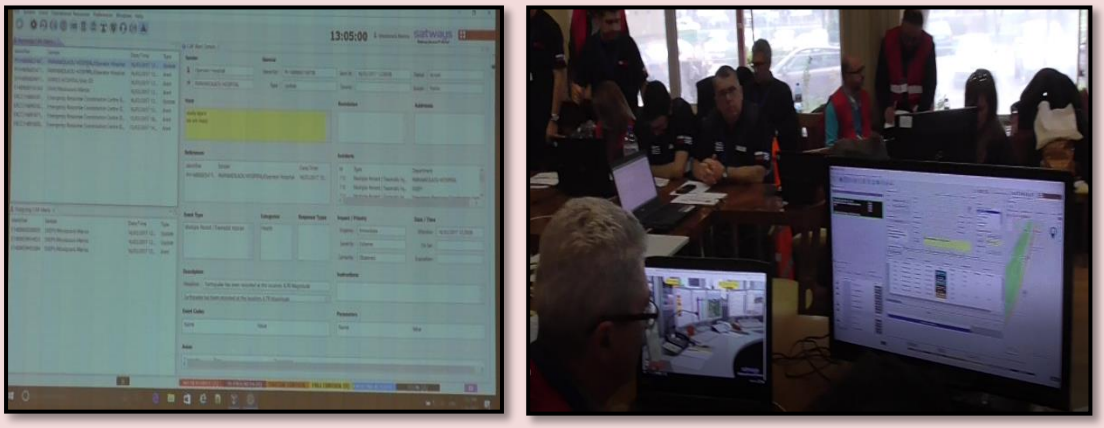
Implemented INCIMAG editions for the Bulgarian Public Services (MoI and MoH)

Given the collapse of the regional capabilities of the health emergency system and due to the excessive number of trauma patients, including patients with neurotrauma, crush injuries and severe burns, the National Authorities decided to request international assistance since road connection was lost in the north side of Kresna (due to road collapse and the consequent traffic disruption) and thus patients transportation to northern hospitals was not possible. The request was sent via INCIMAG to EU-CPM ERCC and then was shared among the EU Civil Protection Agencies of the member states. Positive feedback to the Bulgarian request was provided by Greece and a joint crisis center set up in both countries.

Introducing the scenario to the Greek actors

The emergency service of the Greek Ministry of Health (EKEPY) checked hospitals' availability in Northern Greece (Thessaloniki and Serres) and requested to initiate a limited surge capacity process. Moreover, EKEPY contacted Thessalonikis' Police authorities to provide escort and traffic control to ambulance fleet all the way to border station. EKEPY assigned EKAV (National Emergency Center) to mobilize a number of ambulances of pre-

hospital type properly manned for the occasion. EKAV confirmed availability and ordered the ambulance fleet to deploy towards the border crossing of Kulata-Promachon.



INCIMAG version of National Emergency Center (EKAV) of North Greece dispatching ambulances to the Greek borders

Bulgarian authorities provides casualties' information to EKEPY through INCIMAG, and gather confirmation through this infrastructure, informing EKAV in the same way. Greek pre-hospital ambulances of EKAV North Greece and mobile medical teams were dispatched (the communication between Greek Coordination center, EMS and Health Services, was conducted through different INCIMAG installations) to the Greek-Bulgarian border (Kulata/Promachon border crossing station), to receive victims delivered by Bulgarian ambulances.

North Greece Hospital (Papanikolaou) declaring availability through WARSYS (IMPRESS component) to EKEPY (left), National Emergency Center (EKAV) of North Greece conducting the secondary triage at the border (right)

The Greek medical teams conducted a secondary triage on site; transferred injured people to the ambulances of EKAV and then transported them to Greek hospitals, taking into consideration the suggestions of the IMPRESS recommendation engine, using the DSS tools. The hospitals' INCIMAGs got the medical information of the arriving patients and their ETA and confirmed these data during the patients' reception at the hospital's ED (using INCIMOB).

The exercise closed formally with the EKEPY reporting to the Bulgarian MoH about the safe transportation of the Bulgarian casualties to the Greek hospitals along with details about their status and contact information. ERCC was also informed about the overall details of the trans-border medical operation.


fp7-impress.eu
Coordination
Collaboration
Save lives
IMPRESS

Feedback from the Greek-Bulgarian tabletop exercise

Although not being a commercial solution, IMPRESS proved its high technology readiness level (TRL), which is capable to address the operational needs of health emergency services and the requirements of mass casualty incidents. The solution is flexible enough for supporting diverse organizational structures in routine operation and support multi-agency coordination.

The system was deployed smoothly for the needs of the TTX with minimum training. It seems to be quite mature to be deployed at Regional or National level for pre-operational validation purposes. The test users considered IMPRESS as a worthy solution for harmonizing health emergency operations and monitoring patients' status and flow to the ED of hospitals during disastrous events.

A number of suggestions provided by the operators during the debriefing session, following the TTX, was taken into account by the IMPRESS consortium for further development and future refinements of the system.

The Editor of the NSL (right in photo), participated in the TTX as member of the consortium representing KEMEA (Center for Security Studies – Athens, Greece)

FURTHER INFO

Project website: www.fp7-impress.eu
E-mail: info@fp7-impress.eu
Twitter: @Impress_FP7
LinkedIn: "IMPRESS FP7 Project" group
Facebook: "Impress Project - FP7" page
Blog: fp7-impress.blogspot.com

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no **608078**.

EENA 2017

The IMPRESS solution was also presented to the European Emergency Number (112) Association (EENA) 2017 Exhibition and Conference held in Budapest, Hungary (5-7 April 2017).

112 is the common emergency telephone number that can be dialed free of charge from most mobile telephones and, in some countries, fixed telephones in order to reach emergency services (ambulance, fire and rescue, police).

112 is a part of the GSM standard and all GSM-compatible telephone handsets are able to dial 112 even when locked or, in some countries, with no SIM card present. **It is also the common emergency number in all member states of the European Union** as well as several other countries of Europe and the world.

112 is often available alongside other numbers traditionally used in the given country to access emergency services. In some countries, calls to 112 are not connected directly but forwarded by the GSM network to local emergency numbers (e.g., 911 in North America or 000 in Australia).

112 is not always supported by VoIP operators or on non-GSM networks

Selecting to right first responder technology

Source: http://www.homelandsecuritynewswire.com/dr20170404-selecting-to-right-first-responder-technology

Apr 04 – With the abundance of tools and technologies available to assist first responders, it is important to address questions such as: How do the tools perform in real-world response situations? Can they withstand uncertain environments? Are they easy to use when a responder is wearing protective gear? How heavy is the technology? Will it weigh down, or fit within the gear of a responder who is already wearing their full kit? The Department of Homeland Security Science and Technology Directorate (S&T) First Responders Group (FRG) wants to help first responders answer these questions so they can make informed decisions about technology acquisition.

S&T says that recently, FRG's National Urban Security Technology Laboratory (NUSTL) hosted an Urban Operational Experimentation (OpEx) to find answers to these types of questions. The three-day event is an annual gathering of more than seventy participants

from federal, state, and local first responder agencies from various disciplines, as well as private industry and academia partners. They gathered to experiment with four emerging first responder technologies in realistic operational scenarios. The event was held in coordination with the New York City Police Department (NYPD), New York City Fire Department (FDNY), New York City Emergency Management (NYCEM) and the Port Authority of New York and New Jersey (PANYNJ).

The first day was spent experimenting with FABIS-Mobile, a facial recognition software designed to enable users to perform real-time identification of individuals using still or video camera images. On the second and third days, first responders experimented with Haystax and LifeRing, two incident management communication technologies, and TSM Tactical Radios, which self-form into a mesh communication network without the need for fixed infrastructure.

Technology evaluators, observers and data collectors included members of S&T's First Responder Resource Group from Massachusetts, New York and Washington, as well as regional first responder representatives from NYPD, NYCEM, FDNY, PANYNJ, Customs and Border Protection, and the Metropolitan Transportation Authority (MTA).

"Urban OpEx yields numerous benefits to all participants – technology developers and first responders alike," explained NUSTL Director Adam Hutter. "It provides first responders with an opportunity to experiment with new technologies that could enhance their mission capabilities, gives technology developers direct feedback and input to consider when modifying their products to better meet first responder needs, and enhances NUSTL's understanding of first responder needs and gaps to guide future homeland security investments."

"The event was an extension on NUSTL's mission focus in serving first responders and making sure they have the knowledge and tools they need to do their jobs," said NUSTL Urban OpEx Program Manager Bhargav Patel.

"This year, we tried to place an emphasis on first responders from urban areas. We invited responders from Boston, Seattle, and engaged with the Offices of Emergency Management for the NYPD, Port Authority Police Department, and FDNY. Our goal is to put new technologies into their hands to see if it meets their mission needs, and if not, we want to know what needs to be changed," Patel said.

S&T notes that most of the technology developers were on-hand to train the first responder evaluators on their technologies and gather feedback about potential improvements. The event also provided responders from different disciplines an opportunity to meet and discuss their unique operational needs and different uses for the technologies.

Michael Lee, MTA Railroad Assistant Chief Security Officer for Technology and Projects, said he appreciated the opportunity to explore emerging technologies in a realistic setting and touch base with other responders.

"It's helpful to know our strategic goals are aligned. If we're looking at the same kind of technology, we can absolutely compare the use-case scenarios and share some of the lessons learned from other technologies they might have already. This is almost a force multiplier," Lee said.

Michael Gemelli, MTA New York City Transit's Department of Security, was also at the event and agreed with Lee. He said he appreciates NUSTL's focus on the technology and the objectivity of the research. Events like Urban OpEx remove the emphasis on marketing or selling the technology and puts it back on what it is, what it does and how it works in a realistic setting. "By answering these questions, FRG helps first responders make informed decisions about which innovative tools and technologies can best meet their needs," S&T says.

EU Project TACTIC

Source: https://www.tacticproject.eu/

TACTIC (Tools, methods And training for CommuniTIes and society to better prepare for a Crisis) aims to increase preparedness to large-scale and cross-border disasters amongst communities and societies in Europe. Throughout its two-year duration (May 2014 – April 2016), **TACTIC** will analyse risk perceptions and behaviour to identify pathways from risk perception to preparedness, and will develop a preparedness self-assessment that communities can use to assess how prepared they are for different types of crises. Additionally, **TACTIC** will focus on identifying

and categorising good practices of communication and education practices for preparedness. The self-assessment, communication and education practices will be discussed and analysed with stakeholders in a series of workshops as part of **TACTIC**'s case studies on four types of crises: terrorism, floods, epidemics, and earthquakes. Subsequently, a long-term learning framework for improving community preparedness to a range of crisis situations will be developed. All of **TACTIC**'s outputs will be presented in a web-based platform.

Objectives

The **TACTIC** project contributes to protecting citizens from threats resulting from crisis situations, including terrorism and natural disasters by assisting decision-makers, emergency managers, local authorities and importantly, local communities in being able to better prepare for large scale and cross-border crisis (including multi-hazard) and disaster situations. Crucially, our research activities will help ensure that community risk awareness is raised, and that the "needs" of European communities are identified and managed.

In addition to that, the project will provide recommendations to stakeholders for future policy initiatives in enhancing communities' preparedness to large scale, cross-border disasters. It will also positively influence citizens' preparedness by incorporating the public into its training curriculum, which emphasises long-term preparedness in its learning framework. As such, it will improve the communication between authorities and members of the public in crisis situations and raise public awareness around threats.

Against the background of these challenges, the overall objectives of TACTIC **are to:**

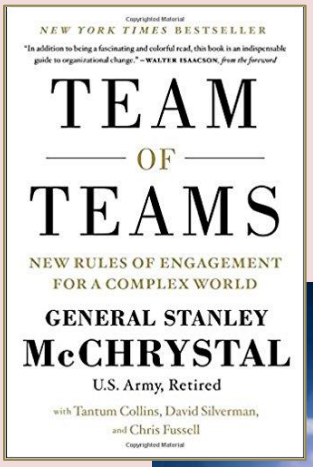
1. Identify factors that lead to a better understanding of how risk perception affects whether individuals take preparedness actions or not as well as identify good practices of existing preparedness programmes that are particularly effective in regards to encouraging preparedness actions to large-scale and cross-border disasters and crises;
2. Develop a participatory multi-hazard community preparedness self-assessment that allows communities (e.g. organisations responsible for disaster risk management as well as local actors (the public, NGOs, etc.) exposed to various risks to assess how prepared they are or feel to a range of hazards;
3. Develop demand-oriented preparedness communication and education material and practices with an emphasis on large-scale and cross-border disasters and crises (including training curricula and tools) that are based on and designed for the expectations of different communities and their different needs;
4. Develop, test and validate the community preparedness self-assessment as well as its preparedness communication and education material and practices in a collaborative and co-productive way by involving various stakeholders from science, policy-making, administration and civil society operating in the field of terrorism, natural disasters (e.g. floods and earthquakes) and epidemics; and
5. Synthesise the central output and insights of the project within a long-term learning framework for improving community preparedness to a wide range of hazards. This framework includes the community preparedness self-assessment as well as the preparedness communication and education material and practices. It will also include indicators to evaluate the overall quality of the process as well as the outcome of the process. The framework will be presented by means of a publicly accessible, user-friendly interactive and web-based platform.

Becoming a Networked Emergency Manager

By Terry Hastings

Source: https://www.domesticpreparedness.com/resilience/becoming-a-networked-emergency-manager/

Apr 12 – Leaders must continually adapt to changing circumstances, which requires a networked approach to managing emergencies by leveraging people, processes, and technology. This article applies lessons and strategies from the U.S. Special Operations Task Force in Iraq to emergency management. A truly networked emergency manager coordinates with all stakeholders, understands their roles and responsibilities, and embraces technology to ensure effective exchanges of critical information.



Former General Stanley McChrystal's book, entitled "Teams of Teams," is about leadership and the need to adapt to changing circumstances. In the book, he explains how the U.S. Special Operations Task Force in Iraq had to become a more nimble and networked organization to combat al-Qaida. Many of the lessons and strategies discussed are directly relatable to other disciplines, including emergency management.

The importance of networks within emergency management is not a new concept as the thinking has evolved to embrace "whole community" partners, including the private sector and nonprofit organizations. Although a fair amount of effort has gone into the idea of networked emergency management, here are some additional perspectives on what it

means to be a networked emergency manager. These perspectives relate to the management consulting theory that organizational success stems from three factors: people, process, and technology.

People, Process & Technology

In terms of people, the networked emergency manager must be willing and able to work with people and all types of personalities. Building and maintaining relationships takes time, but it is well worth the effort, particularly when there is a need to rely on other people for information or assistance during an emergency. Emergency managers also play an important role in helping to organize people and in bringing different groups and individuals together to tackle problems, often during a crisis. Investing in these people and relationships ahead of time will help build trust and increase the likelihood of success when it matters the most.

Emergency managers must understand process and be able to navigate bureaucracy, especially when dealing with multiple layers of government or complex issues that involve many different stakeholders. A firm understanding of the Incident Command System is certainly very important, but it is equally important to understand the roles and responsibilities of the various stakeholders involved and how they contribute to the larger emergency management effort. This deeper level of knowledge is necessary to better coordinate and facilitate response activities and should be obtained before a disaster occurs, which is why planning and other preparedness activities are so critical. Taking the time to plan, train, and exercise with different agencies and organizations allow all parties involved to better understand each other's processes and potential challenges. The networked emergency manager seeks these collaborative preparedness opportunities and new partnerships.

Finally, the networked emergency manager must understand and embrace technology and appreciate the rate at which technology is changing. Social media, emergency alerting

applications, mobile devices, and other emerging technologies such as unmanned aircraft systems (a.k.a., drones), are changing the way information is received and shared. Emergency managers must leverage new technology to better communicate with the public. The days of relying on trifold pamphlets and traditional press releases are over. Today, it is critical to have a have a social media strategy and the ability to use multiple forms of technology to communicate and connect with an increasingly networked population. Given the rate at which technology changes, it is also important to stay current and always explore ways to use new technology effectively.

An Ongoing Need to Evolve & Adapt

Emergency management has evolved greatly over the past several decades and will continue to evolve to address climate change, terrorism, cyberthreats, and other new challenges. Like General McChrystal's Special Operations Task Force, the discipline of emergency management must be able to adapt to the changing environment. Doing so requires networked emergency managers with the ability to understand people, process, and technology.

Terry Hastings *is the senior policy advisor for the New York Division of Homeland Security and Emergency Services, where he is responsible for the development and maintenance of New York State's Homeland Security Strategy and other statewide initiatives. He is also an adjunct instructor for the College of Emergency Preparedness, Homeland Security and Cybersecurity, at the State University of New York at Albany.*

3 Reasons to Invest in Tabletop Exercises

By Rob Burton

Source: http://www.preparedex.com/3-reasons-invest-tabletop-exercises/

In any discussion on continuity of operations, it is reasonable to ask, "Why should my organization invest in a tabletop exercise program?" While the reasons are many, some that serve as a foundation for a strategic-based approach to tabletop exercise programs include:

1. **Increased operational resilience:** Operational resilience requires comprehensive knowledge of the organization; as such, it cannot be achieved by a single department or managed by a single individual. Best business practice calls for effective BCP's (Business Continuity Plans), EAP's (Emergency Action Plans),

CMP's (Crisis Management Plans) as well as other plans based on the organizations needs. These plans are only effective once they've been validated through an exercise program. The result is a greater opportunity to actualize operational resilience enterprise-wide.

Related: 5 Common Tabletop Exercise Mistakes

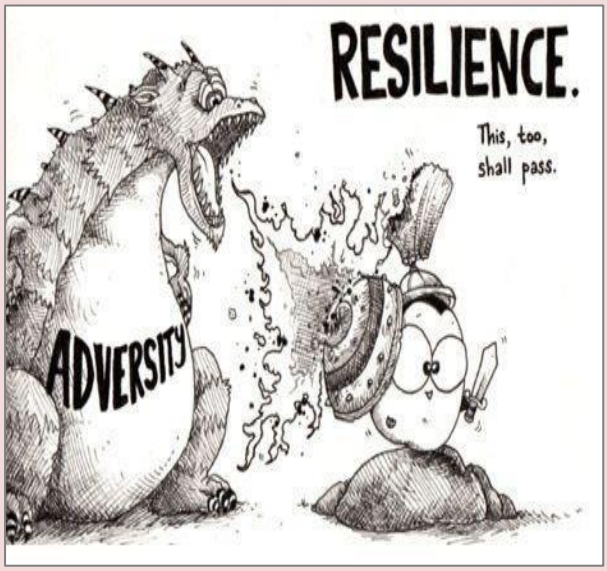
2. **Enhanced protection of shareholder value:** Studies have shown that organizations who experience an outage without any plan in place have a more difficult time recovering; for many, lost revenue may lead to closed businesses or significant decrease in value as well as reputational damage.
3. **Improved operational effectiveness and efficiency:** Experience has shown that the collaborative style required to conduct effective simulation exercises will invariably identify gaps in response planning and capabilities which are counterproductive to a resilient operation, and which are usually also counter to operational effectiveness. The result of mitigating the findings though comprehensive tabletop exercises and other types of exercises will usually lead to a more effective and efficient organization.

5 Steps to Creating and Delivering Tabletop Exercises – An eBook

Rob Burton *is a Principal at PreparedEx where he manages a team of crisis preparedness professionals and has over 20 years of experience preparing for and responding to crises. Part of his leadership role includes assisting PreparedEx clients in designing, implementing and evaluating crisis, emergency, security and business continuity management programs. During his career Rob has worked for the US State Department's Anti-Terrorism Assistance Program, as a crisis management consultant in Pakistan and Afghanistan where he negotiated with the UN and Pashtun tribal warlords and he served with the United Kingdom Special Forces where he operated internationally under hazardous covert and confidential conditions. Rob was also part of a disciplined and prestigious unit The Grenadier Guards where he served Her Majesty Queen Elizabeth II at the Royal Palaces in London. Rob was a highly trained and experienced infantryman serving in Desert Storm and commanded covert operational teams and was a sniper. Rob has keynoted disaster recovery conferences and participated in live debates on FOX News regarding complex security requirements and terrorism. Rob has a Queen's Commendation for Bravery.*

New resilience study helps governments prevent disaster-related loss

Source: http://www.homelandsecuritynewswire.com/dr20170411-new-resilience-study-helps-governments-prevent-disasterrelated-loss



Apr 11 – Hurricanes, wildfires, tsunamis, and other disasters cannot be stopped, but countries can plan for them — something some areas of the world seem to do better than others, according to a new study published in the journal *Risk Analysis*.

Oceania, which includes Australia and surrounding Pacific islands, was deemed to be the most resilient region of the world, meaning it would likely suffer fewer losses during a disaster than other areas. The study also revealed that Asia is the least resilient. Understanding resilience — and how to improve it — can help governments better prepare for disasters and reduce risks to human life.

"Resilience is the ability to prevent loss caused by disasters," according to Hong Huang, corresponding author and professor at the Institute of Public Safety Research at Tsinghua University in Beijing. "High resilience is like an umbrella that can protect against not only single and normal disasters, but also against miscellaneous and unconventional emergencies."

SRA says that in the study, "Resilience Analysis of Countries Under Disaster Based on Multi-Source Data," thirty-eight factors that affect a country's resilience were derived from national and international databases including the U.S. Census, the United Nations and the World Health Organization. The researchers used these databases to grade the resilience of each country and continent and develop a comprehensive index that includes indicators such as the number of disasters and their death tolls, as well as an area's population, infrastructure, economy and educational system.

The researchers also analyzed 100 years of historical data from more than 20,000 disasters and accidents to develop a resilience score for each country. They researchers also ranked each country based on the danger it faces from disasters and the degree to which its resilience to disaster has improved over time.

Extreme heat, tsunami and drought ranked as the most severe types of disasters, causing about 5,000 deaths in countries with a population density of at least 100 people per square kilometer. According to the data, Estonia, Libya, Sudan, Russia, and Myanmar had the lowest resilience scores. The latter three countries cover large areas and therefore have difficulty implementing comprehensive resilience plans encompassing the entire region. In general, African countries have low resilience because of poor infrastructure, bad economies, and lower education levels.

The researchers found it was easier for smaller nations to be more resilient than larger nations. Some of the most resilient nations included Barbados, Marshall Islands, Singapore, Cayman Islands, and Antigua and Barbuda.

Many countries have become more resilient to the threats posed by disasters over the last fifty years, particularly developing nations. Having a higher population density and GDP positively affected countries' resilience scores. Other factors that play critical roles in improving a nation's resilience include its ratio of insurance consumption to GDP and how many hospital beds it has per 1,000 people. Countries should consider these factors first when looking to increase resilience, the researchers said.

Becoming more resilient to disaster also varies by country because the impact from a certain type of disaster and countries' infrastructures and economies vary. "Different cities and countries have their own characteristics," Nan Zhang, assistant professor at Tsinghua University and lead author said. "Developing an index system is a very useful way not only to uncover the vulnerable areas, but also to discover the sensitive influencing factors that can improve resilience."

More areas are also looking to make changes that improve their resilience, according to the researchers. For example, New York is working to become more resilient to flooding by improving flood insurance, building codes, and flood zoning. Tokyo is using operational meteorological networks and advanced instruments to build infrastructure that is better equipped to withstand extreme weather conditions.

The researchers recommended that future studies should focus on determining the resilience of each country as it relates to each type of disaster.

— Read more in Nan Zhang and Hong Huang, "Resilience Analysis of Countries under Disasters Based on Multisource Data," Risk Analysis (6 April 2017) .

Bionic Tech Increases First Responders' Mobility

Source: http://i-hls.com/archives/76057

Apr 15 – Exoskeleton technologies are fulfilling new roles in the military, industrial, commercial and first-responder applications. Lockheed Martin has licensed the bionic augmentation technology Dermoskeleton from B-Temia, Inc.

Dermoskeleton is the basis for computer-controlled devices that can increase mobility and load-carrying capacity by counteracting overstress on the lower back and legs, according to defenseworld.net.

The **FORTIS exoskeleton** is an unpowered, lightweight exoskeleton that increases an operator's strength

and endurance by transferring the weight of heavy loads from the operator's body directly to the ground through a series of joints at the hips, knees and ankles.

"This technology offers a pathway to increased loadbearing and greater agility for our FORTIS industrial exoskeleton," said Glenn Kuller, Advanced and Special Programs vice president at Lockheed Martin Missiles and Fire Control. "It can also help to solve existing limitations of powered exoskeletons for our military and first responders."

"This agreement confirms our company's technology leadership and value of our work in increasing human mobility in both industrial and defense applications," said B-Temia President and CEO Stéphane Bédard. "Our arrangement with Lockheed Martin provides another avenue for our bionic technology to enhance human performance."

According to Lockheed's website, the Exoskeleton technologies can bring new capabilities to fighting forces and improve endurance and safety in industrial settings. The company focuses primarily on unpowered exoskeletons for industrial use, such as lightweight suits designed to increase in industrial productivity and prevent common workplace injuries. Military applications are focused on soldier load carriage and sustainment applications.

Climate breaks multiple records in 2016, with global impacts

Source: http://www.homelandsecuritynewswire.com/dr20170323-climate-breaks-multiple-records-in-2016-with-global-impacts

Mar 23 – The year 2016 made history, with a record global temperature, exceptionally low sea ice, and unabated sea level rise and ocean heat, according to the World Meteorological Organization (WMO). Extreme weather and climate conditions have continued into 2017. The WMO says that itissued its annual statement on the State of the Global Climate ahead of World Meteorological Day on 23 March. It is based on multiple international datasets maintained independently by global climate analysis centers and information submitted by dozens of WMO Members National Meteorological and Hydrological Services and Research Institutes and is an authoritative source of reference. Because the social and economic impacts of climate change have become so important, WMO partnered with other United Nations organizations for the first time this year to include information on these impacts.

"This report confirms that the year 2016 was the warmest on record – a remarkable 1.1 °C above the pre-industrial period, which is 0.06 °C above the previous record set in 2015. This increase in global temperature is consistent with other changes occurring in the climate system," said WMO Secretary-General Petteri Taalas.

"Globally averaged sea surface temperatures were also the warmest on record, global sea levels continued to rise, and Arctic sea-ice extent was well below average for most of the year," he said.

"With levels of carbon dioxide in the atmosphere consistently breaking new records, the influence of human activities on the climate system has become more and more evident," said Taalas.

The increased power of computing tools and the availability of long term climate data have made it possible today, through attribution studies, to demonstrate clearly the existence of links between man-made climate change and many cases of high impact extreme events in particular heatwaves, he said.

Each of the sixteen years since 2001 has been at least 0.4 °C above the long-term average for the 1961-1990 base period, used by WMO as a reference for climate change monitoring. Global temperatures continue to be consistent with a warming trend of 0.1 °C to 0.2 °C per decade, according to the WMO report.

The powerful 2015-2016 El Niño event boosted warming in 2016, on top of long-term climate change caused by greenhouse gas emissions. Temperatures in strong El Niño years, such as 1973, 1983 and 1998, are typically 0.1 °C to 0.2 °C warmer than background levels, and 2016's temperatures are consistent with that pattern.

Global sea levels rose very strongly during the El Niño event, with the early 2016 values reaching new record highs. Global sea ice extent dropped more than four million square kilometers below average in November, an unprecedented anomaly for that month.

The very warm ocean temperatures contributed to significant coral bleaching and mortality was reported in many tropical waters, with important impacts on marine food chains, ecosystems and fisheries.

Carbon dioxide levels in the atmosphere reached the symbolic benchmark of 400 parts per millions in 2015 – the latest year for which WMO global figures are available – and will not fall below that level for many generations to come because of the long-lasting nature of CO2.

Noteworthy extreme events in 2016 included severe droughts that brought food insecurity to millions in southern and eastern Africa and Central America. Hurricane Matthew caused widespread suffering in Haiti as the first category 4 storm to make landfall since 1963, and inflicted significant economic losses in the United States of America, while heavy rains and floods affected eastern and southern Asia.

WMO has issued annual climate reports for more than twenty years and submits them to the Conference of the Parties of the Framework Convention on Climate Change. The annual statements complement the assessments reports that the Intergovernmental Panel on Climate Change (IPCC) produces every six to seven years.

It will be presented to UN member states and climate experts at a high-level action event on Climate Change and the Sustainable Development Agenda in New York on 23 March (World Meteorological Day) hosted by the President of the UN General Assembly Peter Thomson.

"The entry into force of the Paris Agreement under the UN Framework Convention on Climate Change (UNFCCC) on 4 November 2016 represents a historic landmark. It is vital

that its implementation becomes a reality and that the Agreement guides the global community in addressing climate change by curbing greenhouse gases, fostering climate resilience and mainstreaming climate adaptation into national development policies," said Taalas.
"Continued investment in climate research and observations is vital if our scientific knowledge is to keep pace with the rapid rate of climate change," said Taalas.

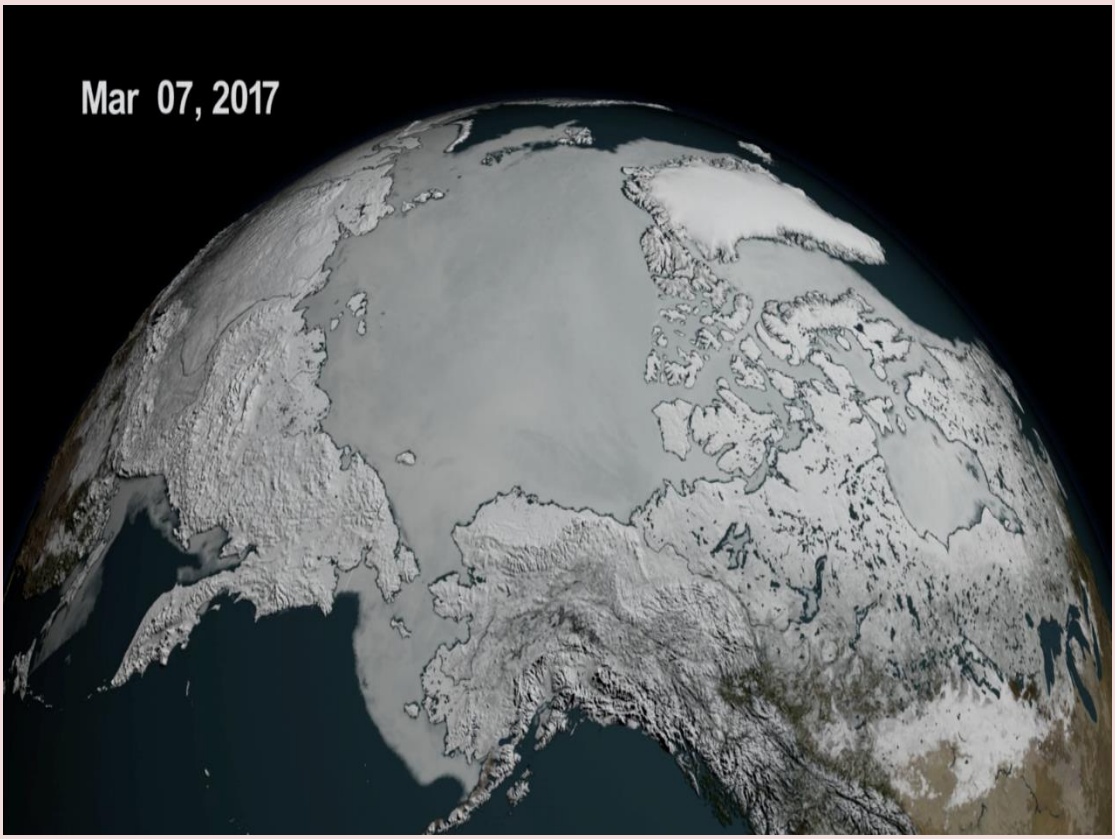
Extremes continue in 2017
Newly released studies, which are not included in WMO's report, indicate that ocean heat content may have increased even more than previously reported. Provisional data also indicates that there has been no easing in the rate of increase in atmospheric carbon dioxide concentrations.
"Even without a strong El Niño in 2017, we are seeing other remarkable changes across the planet that are challenging the limits of our understanding of the climate system. We are now in truly uncharted territory," said World Climate Research Program Director David Carlson.
At least three times so far this winter, the Arctic has witnessed the Polar equivalent of a heatwave, with powerful Atlantic storms driving an influx of warm, moist air. This meant that at the height of the Arctic winter and the sea ice refreezing period, there were days which were actually close to melting point. Antarctic sea ice has also been at a record low, in contrast to the trend in recent years.
Scientific research indicates that changes in the Arctic and melting sea ice is leading to a shift in wider oceanic and atmospheric circulation patterns. This is affecting weather in other parts of the world because of waves in the jet stream – the fast moving band of air which helps regulate temperatures.
Thus, some areas, including Canada and much of the United States, were unusually balmy, whilst others, including parts of the Arabian peninsula and North Africa, were unusually cold in early 2017.
In the United States alone, 11,743 warm temperature records were broken or tied in February, according to the U.S. National Oceanic and Atmospheric Administration. Prolonged and extreme heat in January and February affected New South Wales, southern Queensland, South Australia and northern Victoria, and saw many new temperature records.

Other highlights of the 2016 Statement

Global Temperatures
2016's warmth extended almost worldwide. Temperatures were above the 1961-90 average over the vast majority of the world's land areas, the only significant exceptions being an area of South America centered on central Argentina, and parts of south-western Australia.
Mean annual temperatures at least 3 °C above the 1961-1990 average occurred in various high-latitude locations, particularly along the Russian coast and in Alaska and far north-western Canada, and on islands in the Barents and Norwegian Seas. In the high Arctic, Svalbard (Norway) Airport's 2016 mean annual temperature of −0.1 °C was 6.5 °C above the 1961-1990 average, and 1.6 °C above the previous record.
Outside the Arctic, 2016's warmth was more notable for its consistency across the globe than for its extreme nature in individual locations.

Oceans
Globally averaged sea surface temperatures in 2016 were the warmest on record. The anomalies were strongest in the early months of 2016.
Global ocean heat content was the second-highest on record after 2015. It reached new record highs in the northern hemisphere, but was cooler in the southern hemisphere.
Globally, sea level has risen by 20 cm since the start of the twentieth century, mostly due to thermal expansion of the oceans and melting of glaciers and ice caps. Global sea levels rose very strongly during the 2015-2016 El Niño, rising about 15 millimeters between November 2014 to a new record high in February 2016. This was well above the post-1993 trend of 3 to 3.5 mm per year. From February to August, sea levels remained fairly stable as the influence of the El Niño declined. Final 2016 sea level data are not yet available at the time of writing.

Arctic sea ice



The seasonal maximum, of 14.52 million square kilometers on 24 March, was the lowest in the 1979-2016 satellite record. The 2016 autumn freeze-up was exceptionally slow – with sea ice extent even contracting for a few days in mid-November.

Precipitation

Much of southern Africa began the year in severe drought. For the second year in succession, rainfall was widely 20 to 60 percent below average for the summer rainy season (October to April) in 2015-2016. The World Food Program estimating that 18.2 million people would require emergency assistance by early 2017.

Provisional figures showed 2016 was the driest on record over the Amazon Basin, and there was also significant drought in north-east Brazil. El Niño brought drought conditions elsewhere in Central America and northern South America.

The Yangtze basin in China experienced, overall, its most significant flood season since 1999, with some tributaries experiencing record flood levels. Averaged over China as a whole, it was the wettest year on record, with national mean rainfall of 730 mm being 16 percent above the long-term average.

Heatwaves

The year started with an extreme heatwave in southern Africa in the first week of January. On 7 January, it reached 42.7 °C at Pretoria and 38.9 °C at Johannesburg, both of which were 3 °C or more above the all-time records at those sites.

Extreme heat also affected South and South-East Asia in April and May, prior to the start of the summer monsoon. South-East Asia was badly affected in April. A national record of 44.6 °C was set at Mae Hong Son, Thailand, on 28 April, and 51.0 °C was observed on 19 May at Phalodi, the highest temperature on record for India.

Record or near-record temperatures occurred in parts of the Middle East and north Africa. The highest temperature observed was 54.0 °C at Mitribah (Kuwait) on 21 July which (subject to ratification) will be the highest temperature on record for Asia. Other extremely high temperatures included 53.9 °C at Basra (Iraq) and 53.0 °C at Delhoran (Islamic

Republic of Iran – a national record), both on 22 July, whilst significant high temperatures were also reported in Morocco, Tunisia, Libya, and the United Arab Emirates.
A late-season heatwave affected many parts of western and central Europe in the first half of September. In southern Spain, 45.4 °C was recorded at Cordoba on 6 September.