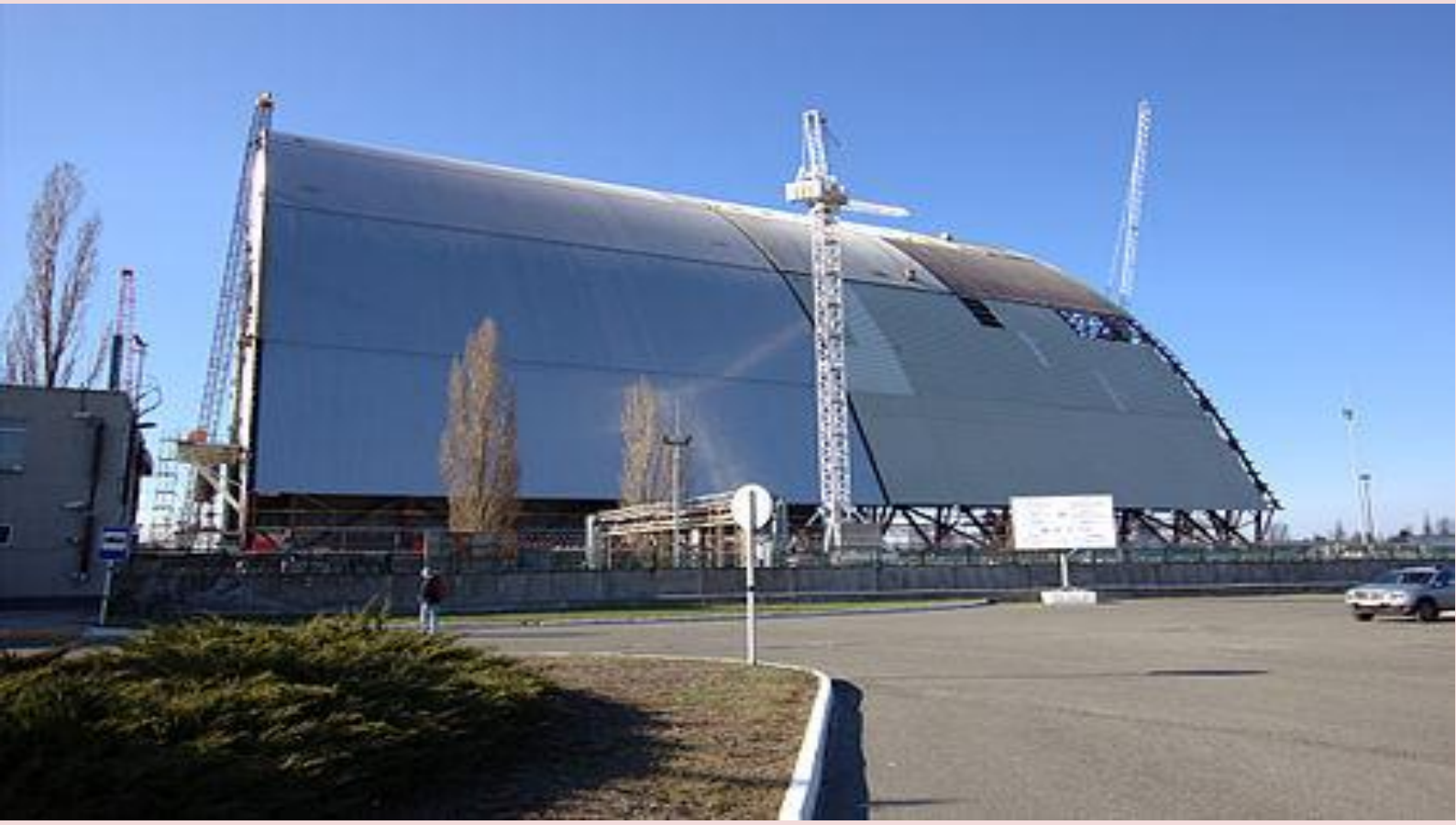

International
CBRNE
Institute
CBRNE
December 2016
NEWSLETTERRORISM
E-Journal for CBRNE & CT First Responders
CBRNE-Terrorism Newsletter
W
O
M
D
20
17
Thank you
First Responders!
www.cbrne-terrorism-newsletter.com

Dome installed over Chernobyl to prevent further fallout

Source: http://www.news.com.au/technology/environment/conservation/dome-installed-over-chernobyl-to-prevent-further-fallout/news-story/9bbbbc1ac24c28a6213d86b5f14c31e1

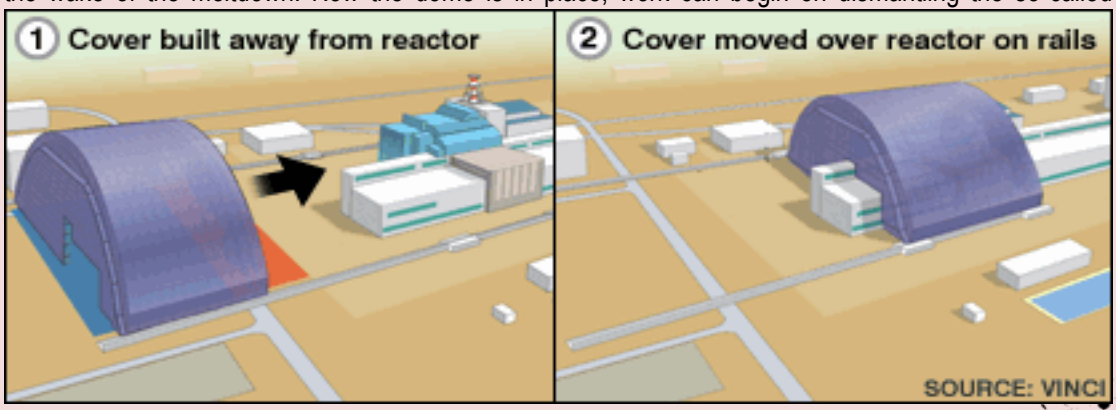
Nov 29 – **Researchers in Europe have built the world's largest land-based moving structure to cover the nuclear fallout from Chernobyl, the power plant that suffered a catastrophic meltdown in 1986.**



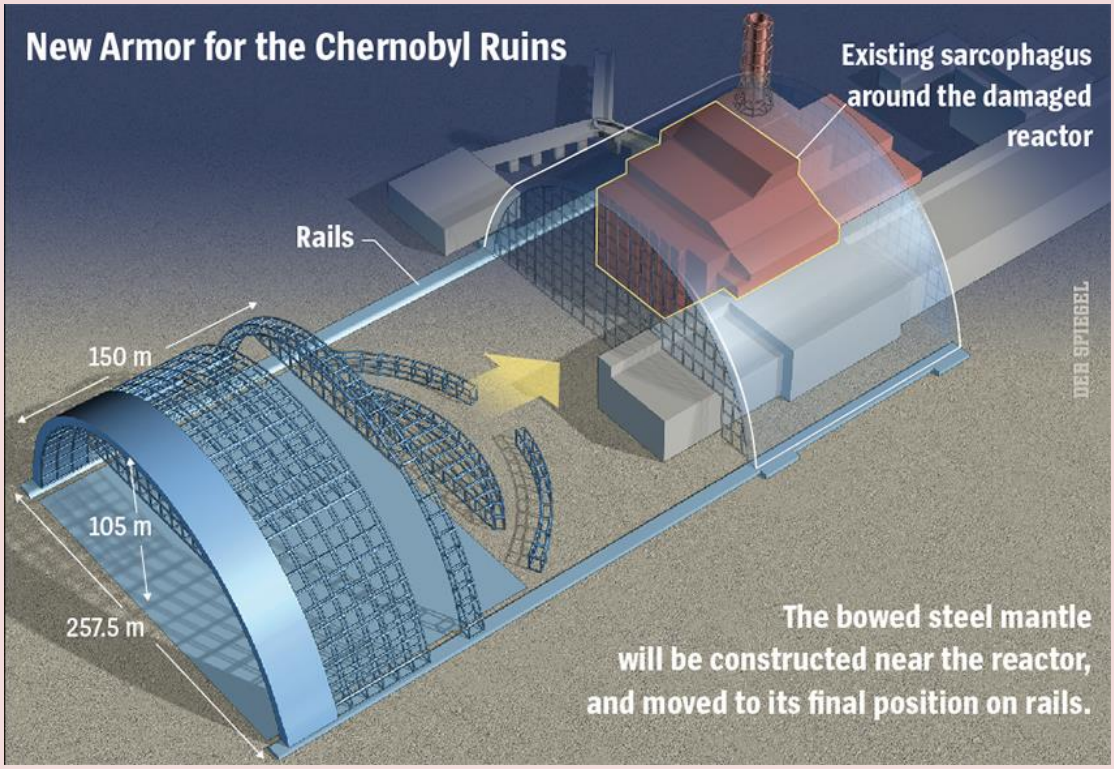
The mega structure was unveiled at the site in Ukraine this week and is designed to prevent further deadly radiation spewing from Chernobyl for at least the next century.

The massive arched dome is dubbed The New Safe Containment and **cost 1.5 billion euros to build.**

It has now been moved on top of the concrete that was hastily poured over the failed nuclear reactor in the wake of the meltdown. Now the dome is in place, work can begin on dismantling the so-called



sarcophagus surrounding the reactor, built to contain the fallout from the explosion 30 years ago.
The Chernobyl disaster in the then Soviet Ukraine was the worst civil nuclear accident in history. Thousands of people were exposed, with radiation spreading through Europe.



The gargantuan structure weighs in at around 36,000 tonnes, is 108 metres high and 162 metres long.

"The New Safe Confinement is an unprecedented engineering success. It is an extremely complex structure build in a contaminated area," said Vince Novak, the nuclear safety director from the European Bank for Reconstruction and Development.
"It's one of the most important projects ever done. People in Ukraine and not only Ukraine — across Europe and large parts of the world — still remember the 1986 accident," Mr Novak told Reuters.
The hi-tech covering of the disaster zone has been "eagerly awaited" and is "huge news and not only for people of Ukraine, for people of Europe, people of the world. It's a huge technological achievement."
To minimise risk to those involved the structure was mostly built away from the site and slid onto the area this week.
Even with the concrete sarcophagus that has encased the failed reactor, there was still the chance radiation could leak out or the concrete building would collapse.
"Now with the New Safe Confinement even if this happens, nothing will leak out in the environment. Yes, it will create a mess within the New Safe Confinement, nobody wants this to happen. And this is why part of the strategy is this early deconstruction of the most unstable part," Mr Novak said.

The legcy of Chernobyl

Reactor Number 4 of the Chernobyl nuclear power plant exploded during an experimental safety check in the middle of the night on **April 26, 1986**. It spewed radioactive contents up to one kilometre into the sky, some falling as debris in the area while the rest was blown by the wind as far as western Europe.

Thirty rescue workers and plant staff, receiving abnormally high doses of radiation, were killed at the site either immediately or in the coming weeks.

The noxious plumes drifted to the northwest, polluting the Soviet republics of Ukraine, Belarus and Russia. The harmful clouds then reached Scandinavian countries before swinging southward and westwards, dropping contaminated rain on central Europe and the Balkans, Italy, France, Britain and Ireland.

Soviet authorities remained silent on the disaster for three days without informing people in nearby villages about the need to evacuate. The official news agency TASS only reported on the accident on April 28 after the Forsmark nuclear plant in Sweden detected unusually high radiation in the environment.

One of the Chernobyl firemen who fought the blaze and subsequently died a few weeks later.

One hundred thousand people were eventually evacuated from an area within 30 kilometres of the plant only weeks later.

In November 1986 a 50-metre-high concrete shelter, dubbed a sarcophagus, was completed to prevent further leakage of radiation from tonnes of highly radioactive magma and allow the other three reactors at Chernobyl to continue producing power for Ukraine.

The concrete sarcophagus was only meant to be temporary and expected to last a couple of decades. But in 1993 its lifespan was estimated at only seven years.

In December 2000 after years of international pressure, the Ukraine government finally agreed to switch off the last reactor at the site and close down the Chernobyl facility.

Brian M. Jenkins and John Lauder: The Nuclear Terrorism Threat: How Real Is It?

Source: http://npolicy.org/article_file/1602-The_Nuclear_Terrorism_Threat.pdf

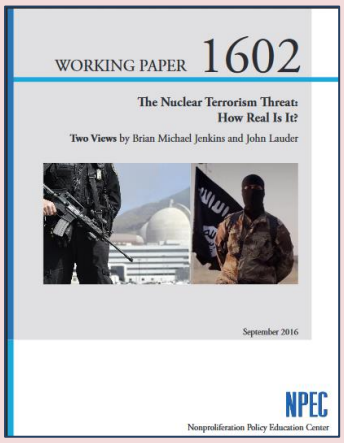
Aug 26 – NPEC Working Paper 1602, "The Nuclear Terrorism Threat: How Real Is It?" presents two opposed views on the threat of nuclear terrorism. **Brian M. Jenkins**, a Rand analyst and a leading expert on nuclear terrorism, argues that the threat is overblown. **John Lauder,** former director of the Central Intelligence Agency's Nonproliferation Center,

argues the opposing case that the threat is growing and we need to be hedging against it now.

INTRODUCTION

How Real Is Nuclear Terrorism?

After the Cold War and nearly 70 years of waging war against communism, the United States and its key allies have adopted the war against terror as their new organizing principal. The king of terrorist threats, however, is nuclear terrorism. As Vice President Dick Cheney once argued, "if there is a one percent chance" of a terrorist developing a nuclear weapon, "we have to treat it as a certainty in terms of our response."[1]



This raises the question, though, just how real is the threat of nuclear terrorism. This working paper presents two opposed views. The first is by Brian M. Jenkins, A RAND analyst and one of the world's leading experts on nuclear terrorism. He argues that the threat of nuclear terrorism is overblown. He recommends officials see it as a lesser included threat to that of the acquisition and possible use of nuclear weapons by states. What we need to do to prevent states from getting nuclear weapons and to secure existing nuclear weapons and fissile materials against sabotage or illicit seizure will largely take care of the more distant prospect of terrorists making nuclear bombs.

A second and opposing view is offered by John Lauder, former director of the Central Intelligence Agency's Nonproliferation Center, who argues that the threat of nuclear terrorism is growing and we need to be hedging against this now.

It would be a mistake to think either of these views is wrong. The trick is figuring out which to emphasize and how much. This set of questions are worthy of discussion and debate.

Henry D. Sokolski

September 2016

Notes

1. Michiko Kakutani, "Personality, Ideology and Bush's Terror Wars," The New York Times, June 20, 2006, available at http://www.nytimes.com/2006/06/20/books/20kaku.html?_r=0.

Living in a radioactive world

By P. Andrew Karam

Source: http://www.cbrneportal.com/living-in-a-radioactive-world/

Dec 05 – Natural radioactivity can make things fun for radiation safety professionals like me – it gives us a chance to tell the public that radiation isn't quite as harmful as they might think, for example, and it lets us confirm that our instruments are working properly. But it does carry with it some drawbacks. For example, we can't clean up a site properly (especially one contaminated with naturally occurring radioactivity) unless we know what was there to begin with. And if natural radiation is everywhere then those who are frightened of radiation always have something to be worried about. Not only that, but if you're responsible for interdiction – trying to find subtle indications of a radiological or nuclear weapon – then background radiation can complicate your job considerably.

First, let me talk a bit about background radiation. There is always radiation in our environment and your instruments should always have a reading above zero. This comes from natural radioactivity in our own bodies, from cosmic radiation, and from radioactivity in rocks and soils (and things made from them). If you're responsible for a fixed location (a city, for example) then your readings from cosmic radiation and from the radioactivity in peoples' bodies won't be changing much. But in a city, the local architecture can have a significant impact on your radiation readings and if you don't account for this then you can end up missing something, or responding to an elevated reading that doesn't amount to anything. **Here are some examples of things I've seen, ranging from fairly straightforward to a bit of a head-scratcher.**

1. As one example, I was doing a radiation survey once and realized that I was seeing radiation levels higher than what I expected. As I approached a building my detector

sounded an alarm, which had me concerned. I knew that granite could cause elevated readings (gray, pink, and red granites often contain elevated levels of natural radioactivity), but I didn't see any granite buildings in the area. I was finally able to determine that the elevated radiation readings were coming from a brick building in front of me and approached it. I surveyed the building, assuming that radiation was shining through the bricks from something on the inside, but I noticed that the levels were remarkably uniform – everyplace I checked had almost identical readings. This had me stumped because if somebody was hiding radioactivity in a particular room I should see a "hot' spot. I finally realized that the radiation was coming from the bricks – more precisely, from naturally radioactive potassium in the clays from which the bricks were made.

2. Another incident happened to me near a natural gas processing plant. In this case, we not only got elevated radiation readings, but one of our RIIDs (a RIID is a RadioIsotope IDentifier) identified the presence of highly enriched uranium. For a number of reasons we were confident that there was none of that in the area, but we still had to explain the reading. In this case, it was important to remember that oil and natural gas deposits are associated with elevated levels of uranium. Not only that, but one of the decay products of uranium is radium-226 – anyplace you find uranium, you're also going to find the radium (where it comes from is the decay of U-238, which decays through over a dozen steps before turning into stable lead). Radium-226 turns out to emit gamma radiation with an energy that's almost identical to that of U-235, the isotope from which reactor fuel and nuclear weapons are made. The gamma radiation emitted by U-235 is so close to that of Ra-226 that the most common type of RIID can't "see" the difference. So in this case, it was natural radium from the nearby natural gas facility that was causing the elevated radiation dose rates and that was fooling our RIID. In this case, we confirmed this hypothesis by identifying other natural radionuclides from the uranium decay series. We could also have used a very precise type of RIID (called a high-purity germanium detector), which is sensitive enough to distinguish between Ra-226 and U-235, but didn't need to in this case.

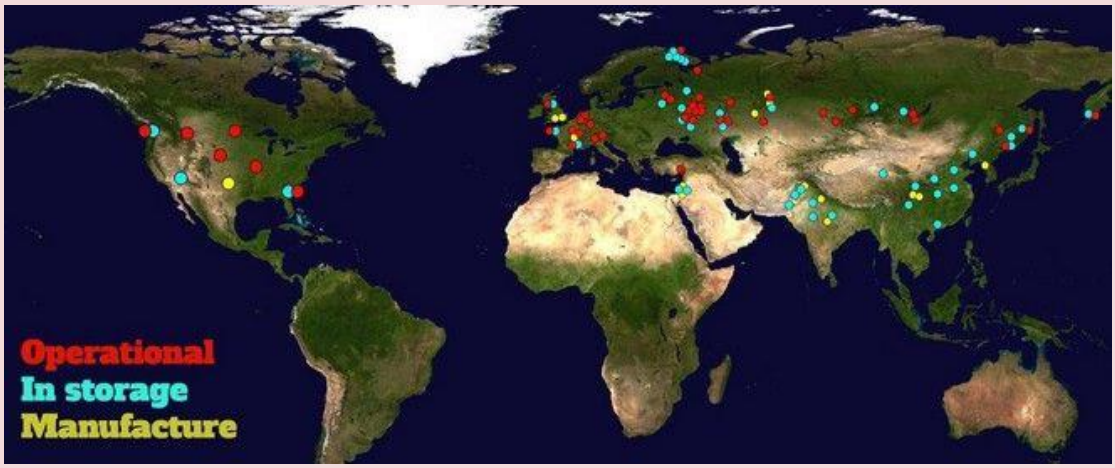
▶▶ **Read the rest of this article at source's URL**.

Andrew Karam *is a radiation safety expert with 35 years of experience, beginning with 8 years in the US Navy's Nuclear Power Program that included 4 years on an attack submarine. He has published over two dozen scientific and technical papers and is the author of 16 books and several hundred articles for general audiences. He has worked on issues related to radiological and nuclear terrorism for over 10 years.*

France's Choice for Naval Nuclear Propulsion: Why Low-Enriched Uranium Was Chosen

This special report is a result of an FAS task force on French naval nuclear propulsion and explores France's decision to switch from highly-enriched uranium (HEU) to low-enriched uranium (LEU). By detailing the French Navy's choice to switch the LEU fuel, author Alain Tournyol du Clos — a lead architect of France's nuclear propulsion program — explores whether France's choice is fit for other nations. **Read or download.**

Sleeping better (???) if you live in Africa, South America or Australia…



Could Isil actually detonate a nuclear 'dirty bomb' in Britain?

By Hamish de Bretton-Gordon

Source: http://www.telegraph.co.uk/news/2016/04/05/could-isil-actually-detonate-a-nuclear-dirty-bomb-in-britain/

April 2016 – Last week's Nuclear Security Summit in Washington DC put the threat of Isil using some sort of fissile or radioactive material in the media spotlight.

If Isil could build an Improvised Nuclear Device (IND) or a "Dirty Bomb" they would certainly use it, and all the better for them if were able to use it in London, Paris or New York.

It would appear that the Isil terror attacks in Belgium two weeks ago were originally planned to have some sort of nuclear element, but through good intelligence-gathering and some luck this nightmare scenario was avoided, for now.

It is possible that some of the 15,000 or more nuclear warheads quoted by Eric Schlosser in his recent book Gods of Metal may be poorly guarded and could fall into terrorist hand, but it is highly improbable. At the end of the Cold War, international efforts were made to secure the most vulnerable storage locations, including the removal of 600 kilograms of weapons-grade uranium under Project Sapphire from Kazakhstan to the US.

But beyond this, having been involved in nuclear security in the UK, I am acutely aware of the challenges and hurdles required for a terror group to successfully smuggle a viable device to a suitable target location and then override the numerous safety features to detonate such a weapon. It's all very unlikely.

In my opinion the real areas of concern in future are, firstly, the development of North Korea's nuclear capability and its "apparent" intercontinental ballistic missile programme; secondly, the possibility of highly enriched, weaponised isotopes falling into terrorist hands through the black market or dark web to build an IND; thirdly, using commonly available radiological sources to create a dirty bomb. These are in ascending order of likelihood.

I am relatively confident that the five permanent members of the UN Security Council, and in particular the US, are keeping a very close eye on North Korea and would take offensive action if it appeared that this country was about to launch some kind of nuclear-tipped missile. It would appear that this is still some way off at the moment.

The next concern is the possibility that nuclear weapons-grade viable material is acquired by Isil and fashioned into an IND. 15-20 kilograms of Highly Enriched Uranium (HEU), with a simple "gun-gadget" initiation device, could yield a blast equivalent to 2000 tonnes of TNT, which would be enough to flatten several blocks. This is probably within the capabilities of Isil's scientists in Iraq and Syria, technically. But I very much doubt they could explode this type of weapon in any P5 member – except perhaps Russia.

It is here that Isil would most likely get the HEU, and it is Chechen jihadists who appear to be at the heart of Isil's chemical, radiological and nuclear weapons programmes. It is the Russians who are the Chechens' greatest enemy, and indeed Chechen militants have used fissile material before to attack the Russian State. With this in mind it is somewhat surprising that President Putin decided to boycott the Nuclear Summit, which aims to prevent such an attack.

What the public appear most afraid of, and what is most likely, is a "dirty" bomb. But this fear is misguided. The only immediate casualties of such an attack would probably be from the blast rather than radiation, which would be unlikely to have many short or long term medical effects. Though radiological material is relatively easy to source, the UK's sophisticated counter-terrorist apparatus would make it extremely unlikely that Isil could detonate such a bomb here.

In sum, the threat to the UK from an Isil nuclear device is extremely low, and only slightly higher for a dirty bomb attack. Still, the psychological impact would outweigh the physiological by many times to 1. Pre-warned and prepared is the best form of defence in this case.

Hamish de Bretton-Gordon *is a chemical weapons adviser to NGOs working in Syria and Iraq. He is a former commanding officer of the UK Chemical, Biological, Radiological and Nuclear (CBRN) Regiment and NATO's Rapid Reaction CBRN Battalion.*

Radiation-related injuries and their management: an update

Semin Intervent Radiol. 2015; 32(2):156-62 (ISSN: 0739-9529)

By Wunderle K and Gill AS

Source: http://reference.medscape.com/medline/abstract/26038622

Ionizing radiation (in the form of X-rays) is used for the majority of procedures in interventional radiology. This review article aimed at promoting safer use of this tool through a better understanding of radiation dose and radiation effects, and by providing guidance for setting up a quality assurance program. To this end, the authors describe different radiation descriptive quantities and their individual strengths and challenges, as well as the biologic effects of ionizing radiation, including patient-related effects such as tissue reactions (previously known as deterministic effects) and stochastic effects. In this article, the clinical presentation, immediate management, and clinical follow-up of these injuries are also discussed. Tissue reactions are important primarily from the patients' perspective, whereas stochastic effects are most relevant for pediatric patients and from an occupational viewpoint. The factors affecting the likelihood of skin reaction

(the most common tissue reaction) are described, and how this condition should be managed is discussed. Setting up a robust quality assurance program around radiation dose is imperative for effective monitoring and reduction of radiation exposure to patients and operators. Recommendations for the pre-, peri-, and postprocedure periods are given, including recommendations for follow-up of high-dose cases. Special conditions such as pregnancy and radiation recall are also discussed.

Russia starts Phase 2 construction at Iran's Bushehr nuclear power plant

Source: https://www.rt.com/news/358887-russia-iran-bushehr-plant/

Sep 10 – **Phase 2, which was launched on Saturday, will add two VVER-1000 reactors to the one already operating in Iran.** Their design was updated with additional safety features based on experience derived from the Fukushima nuclear disaster.

Russia and Iran signed a contract for the expansion of Bushehr in 2014, a year after Russian specialists commissioned the plant's first reactor. The contract includes an option for six more reactors, which could be built at other sites sometime in the future. Phase 3 may be commenced as soon as 2018, Iranian Vice-President Eshaq Jahangiri said during the ceremony.

The Bushehr project was launched in 1975 under the shah's government, but it ground to a halt after the Islamic revolution of 1979 because German manufacturers withdrew. Russia's nuclear construction company Atomstroyexport took over the project in the 1990s.

"The competition of Phase 1 has proven that Russia always delivers on its promises to foreign partners, regardless of the political climate in the world," said Russian nuclear chief Sergey Kirienko during the opening ceremony in Iran.

"Phase 2 is [Russia's] practical contribution to fostering Russian-Iranian cooperation and a big step forward in strengthening Russia's position in the world nuclear technology market."

The Bushehr plant is the first nuclear power facility in the Arab Middle East. **Tehran estimates that each 1,000 MW reactor will save Iran 11 million barrels of crude annually.** Iran is eyeing several ways to spend the additional megawatts, including powering a water desalination plant in Bushehr province.

"The plant would produce 200,000 cubic meters of freshwater per day, compared to the 50,000 to 60,000 cubic meters per day the province needs," said Iranian Atomic Energy Organization head Ali Akbar Salehi.

As part of the project, which is seen as a step in fulfilling Iran's ambition to develop a civilian nuclear industry, Russian specialists will also train Iranian staff working at the nuclear plant.

Iran to develop nuclear propulsion for maritime use, cites US 'violation' of deal

Source: https://www.rt.com/news/370132-iran-nulclear-marine-propulsion/

Dec 13 – The Iranian president has ordered the national nuclear agency start developing nuclear propulsion capability for marine transportation. Hassan Rouhani said the move is response to US 'violation' of the nuclear deal with Iran.

Rouhani's Tuesday order to Ali Akbar Salehi, the head of the Atomic Energy Organization of Iran, says the agency must prepare **a project for development of both reactors for maritime use and fuel production for this purpose in three months**.

Nuclear propulsion uses a nuclear power reactor to generate electricity on a vessel. Such systems are best known for their use on strategic nuclear submarines, which allow them to stay submerged for weeks avoiding detection. Nuclear propulsion is also used on some big surface ships like aircraft carriers or icebreakers.

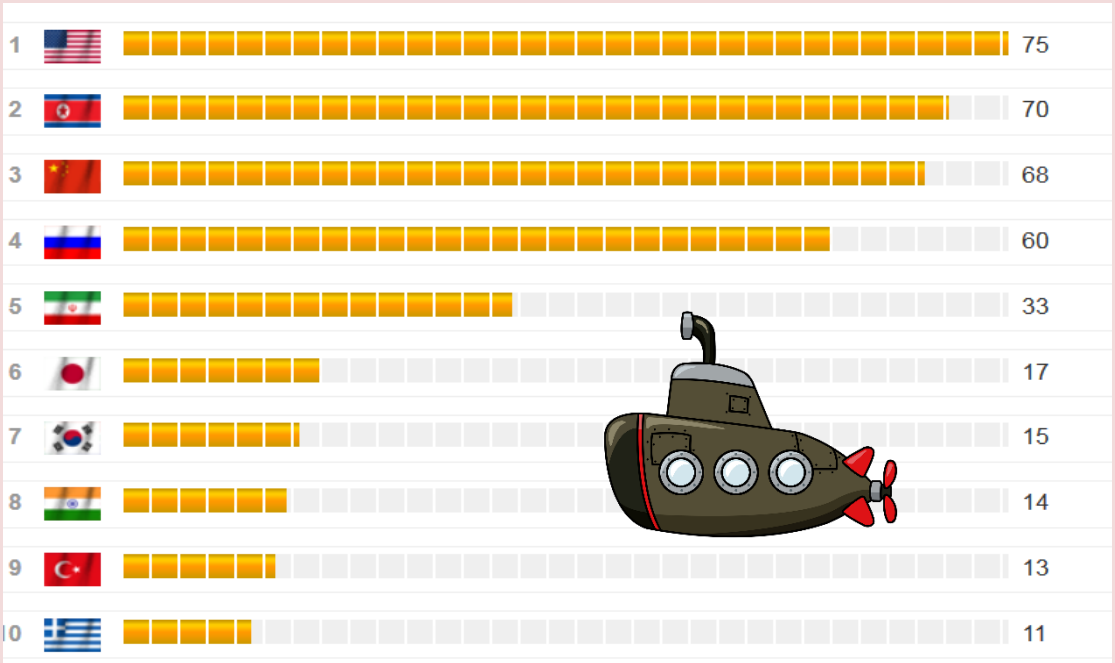
The technology is different from nuclear weapons, but has a definite military leaning. **The only operator of nuclear-powered civilian vessels at the moment is Russia, mostly due to its fleet of icebreakers.** The US and Germany had nuclear-propelled merchant ships in the past, while the Japanese ship 'Mutsu' was finished but never carried commercial cargo.

The Iran nuclear deal was negotiated by Tehran and six leading world powers. It sought to address concerns that Iran may have a clandestine project to develop nuclear weapons. Iran denied the accusation, but agreed to restrict its nuclear industry in exchange for the lifting of economic sanctions imposed by the UN Security Council, the US and the EU.

The deal was hailed as a breakthrough at the time of its signing in 2015 by all parties involved, despite dissenting voices from Republicans in the US, hardliners in Iran and Israel in the Middle East. Iran has since held its part of the bargain and is complaining that the US continues its anti-Iranian policy and imposes new sanctions under different pretexts.

Commenting on the December prolongation of the Iran and Libya Sanctions Act of 1996 (ILSA), Iranian Supreme Leader Ayatollah Khamenei warned that it puts the nuclear deal in jeopardy.

There is also concern that the deal would be targeted by US President-elect Donald Trump after he takes office on January 20. In a recent interview Israeli Prime Minister Benjamin Netanyahu said he has at least five ideas in mind for Trump to undermine the nuclear deal with Iran.



Top 10 submarine nations (2016)

Source: NTI (Aug 2015)(http://www.nti.org/analysis/articles/iran-submarine-capabilities/)

Iran's submarine force currently consists of three Russian Kilo-class (4,000 ton) diesel-electric submarines (Tareq 901, Noor 902, Yunes 903), one 350-400-ton Nahang and an

expanding force of roughly a dozen 150-ton Ghadir-class (Qadir/Khadir) midget submarines. The Iranian Navy plays a crucial strategic role in Iran's national security architecture due to Tehran's dependence on the Persian Gulf for trade and security. However, its naval forces also operate in the Gulf of Oman, the Caspian Sea and, possibly, the Indian Ocean.

Dec 4, 2016 (http://theiranproject.com/blog/tag/irans-fateh-submarine/)
A top Iranian Navy commander says the Islamic Republic will soon launch a new domestically-manufactured submarine.
"The Fateh (Conqueror) submarine with a 100-percent domestically-sourced technology will join Iran's Navy and become operational soon," Rear Admiral Siavash Jarreh, a senior advisor to the Iranian Navy Commander Rear Admiral Habibollah Sayyari, told IRNA on Sunday.

He added that few countries in the world are capable of manufacturing submarines and thanks to the great efforts of Iranian experts and reliance on domestic know-how, the Islamic Republic currently enjoys such a capability along with China, the US, Russia, France and Britain.
Iran's Navy deployed its first submarine some two decades ago and has succeeded in acquiring advanced technology in this sector despite all the sanctions imposed against the country, he said.
Iran has so far launched different classes of domestically-built advanced submarines including Ghadir, Qaem, Nahang, Tareq and Sina. The 600-ton Fateh is among semi-heavy submarines and is equipped with state-of-the-art weaponry such as torpedoes and marine mines.

EDITOR'S COMMENT: It was quite confusing to locate the exact number of Iranian submarines – perhaps the most detailed list is (without the Fateh), at:
https://en.wikipedia.org/wiki/List_of_current_ships_of_the_Islamic_Republic_of_Iran_Navy

Tom Ridge and Joseph Lieberman: How Donald Trump Can Protect America from Bioterrorism

By Tom Ridge and Joseph Lieberman
Source: http://time.com/4598145/donald-trump-biological-terrorism/

Dec 13 – Leaders from more than 120 nations just concluded the Eighth Biological Weapons Convention Review Conference in Switzerland, which focused on the threat posed by biological terrorism. During the conference, the U.S. delegation urged countries to reduce that threat by implementing strategies for detecting and responding to bioweapons. **The United States needs to heed its own advice.** The country has been and continues to be ill prepared for a biological attack.

When President-elect Trump assumes the Oval Office this January, he has a unique opportunity to fulfill his promise to make America safe again—by taking steps to protect the nation from bioterrorism.

More than a year ago, the bipartisan Blue Ribbon Study Panel on Biodefense, which we chair, issued 87 recommendations for improving America's biodefenses. They are easily achievable and require little extra funding. But they'd vastly improve our ability to detect, prevent and respond to biological attacks and major outbreaks.

Fifteen years after the deadly anthrax attacks in the U.S., and more than two years after Ebola reached America, our nation still lacks a centralized leader to coordinate prevention and response activities to these kinds of events. We also have no strategic plan or unified approach to coordinate the biodefense budgets of more than a dozen agencies.

In a new report, we have found that the government has made progress on just 17 of our recommendations and completed only two. Forty-six could have been accomplished by now.

We've known about biological risks for a long time. In 1999, President-elect Trump himself warned in his book *The America We Deserve* about the need to better prepare for the threat of bioterrorism by stockpiling medicines, for instance. **Yet by 2010**, a report from a bipartisan commission on the proliferation of weapons of mass destruction had given the country an "F" for readiness against a bioterrorism attack.

The risk has only increased. Earlier this year, the Director of National Intelligence cautioned Congress about the ease with which bioweapons could move around the globe. Belgium has found members of ISIL in possession of biological weapons materials. **Turkish officials recently uncovered an ISIL plot to contaminate the country's water supplies.** This spring, Kenya said they foiled a plan by the Islamic State to unleash anthrax in the east African nation.

Then there are the risks from naturally occurring pandemics—like the recent Zika and Ebola crises—or the repeated biological accidents by our own government labs. One federal report found that U.S. labs had mistakenly exposed nearly 1,000 workers to pathogens 199 times over just one year.

Such attacks could be devastating. An attack on our nation's agricultural sector, for instance, could prove catastrophic. The agricultural supply chain is a trillion–dollar business and employs almost one in every ten American workers.

So what should President-elect Trump and the 115th Congress do when they take office?

For his part, Mr. Trump should immediately put the vice president in charge of the nation's biodefense efforts. The absence at the White House of an individual with this kind of authority has led to disjointed interagency efforts and financial inefficiency, as the government's responses to Ebola and Zika have demonstrated. The vice president should have the authority to review and advise on biodefense budget matters and to oversee a biodefense coordination council that includes representatives from the private and public sectors.

Congress must streamline oversight. At least 20 congressional committees have biodefense jurisdiction, but few spend much time on the issue. When a crisis arises, they all lose time providing reactive oversight and fighting over jurisdiction.

The 115th Congress's leaders should instead put together a bicameral, comprehensive oversight agenda, host joint House-Senate hearings and consolidate jurisdiction.

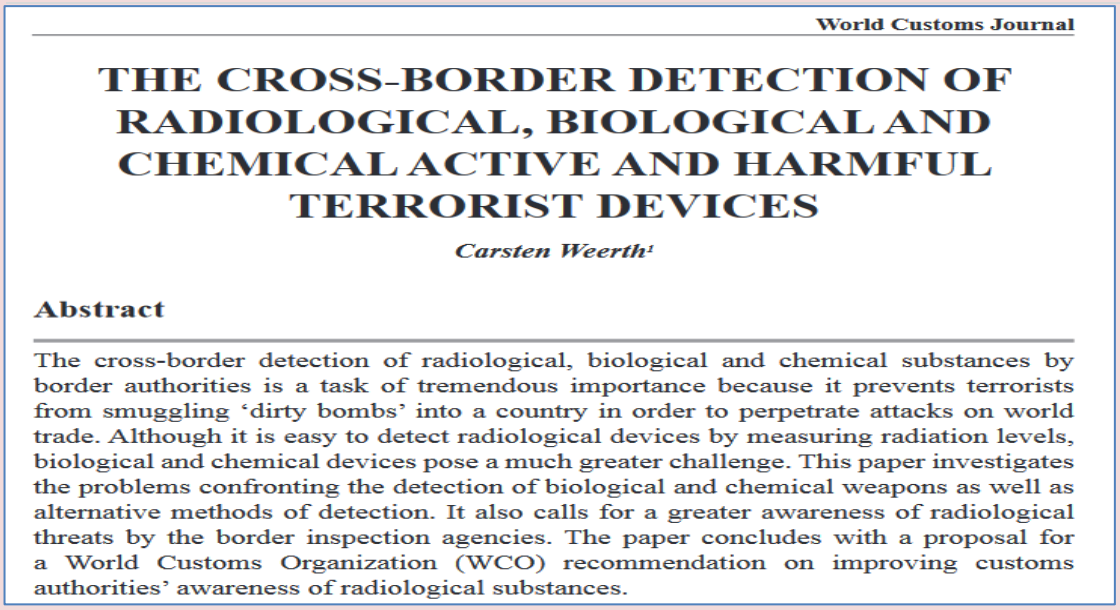
Lawmakers have started to take action. Congress just passed the National Defense Authorization Act, which will require the federal government to develop a comprehensive biodefense strategy. We also urge Congress to implement uniform budgeting and build preparedness measures into annual budgets, instead of relying on emergency funding bills that cost lives and financial resources.

These acts and the other measures we recommend don't involve significant new spending. Most simply require better use of existing resources.

Next year offers a real chance for our leaders to get biodefense right. The risks are clear. So are the solutions. President-elect Trump and the new Congress must simply enact them.

***Tom Ridge** served as governor of Pennsylvania and the first Secretary of Homeland Security.*

***Joseph Liberman** is a former Senator from Connecticut. They are co-chairs of the bipartisan Blue Ribbon Study Panel on Biodefense.*



World Customs Journal

THE CROSS-BORDER DETECTION OF RADIOLOGICAL, BIOLOGICAL AND CHEMICAL ACTIVE AND HARMFUL TERRORIST DEVICES

Carsten Weerth[1]

Abstract

The cross-border detection of radiological, biological and chemical substances by border authorities is a task of tremendous importance because it prevents terrorists from smuggling 'dirty bombs' into a country in order to perpetrate attacks on world trade. Although it is easy to detect radiological devices by measuring radiation levels, biological and chemical devices pose a much greater challenge. This paper investigates the problems confronting the detection of biological and chemical weapons as well as alternative methods of detection. It also calls for a greater awareness of radiological threats by the border inspection agencies. The paper concludes with a proposal for a World Customs Organization (WCO) recommendation on improving customs authorities' awareness of radiological substances.

Source:http://worldcustomsjournal.org/Archives/Volume%203,%20Number%202%20(Sep%202009)/08%20WCJ_V3N2_Weerth_(web).pdf

***Dr Carsten Weerth**, BSc (Glasgow), PhD, is a customs law expert (Diplom-Finanzwirt from the Fachhochschule des Bundes für öffentliche Verwaltung, Fachbereich Finanzen in Münster – University of Applied Sciences), a Customs officer, working with Germany's Federal Customs and Excise Service; and a frequent contributor to scientific journals. He is the author of eight textbooks on European customs law, and a contributing lecturer with the Hochschule für Öffentliche Verwaltung, Bremen, University of Applied Sciences. The topic of his PhD thesis was 'Uniform Application of the Common Customs Tariff at Market Entry to the Common Market?, published Sierke Verlag, Göttingen, 2007.*

"Nightmare scenario": Nuclear power plants vulnerable to hacking by terrorists

Source: http://www.homelandsecuritynewswire.com/dr20161216-nightmare-scenario-nuclear-power-plants-vulnerable-to-hacking-by-terrorists

Dec 16 – Security experts fear Fukushima-like disaster as terrorists use new technology to attempt attacks. Jan Eliasson, the deputy secretary-general of the United Nations, told the Security Council that a nightmare scenario – that is, radioactive material being released from nuclear power stations subject to cyberattacks by terrorists – is not far-fetched.

Eliasson said that "vicious non-state groups" were making efforts to acquire weapons of mass destruction (WMDs), and warned: "These weapons are increasingly accessible."

A hacking attack on a nuclear power plant would be a "nightmare scenario," he added.

NewsOK reports that terrorist groups such as ISIS and al-Qaeda have train to obtain WMDs, and ISIS operatives in Belgium had been following a scientist who worked at a nuclear power station, hoping to use him to gain access to the plant.

Eliasson noted that technological advances such as 3D printing, the growing use of drones, and the increasing sophistication of cyberattacks have made it easier for terrorists to acquire deadly weapons.

"Preventing a WMD attack by a non-state actor will be a long-term challenge that requires long-term responses," Eliasson said.

The UN convened the meeting to examine ways to prevent terrorists from getting hold of nuclear, chemical, and biological weapons.

Dr. Patricia Lewis, Research Director of the International Security Department at Chatham House, told the*Independent* a cyber-attack on a nuclear power station was "a real risk."

"There's an idea that the systems are protected…and that is a myth. Every system has vulnerabilities. We are seriously straying into what sounds like science fiction but isn't. We are there now," she said.

She added: "This isn't just imagined – this is already going on."

Nuclear plants have already been subject to attacks. In 2009 an attack on an Iranian facility had disrupted its nuclear enrichment program. Plants in South Korea and Germany have also come under cyberattacks.

These attacks were small, but bigger ones could have been disastrous.

Lewis warned the worst case cyber-attack could potentially cause "a Fukushima-style scenario."

She said: "It is probably beyond the capabilities of a non-state armed group but it may be very possible for a state to do that. Energy companies really need to understand the threat better [because] they don't yet. There are things going on that we don't fully understand."

Experts worry that attacks aiming to disrupt nuclear power stations, could also be launched against nuclear weapons facilities.

Lewis said: "When it comes to nuclear weapons the consequences are far higher. Even if the probabilities are lower, the risk is huge."

Attacks on nuclear power stations will not only release deadly radiation, but would also shut down the grid, wreaking economic havoc and risking public disorder, Lewis added.

Cyberattacks on nuclear power plants may have different goals. Some may aim to obtain data about the way the plant works or information on personnel at the facility; others may be ransom attacks, threatening the plant operator with damage unless money is paid.

Hacks may also see information about the layout and structure of nuclear reactors in preparation for a physical attack.

The frequency and scope of cyberattacks on nuclear plants have increased dramatically, and experts say that a successful hack is now all but inevitable. They say that nuclear plant operators should focus more on preparing to contain and limit the damage when it does occur.

Lewis said: "We need a different type of approach to cyber-security – one that doesn't imagine that you can completely defend against attacks.

"What we're trying to do is introduce a culture where you…expect the attacks and build in resilience so that when they come it doesn't really have much effect."

Is Iran cooperating with North Korea on a nuclear weapon?

Source: http://www.homelandsecuritynewswire.com/dr20161219-is-iran-cooperating-with-north-korea-on-a-nuclear-weapon

Dec 19 – Spurred by a letter written by Sen. Ted Cruz (R–Texas) to three senior Obama administration officials, investigative journalist Claudia Rosett on Thursday examined the possibility that Iran and North Korea are collaborating on nuclear weapons research in the wake of last year's nuclear deal.

The most salient question, Rosett wrote in *Forbes*, is the one Cruz addressed to Director of National Intelligence James Clapper: "Has the U.S. intelligence community observed any possible nuclear collaboration between Iran and North Korea…?"

She explained that the two nations have a history of collaborating on weapons development. Usually, North Korea undertakes much of the development while Iran that foots the bill, with technicians traveling back and forth between the countries.

Although there is currently no official confirmation from Washington that the two nations have collaborated in nuclear weapons development, their cooperation on ballistic missiles is well-documented. This raises the possibility, Rosett wrote, that "the two countries are also in nuclear cahoots, because ballistic missiles are basically cost-efficient only as vehicles for delivering nuclear warheads."

While Iran has publicly scaled back parts of its nuclear program in exchange for billions in sanctions relief, "cash-hungry North Korea has never been busier," Rosett pointed out.

North Korea is believed to have carried out two nuclear tests this year, bringing the total it has conducted since 2006 to five.

Rosett observed that it is odd for Iran to "pour resources into testing ballistic missiles," which are designed to carry nuclear warheads, if it has truly sworn off developing such weapons. This suggests that "North Korea's nuclear program might be secretly doubling as a nuclear backshop for Iran."

In his letter, Cruz raised concerns about a North Korean ballistic launch in September that, according to state media, **had a thrust of 80-ton — enough power to carry "a heavier, or less-minaturized nuclear warhead to the United States**." The eighty tons thrust was mentioned in a 17 January 2016 press release by the Treasury Department sanctioning Iranian entities for ballistic missile procurement. "Within the past several years, Iranian missile technicians from SHIG traveled to North Korea to work on an 80-ton rocket booster being developed by the North Korean government," the release noted.

While these link do not constitute proof of nuclear collaboration, they do raise red flags, Rosett wrote. "If the silent officials of the Obama administration are confident that there has been no nuclear cooperation between Iran and North Korea, it's time to put that assessment in writing and send it to Cruz," she concluded.

Rosett's concerns echo those expressed by Ilan Berman in the *National Interest* in August 2015, who wrote that for decades Iran and North Korea have forged a "formidable alliance – the centerpiece of which is cooperation on nuclear and ballistic-missile capabilities." He explained that for years reports have indicated that North Korea has actively worked to aid Iran's nuclear program. North Korea sent "hundreds of nuclear experts" to work in Iran, while making "key nuclear software" available to Iranian scientists.

After Pyongyang tested a nuclear weapon in early January, retired Army Maj. Gen. Robert Scales, a former commandant of the U.S. Army War College, told Fox News, "We know that the Iranians were at the last nuclear test a couple of year ago, [and] we know that the Iranians are helping the North Koreans miniaturize their nuclear weapons." He indicated that the North Korean nuclear program experienced several failures until it received assistance from Iran. "What does this say about our nuclear deal with Iran?" Scales asked. "It says Iran is able to circumvent it by using their technological colleagues in Pakistan and their test site facility in North Korea to push their own nuclear ambitions." He added that "the Iranians and North Koreans are both developing long-range ballistic missiles by collaborating together."

Later in January, researchers from the Foundation for Defense of Democracies published a research paper outlining Iran's past and present military dealings with North Korea, concluding that "the signs of military and scientific cooperation between Iran and North Korea suggest that Pyongyang could have been involved in Tehran's nuclear and ballistic-missile program, and that state-run trading companies may have assisted in critical aspects of Iran's illicit nuclear-related activities." They added that more needs to be known about Iranian-North Korean cooperation, recommending a number of measures, including getting China more involved in non-proliferation efforts, increasing the study of locations where Iran and North Korea focus their efforts on procuring sanctioned technologies, and ensuring the transparency of the international financial system.

In How Iran and North Korea Became Cyber-Terror Buddies, which was published in the January 2015 issue of The Tower Magazine, Rosett offered some background on the two rogue nations' history of joint missile development.

In recent decades, this relationship has proven particularly fruitful. In 1992, for example, a North Korean freighter slipped past U.S. Navy surveillance and delivered a cargo of Scud missiles to the Iranian port of Bandar Abbas. In 2003, a North Korean defector testified before Congress that he traveled from North Korea to Iran in 1989 and helped the Iranians test-fire a North Korean missile. In 2007, a secret State Department cable made public by Wikileaks stated,

Iran and North Korea have continued their longstanding cooperation on ballistic missile technology via air-shipments of ballistic-missile related items. We assess that some of the shipments consist of ballistic missile jet vanes that frequently transit Beijing on regularly scheduled flights of Air Koryo and Iran Air.

In 2010, a Congressional Research Service report by analyst Larry A. Niksch estimated that "**North Korea earns about $1.5 billion annually from missile sales to other countries.** It appears that much of this comes from missile sales and collaboration with Iran in missile development." Also in 2010, the *New York Times* reported that **Iran obtained 19 missiles from North Korea that were "much more powerful than anything Washington has publicly conceded that Tehran has in its arsenal**." This too was based on a classified State Department cable made public by Wikileaks. In 2013, a report from the National Air and Space Intelligence Center stated, "Iran has an extensive missile development program, and has received support from entities in Russia, China, and North Korea." Among Iran's ballistic missiles is the intermediate-range Shahab 3, based on North Korea's No Dong missile, with a range long enough to strike Israel.

Galway man gets 30 years for X-ray plot

Source: http://www.saratogian.com/general-news/20161219/galway-man-gets-30-years-for-x-ray-plot?source=most_viewed

Glendon Scott Crawford leaves the Federal District Court in Albany after he was arraigned in 2014 in connection with a conspiracy to use a weapon of mass destruction, distributing information related to such weapons and attempting to produce a device to endanger people by releasing radiation. File photo

Dec 19 – A New York industrial mechanic convicted of attempting to produce a mobile X-ray device intended to kill Muslims has been sentenced in federal court to 30 years in prison.

Fifty-two-year-old Glendon Scott Crawford, of Galway, also was ordered Monday by Judge Gary L. Sharpe to undergo a lifetime of supervised release after serving the sentence.

Crawford was convicted of conspiring to use a weapon of mass destruction and distributing information about weapons of mass destruction.

Crawford and co-defendant Eric Feight worked for General Electric in Schenectady. Prosecutors say the two conspired to **design and build the device, which was to be set off remotely and would have exposed targets to deadly radiation.**

Feight pleaded guilty to lesser charges a year ago and was sentenced to eight years in prison.

On Aug. 21, 2015, following a week-long trial, a jury voted to convict Crawford on all charges of a three-count indictment: attempting to produce and use a radiological dispersal device, conspiracy to use a weapon of mass destruction, and distributing information relating to weapons of mass destruction.

He is the first person in the U.S. to be found guilty of attempting to acquire and use a radiological dispersal device, in violation of the "dirty bomb" statute passed by Congress in 2004.

United States Attorney Richard S. Hartunian stated: "This case shows both the dangers we face from extremist views, and our resolve to stop those who plan to act on those views." U.S. Attorney Richard S. Hartunian said. "Crawford planned to kill Muslims on account of their religion and other people whose political and social beliefs he disagreed with, including government officials."

FBI Special Agent in Charge Andrew W. Vale said Monday's sentencing is a victory for both the community and law enforcement.

"It is a powerful reminder of the strength and solidarity of our communities, Vale said. "When confronted with Crawford's deadly intentions, concerned citizens came forward and alerted law enforcement of Crawford's plans. While we enjoy today's success, it is important that we continue in the diligent effort to identify and disrupt those who would go beyond hateful rhetoric to commit violent, criminal acts."

The evidence presented at trial showed that in April 2012, Crawford approached local Jewish organizations seeking financial support for his plan to acquire a device to be used against people he described as being "enemies of Israel." Crawford, a self-professed member of the Ku Klux Klan, drove from the Albany area to North Carolina to directly solicit funding for his plan from senior members of the KKK. Crawford, with help from Feight, took steps to design, acquire parts for, build, and test a remote-control unit that would activate a radiation dispersal device from a distance. Evidence presented at trial showed that Crawford sought and eventually received a radiation dispersal device from people he believed were businessmen affiliated with the KKK, but were, actually, undercover FBI special Agents. Before providing the device to Crawford, FBI agents had rendered it safe.

Feight, acting at Crawford's direction, built and delivered a remote-control unit. Crawford scouted mosques in Albany and Schenectady, and an Islamic community center and school in Schenectady, as possible **target** locations. Other targets considered by Crawford included the White House and the New York Governor's Mansion in Albany.

U.S. Invests in Amgen, Sanofi Countermeasures for Radiological Incidents

Source: https://globalbiodefense.com/2016/10/11/u-s-invests-amgen-sanofi-countermeasures-radiological-incidents/

Oct 2016 – The U.S. Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response (ASPR) is purchasing **two medical products to treat injuries to bone marrow in victims of radiological or nuclear accidents or acts of terrorism.**

The two products, called colony stimulating factors, stimulate bone marrow to produce blood cells including neutrophils that reduce the body's risk of developing an infection and decrease risk of death from acute radiation syndrome.

Infections often occur after exposure to high doses of radiation. These types of products are used commonly to reduce the risk of infection in patients with cancer.

ASPR's Biomedical Advanced Research and Development Authority (BARDA) is purchasing the first of these two leukocyte growth factor products, called Neulasta, from Amgen USA, Inc. of Thousand Oaks, California, under an approximately $37.7 million agreement. BARDA will purchase the second product, called **Leukine**, from Sanofi-Aventis U.S., LLC of Bridgewater, New Jersey, under a $37.6 million agreement. Sanofi-Aventis is a subsidiary of Sanofi.

Neulasta is approved by the U.S. Food and Drug Administration (FDA) to treat adults and children exposed to high levels of radiation that damage bone marrow. BARDA continues to work with Sanofi-Aventis to support the studies needed to request FDA approval of Leukine.

BARDA will purchase both products using funding and authority provided through the Project BioShield Act of 2004. Under the Project BioShield Act, the U.S. government supports the advanced development and procurement of new medical countermeasures – drugs, vaccines, diagnostics, and medical supplies – to protect health against chemical, biological, radiological and nuclear threats.

The products add to the available treatment options in the Strategic National Stockpile for acute radiation syndrome. Previously, BARDA sponsored advanced development and purchased another leukocyte growth factor product called Neupogen, which is now also FDA-approved for use in treating adults and children exposed to levels of radiation that damage the bone marrow.

The purchase of Neulasta and Leukine increases the number of colony stimulating factor doses available for use in an emergency response. It also increases operational capability since treatments with Neulasta are given once weekly, whereas treatment with Neupogen are given daily.

Long After ISIS Collapses, Its Empire of Explosives Will Reign

Source: http://counteriedreport.co.uk/long-after-isis-collapses-its-empire-of-explosives-will-reign

Nov 22 – It doesn't look like an improvised explosive device – at least, not the stereotypical kind. This one, from a part of northern Syria that ISIS used to control, looks more like a high-school science project volcano. Covered with a little dirt and some leaves, it'd probably pass for a rock, until someone tripped the hidden trigger and detonated the fragmentation device hidden inside.

Fragmentation device disguised as a rock

But the trickiest part of the bombs ISIS has left behind, across thousands of square miles of Iraq and Syria, isn't just their looks. "The coverage area appears to be huge swaths of the territory and growing all the time. The density is high, as well" says Ed Rowe, a program manager for Norwegian People's Aid, a humanitarian group putting together an IED clearance and risk education program in Iraq. "The level of sophistication seems to be increasing, and they're definitely targeting the clearance teams."

IEDs aren't a new weapon for ISIS. In fact, the group is still using some of the same designs its predecessors used during the US occupation of Iraq. But ISIS's IEDs are causing unique problems for those tasked with clearing them because of both the unprecedented scale of production and the fact that it's using the weapons in different ways, and against different targets.

New Bombs

During the Iraq occupation, the Islamic State of Iraq and al-Qaeda used improvised bombs to, among other things, target coalition vehicles along roads and highways. But as the Assad regime's grip on Syria crumbled, ISIS gained territory and strength, controlling a caliphate that stretched from Syria almost to the outskirts of Baghdad. With thousands of square miles to defend, ISIS began using IEDs like traditional landmines, planting them underground in large, densely-packed defensive swathes outside important population centers to seal residents in and keep enemies out.

"They have the same role as a conventional landmine, except they contain much more explosive and can be activated over a larger area of ground," Rowe says.

The demand for mass production led to greater standardization of designs and components. Even today, as the caliphate crumbles, Norwegian People's Aid is seeing a new IED design, complete with machined firing pins and a fuse derived from commercial equipment.

ISIS has also been known to add booby-traps within IEDs to target explosive ordnance disposal teams trying to disarm them. Even if only a small percentage of the weapons are outfitted to kill EOD personnel, clearance teams still have to treat every device as a potential trap. "You have to treat every item you see as if it's an IED until you prove it's not, so that necessarily makes the pace of work go a lot slower," says Jerry Guilbert, deputy director for programs at the US State Department's Office of Weapons Removal and Abatement.

WIRED showed images of IEDs taken by the ROJ Mine Control Organization, one of the groups trying to deal with the problem, to Kenton Fulmer, an explosives expert at Armament Research and Johns Hopkins University. Fulmer says they're similar to IEDs he saw with the military in Mosul in 2008. "The sealant is a design signature," he says; ISIS' predecessor organizations sometimes used sealant to keep moisture out of their devices.

"The caliphate, it has essentially a weapons program. IEDs are standardized to a high degree," Fulmer says.
In urban areas, the terrorist group uses a different, often more complex kind of IED. They're more like booby traps themselves, designed to explode when someone picks up a blanket or opens a door. That's what Janus Global Operations, a State Dept. contractor, is reporting in schools and buildings in Iraq*. "A lot of the items that Janus is finding in urban areas were planted specifically to target civilians," Guilbert says.

A Cleanup Problem

Getting rid of IEDs isn't simple, even for organizations that work in the dicey business of removing explosives from the battlefields. The humanitarian groups often charged with clearing explosive ordnance aren't used to working with IEDs. Traditional mine action operations have focused on removing mines produced by established arms companies with well-known disposal procedures. Skilled personnel can teach those to locals in a matter of weeks. IEDs, however, require personnel with harder-to-find and more expensive skills, like military veterans.

IED charges. Fulmer estimates the metal containers towards the front could contain up to 100kg of explosives.

In Iraq today, dealing with leftover IEDs is relatively easier—the country has a functioning government. Humanitarian groups, the United Nations Mine Action Service, and non-governmental organizations funded by the State Department can coordinate with Iraqi government's mine action agencies.
But in northern Syria, where the American-backed Syrian Democratic Forces have pushed ISIS out of a handful areas, the landscape of IED cleanup is less clear. In Syria's Al-Hasakah governorate, RMCO and its team of roughly 30 people has been working on its own, without help from international humanitarian groups or the US-backed anti-ISIS coalition. But Col. John Dorrian, a spokesperson for the US-led coalition, says that the US provides training on the IED threat at the unit and staff level to allies, including an IED awareness course and basic equipment.
Teaching local forces how to dispose of explosives can be a delicate issue, though. The military sometimes holds back on teaching select techniques. "Everyone's really testy when you learn about how to take an IED apart safely, because that goes hand-in-hand with learning how to build an IED. It also goes hand-in-hand with how to kill people who are

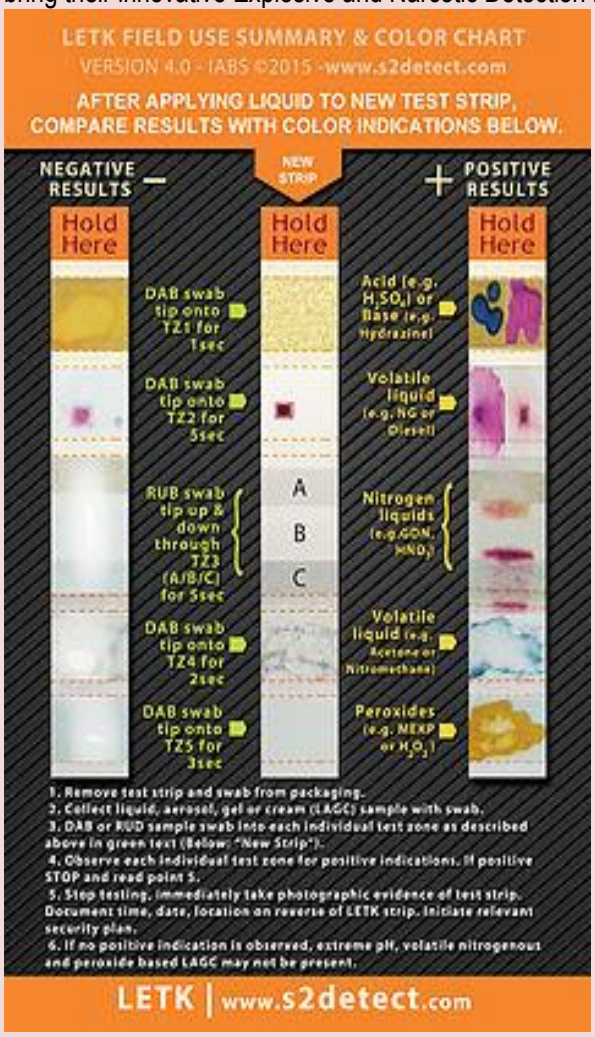
taking apart IEDs," says Fulmer. "As an EOD tech, I don't want lots of people knowing how to kill me while I work."

Many more people will have to learn that trade, though. In Syria and Iraq, an empire of explosives still reigns in hidden underground and urban caches. Disposal teams and civilians will be fighting the last vestiges of the caliphate long after it collapses.

BBI Detection to launch new range of Explosive and Narcotic Threat Detection kits at UK Security Expo 2016

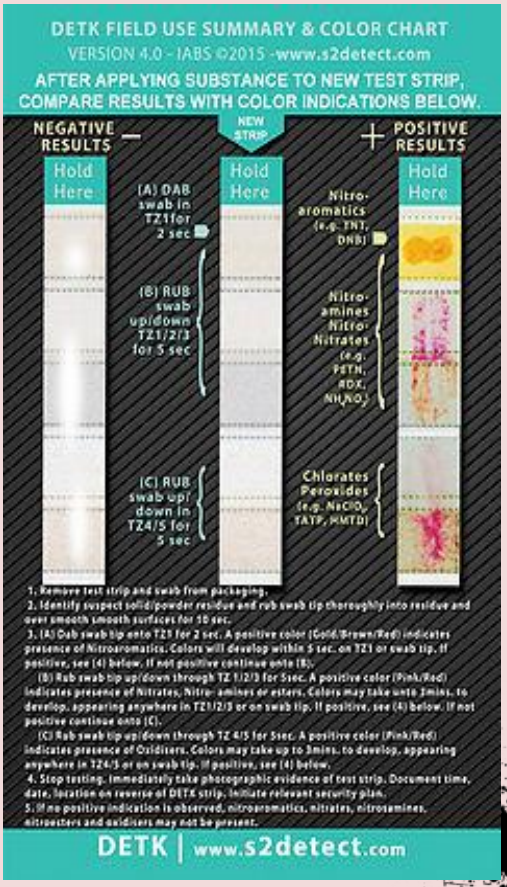
Source: http://counteriedreport.co.uk/news/bbi-detection-to-launch-new-range-of-explosive-and-narcotic-threat-detection-kits-at-uk-security-expo-2016

Nov 24 – BBI Detection are proud to announce a partnership with S2 Threat Detection Technologies to bring their innovative Explosive and Narcotic Detection kits to the wider Defense and Security market.



This unique product portfolio provides simple to use, rapid and low cost solutions for the presumptive identification of potential threat items in a variety of scenarios such as screening at secure checkpoints or the assessment of suspect powders or materials in clandestine labs.

- The **Dry Explosive Test Kit (DETK)** is a single use colorimetric-based test kit for the presumptive identification of military grade explosives and precursors used in manufacture of improvised explosives
- The ECAC certified **Liquid Explosive Test Kit (LETK)** is a colorimetric-based test kit for detecting liquid explosive residues found in liquids, aerosols, gels and creams and is designed for presumptive identification of concealable liquid threat materials.
- The **Narcotics Test Kits (NTK)** and **Cannabis Test Kit (CTK)** are a rapid, simple, and reliable technology designed for identification of Drugs of Abuse by first responders and frontline personnel.



These new products are complimentary to BBI Detections existing portfolio which includes the

Biothreat and Explosive Detection IMASSTM platforms.

Sandia team revolutionizes bomb X-ray technology

Source: http://www.newsobserver.com/news/technology/article116605493.html

Nov 23 – Jake Deuel, Justin Garretson and Scott Gladwell are quickly becoming bomb technicians' best friends.

The trio of Sandia National Laboratories researchers has developed a software package that greatly reduces the amount of time a bomb tech spends determining what's inside the "package" they've been called to examine. It also speeds up the process the techs use to disarm a potentially lethal bomb.

And when that package is "ticking," every second counts, reported the Albuquerque Journal (http://bit.ly/2fxXkX6).

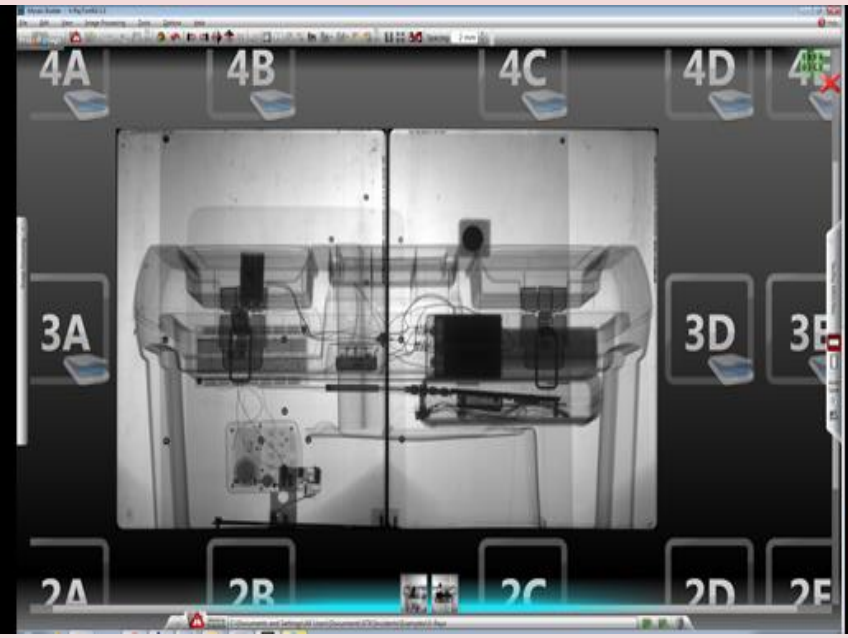
In 2009, Sandia was approached by the Department of Energy about developing a uniform software package specifically designed for use in the field by Explosive Ordnance Disposal teams, said Garretson, the lead developer of what has become known as the **X-Ray Toolkit, or XTK.**

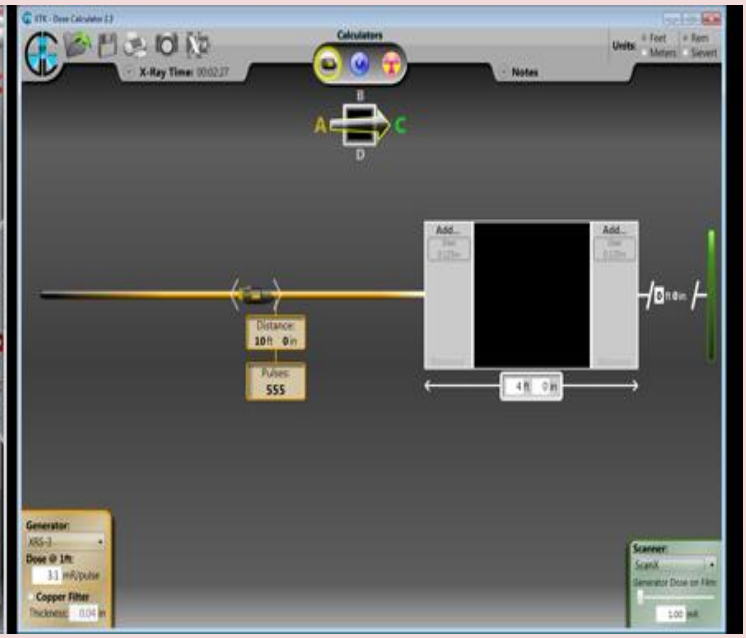
which can be anything from old military munitions to sophisticated "pressure cooker" bombs like the ones that killed three and maimed hundreds at the 2013 Boston Marathon. They've even found bombs disguised as grease guns.

Although two parts of the X-ray system - the unit that produces the X-rays and the one that processes the images - are somewhat standardized, each system had different software for the laptop computers, the critical third element of the system.

"The problem was, each manufacturer developed its own software, which led to a huge learning curve" for bomb techs, Crisp said. "It was like constantly switching between Windows, Mac OS X and Linux."

Exacerbating the problem was that most of the X-ray software had been developed for medical applications rather than bomb techs.





Among the earliest users of XTK was Kirtland Air Force Base's 377th Explosive Ordnance Disposal Flight, a unit charged with handling bomb threats in New Mexico, southern Colorado and eastern Arizona - or anywhere in the world they're needed.

Tech Sgt. William Crisp, an EOD team leader who has been in the bomb-handling business for 14 years, explained that a team responding to a potential bomb typically uses a portable X-ray system to see what's inside the "package,"

The varying software also affected interoperability, the ability for one OED team to interact with and assist other teams, Crisp said. It wasn't unusual for techs to have to learn several different software packages to remain proficient.

Learning from the techs

With funding from the DOE's National Nuclear Security Administration - which has a focus on responding to nuclear terrorism

threats - and the Defense Department's Combatting Terrorist Technical Support Office, Sandia's Robotics & Security Systems division began meeting with numerous EOD technicians to find out what they needed to better accomplish their mission.

"Rather than having a lot of features all at once, we started with something really basic," said Gladwell, principal member of the division's technical staff. "Then we'd add capabilities over time as the users provided feedback."

Gladwell said the XTK developers worked closely with EOD techs each step of the way, adding whatever features they found helpful and omitting any deemed superfluous.

By late 2010, the first version of XTK was in the hands of a select group of federal EOD squads - including the 377th EOD Flight - who were tasked with testing the system and offering suggestions to improve it.

"XTK works across a wide variety of X-ray platforms - which is why it's such a boon" to the EOD community, Crisp said.

New bomb techs can learn the program quickly and, with tens of thousands of bomb techs in the military and law enforcement now using XTK, it provides a very high level of interoperability, he said.

Keeping it simple

Senior Airman Josh Patterson, an EOD tech at the 377th, said XTK also assists bomb techs in determining how to set up the X-ray system to penetrate whatever type of container the explosive device might be housed in, without risking overexposure.

The amount of X-ray exposure used, Patterson said, "depends on what you're trying to see through."

"Because the material and thickness varies, you have to determine how much (X-ray) exposure you'll need to get a good image," he said.

Prior to XTK, that required complicated mathematical formulas that could take considerable time to apply. XTK, he said, does the calculations for you with a few quick keystrokes, ensuring a usable image.

"We went from probably five minutes of calculation to nearly zero," Crisp said.

The FBI's Hazardous Devices School, which trains and certifies nearly 500 civilian law enforcement bomb squads, has adopted XTK as its premier software suite, Sandia researcher Deuel said.

How XTK wound up in the hands of an estimated 20,000 civilian law enforcement bomb techs so quickly is a testament to its developers and Sandia, Deuel said.

"One of the reasons XTK took off was because it's free," Deuel said. "The reason it's free is because the developers agreed to give it away" rather than accept royalties to which they are legally entitled.

Realizing that cash-strapped civilian bomb teams likely couldn't afford the royalties - and recognizing the importance of their work - the developers opted for free distribution to qualified civilian bomb teams, he said.

"That was their decision, and it was huge," Deuel said.

Sandia also offered free test and evaluation licenses to X-ray system manufacturers to ensure XTK is compatible with their systems and offered low-cost licenses to companies that agreed to provide quality training for civilian XTK users.

Those efforts won Sandia the 2016 Federal Laboratory Consortium Award for Excellence in Technology Transfer, Deuel said.

Sniffing Like a Dog Can Improve Trace Detection of Explosives

Source: https://www.nist.gov/news-events/news/2016/12/sniffing-dog-can-improve-trace-detection-explosives

Dec 01 – By mimicking how dogs get their whiffs, a team of government and university researchers have demonstrated that "active sniffing" can improve by more than 10 times the performance of current technologies that rely on continuous suction to detect trace amounts of explosives and other contraband.

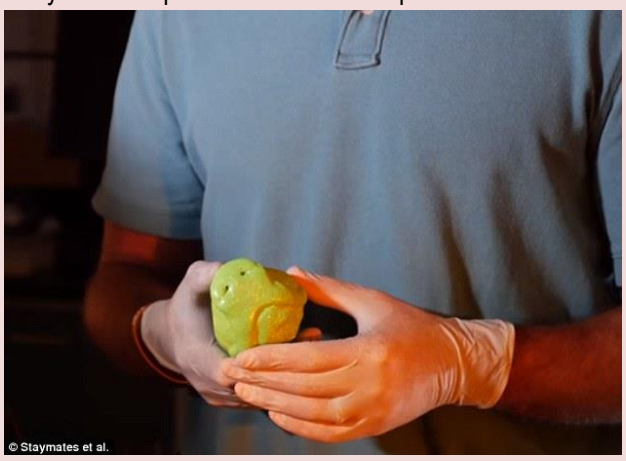
"The dog is an active aerodynamic sampling system that literally reaches out and grabs odorants," explained Matthew Staymates, a mechanical engineer and fluid dynamicist at the National Institute of Standards and Technology (NIST). "It uses fluid dynamics and entrainment to increase its aerodynamic reach to

sample vapors at increasingly large distances. Applying this bio-inspired design principle could lead to significantly improved vapor samplers for detecting **explosives**, **narcotics**, include equipment that requires swabbing hands or other surfaces and then running the sample through a chemical detector—typically an ion mobility spectrometer. Wand-like vapor

pathogens—even **cancer**."

Following nature's lead, Staymates and colleagues from NIST, the Massachusetts Institute of Technology's Lincoln Laboratory and the U.S. Food and Drug Administration fitted a dog-nose-inspired adapter to the front end of a commercially available explosives detector. **Adding the artificial dog nose—made on a 3-D printer—to enable active sniffing improved odorant detection by up to 18 times, depending on the distance from the source.**

Trace detection devices now used at points of entry and departure such as airports and seaports, and other sensitive locations, typically employ passive sampling. Examples



detectors accommodate more sampling mobility, but unless the detector scans immediately above it, the chemical signature of a bomb-making ingredient will go unnoticed.

Aiming to uncover clues on how to improve trace detection capabilities, the researchers turned to one of nature's best chemical detectors: the dog. Through their review of previous studies, the team distilled what occurs during sniffing. Five times a second, dogs exhale to reach out, pull and then inhale to deliver a nose full of aromas for decoding by some 300 million receptor cells.

Using a 3-D printer, Staymates replicated the external features of a female Labrador retriever's nose, including the shape, direction, and spacing of the nostrils. Moving air through the artificial nose at the same rate that a dog inhales and exhales allowed them to mimic the air sampling—or sniffing—of dogs.

With schlieren imaging—a technique widely used in aeronautical engineering to view the flow of air around objects—and high-speed video, the team first confirmed that their imitation nose could indeed sniff much like the real thing, a property documented in previous studies of live dogs.

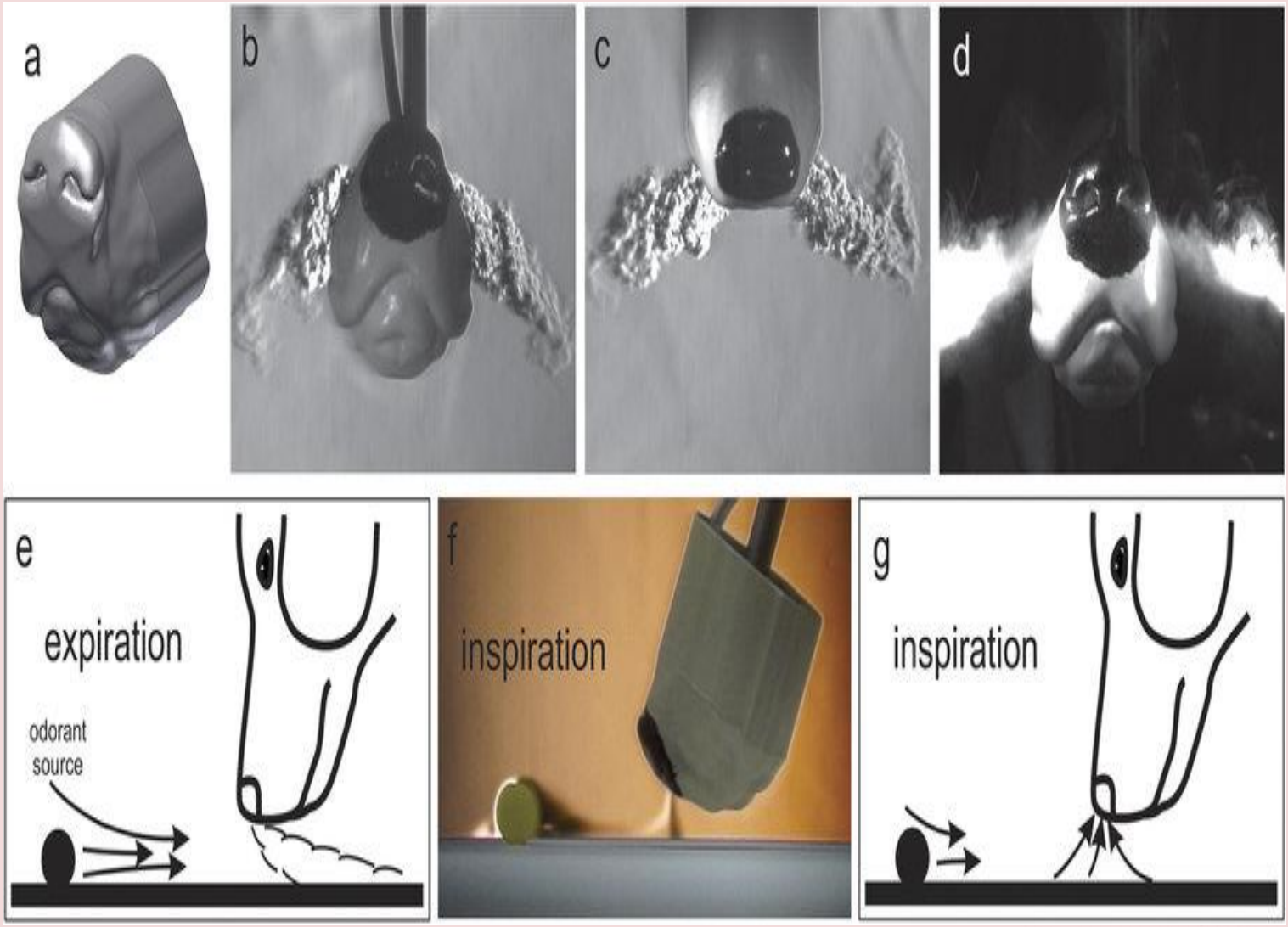
With each sniff, air jets exit from both nostrils, moving downward and outward. Though it might seem counterintuitive, the air jets entrain—or draw in—vapor-laden air toward the nostrils. During inhalation, the entrained air is pulled into each nostril.

The team's first set of experiments compared the air-sampling performance of their "actively sniffing" artificial dog nose with that of trace-detection devices that rely on continuous suction. The head-to-head comparison with an inhalation system used with a real-time monitoring mass spectrometer found that sampling efficiency with the sniffing artificial dog nose was four times better 10 centimeters (3.9 inches) away from the vapor source and 18 times better at a stand-off distance of 20 centimeters (7.9 inches).

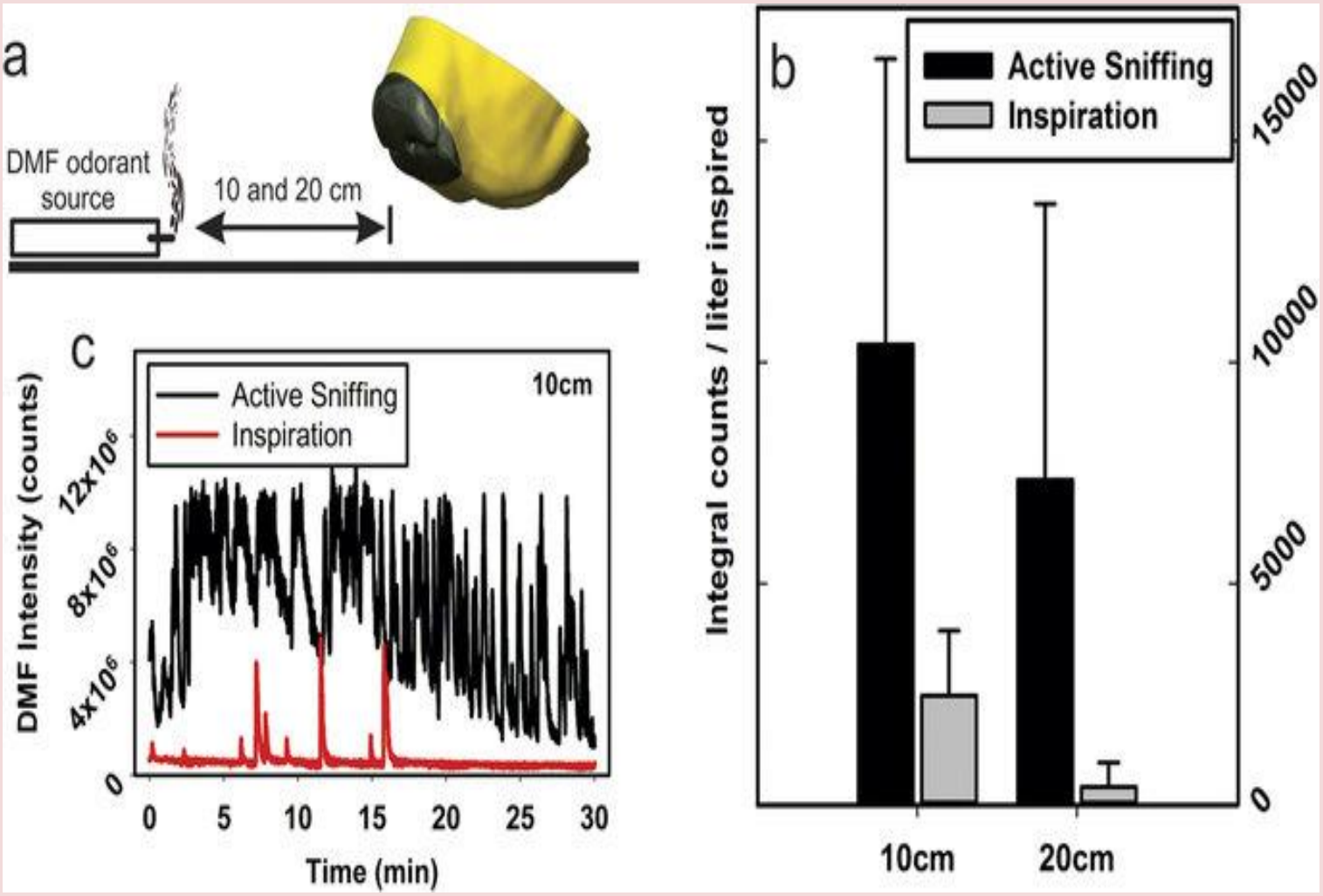
On the basis of those results, the team chose to outfit a commercially available vapor detector with a bio-inspired 3D-printed inlet that would enable it to sniff like a dog, rather than to inhale only in 10-second intervals, the device's normal mode of operation. The switch resulted in an improvement in odorant detection by a factor of 16 at a stand-off distance of 4 centimeters (1.6 inches).

"Their incredible air-sampling efficiency is one reason why the dog is such an amazing chemical sampler," Staymates said. "It's just a piece of the puzzle. There's lots more to be learned and to emulate as we work to improve the sensitivity, accuracy and speed of trace-detection technology."

The research is reported (link is external) in the journal *Scientific Reports*.



(a) Reconstructed model of the canine nose based on the model of Craven *et al.*[36,38,59] (2007, 2009, 2010) that includes the nasal vestibule, external nose, lower jaw, and about 10 cm of the snout. (b,c) Images extracted from high-speed schlieren videography flow visualization with helium illustrate the directionality of the expelled air jets from anterior (b) and dorsal (c) views. (D) Visualization of theatrical fog shows the ventral-laterally directed turbulent air jets exiting the naris during expiration. (e) During the expiratory phase of sniffing, turbulent air jets vectored ventrally and laterally entrain odorant vapor from tens of centimeters ahead of the nose that would otherwise be inaccessible to the dog. (f) Schlieren image of the 3D printed dog's nose during the inspiratory phase of sniffing showing acetone vapor be drawn into the nose from a source that is located approximately 10 cm away. (g) During the inspiratory phase of sniffing each nostril draws in air from all directions, including odorant-laden air that was drawn toward the nose during expiration.



(**a**) Illustration of the experiment. (**c**) Representative signal responses from the mass spectrometer comparing DMF signal intensity at 10 cm for active sniffing versus steady inspiration. (**b**) Total mass spectrometer response intensity, calculated as the integrated area under each curve, normalized by the total volume of inspired air for each experiment shows that active sniffing results in a significantly higher normalized response intensity compared with steady inspiration. The error bars are the standard deviation three sampling experiments for each case and are representative of the natural variance of the plume dynamics generated at the DMF vapor source. The improvements in DMF vapor detection performance (sniffing vs. steady inspiration) were approximately a factor of 4 at a standoff distance of 10 cm, and a factor of 18 at a 20 cm standoff distance.

▶ **You can watch some related videos at source's URL.**

ISIS drones take the IED to Western troops

By Alex Hollings

Source: https://sofrep.com/67685/isis-drones-take-ied-western-troops/

Nov 14 – **IEDs, or Improvised Explosive Devices, have been responsible for three out of five combat deaths in Iraq since the start of the Iraq war in 2003.** These bombs come in a variety of forms, often concealed near or beneath driving surfaces to be detonated remotely when poised to do the most possible damage, but recent reports from the ongoing battle between ISIS and coalition forces in Iraq indicate that ISIS may have found an even deadlier use for their explosives: arming drones.

On October 2nd of this year, an ISIS controlled drone armed with an improvised explosive killed two Peshmerga soldiers and injured two French paratroopers in Irbil, Iraq.

This development confirmed reports made by Conflict Armament Research that one of their investigators uncovered an ISIS "drone workshop" in Ramadi. The investigator, whose name was not disclosed, reported that he found plywood fuselages and Styrofoam wings inside the building, as well as a disassembled shoulder launched surface-to-air missile. For Conflict Armament Research investigators, the presence of these components together strongly implied that ISIS was trying to "arm their drones with something that would be light enough to be carried by a drone, but also that would have the right kind of explosives for potency,"

Unfortunately, recent reports would seem to indicate that they found the right combination to

do just that. ISIS seems to be building their drone IEDs from scratch, as off the shelf drones available to them often don't possess the necessary battery lifespan or payload capacity to be an effective means of explosive delivery. Instead, they are building these drones out of components they are able to procure through international trade and captured weapon systems. **Notably, investigators in the "drone workshop"**

located a gyroscope sold by the Turkish company Bomec Robot Teknolojileri. These devices are intended only for domestic sale within Turkey and are an integral component when building a navigational system for drones.

The workshop appeared to have been abandoned prior to coalition forces arriving, and if there were any functioning models of ISIS' drones present, they were taken by the extremists as they evacuated. The absence of any controllers, cameras, or propulsion systems in the lab leaves many questions still unanswered about the drones range, payload or remote control capabilities.

Kurdish forces have reported sightings of ISIS controlled drones as early as last winter, but October 2nd marks the first time any Western fighter has been injured or killed by these remote controlled aircraft.

Concerns about ISIS controlled drones has prompted the Pentagon to request funding for a $20 million project to engage and take down these small drones before they are able to reach troops on the ground. The money, according to the Pentagon's request, would go toward funding the research and development of ways to "counter the effects of unmanned aerial systems and the threats they pose to U.S. forces."

Reports have emerged of a new weapon in the war against ISIS making its way to the front lines that allows U.S. troops to jam the radio signal controlling the drones, causing them to either land or crash. The Battelle DroneDefender can mount on any rifle with a picatinny rail, weighs ten pounds, and uses restricted radio bands to block both remote control and GPS signals. Although the price for this device has not yet been made public, Popular Science reported its presence in at least one American base in Iraq as early as July of this year.

The DroneDefender may not cause all ISIS drones to simply fall out of the sky. If ISIS uses off the shelf drones without modifying their internal software, the weapon may allow us to force the drones to land, permitting further research into their construction and use of drones for warfare. Most commercial drones come equipped with lost signal protocols that force the drone to land in a controlled manner immediately upon severing its connection with the control unit that steers it.

While there are other anti-drone systems in production and testing, the DroneDefender is the first system designed to be equipped on firearms already in use in the region. U.S. forces, already familiar with their rifles, will experience a shorter learning curve in terms of how to aim the weapon accurately.

Use of drones by terrorist and insurgent groups has risen steadily in recent years as a result of the advances in commercially available drone technology. Until recently, these drones were used for surveillance and even to aid in filming propaganda to be used to attract new recruits to their causes. Attaching explosives to these drones would seem to have been the logical next step for groups like ISIS. However, the difficulty in finding potent enough explosives to be carried by foam and balsa wood aircraft without seriously limiting the range of the drone would seem to be the largest hurdle for the Islamic State and their efforts to weaponize them.

The investigators that uncovered the lab in Ramadi warn that the presence of a disassembled surface-to-air missile in their makeshift workshop could indicate that ISIS is learning how to make smaller, better, more powerful bombs for their drones.

Even if they have yet to acquire or master the technology required to create elaborate targeting systems, an off the shelf wireless video camera would provide the Islamic State with an effective, if not simple, targeting mechanism simply by steering the drone toward the intended target remotely.

As commercial drones continue to become more powerful and technologically advanced, it can be assumed that terrorist organizations like ISIS will also expand upon their existing drone capabilities. Hopefully, platforms like the DroneDefender will see widespread distribution in time to quell the threat of these new flying IEDs.

Even if ISIS falls before they have an opportunity to create many more explosive aircraft, their use of drones marks a shift in modern combat that will have to be addressed.

Alex Hollings *served as an active duty Marine for six and a half years before being medically retired. A college rugby player, Marine Corps football player, and avid shooter, he has competed in multiple mixed martial arts tournaments,*

raced exotic cars across the country and wrestled alligators in pursuit of a story to tell. His novel, "A Secondhand Hero" is currently seeking publication.

EUROPOL 2016 TESAT (Explosives)

In 2015 terrorists' use of explosives varied across EU countries and between terrorist groups. The main change in modus operandi occurred in jihadist terrorist attacks, where new tactics, techniques and procedures were detected in conducting bomb attacks.

Improvised explosive devices (IEDs)

For the first time in the EU, jihadist terrorists combined the use of firearms and person-borne improvised explosive devices (PBIED) in a large-scale roaming attack in Paris. The suicide attacks in public places show similarities in tactics, techniques and procedures to those which had been previously utilised by jihadist terrorists outside the EU. The attacks resembled in particular those in Mumbai, India in November 2008 in terms of modus operandi, targets chosen, numbers of attackers and impact.

It is apparent that there has been a transfer of technical knowledge and capability in IED design and construction. Some elements of the IEDs utilised were slightly modified in order to adapt to the EU circumstances and available resources, e.g. the use of improvised components instead of relatively scarce military components.

Dissident Republican (DR) groups in Northern Ireland (UK) deployed a variety of types of attack in 2015 including: postal IEDs, under vehicle IEDs, command wire IEDs, radio controlled IEDs, use of grenades, incendiaries and firearms. The main explosive charge of those IEDs mainly consisted of low-explosives (pyrotechnics mixture and gunpowder), although in some cases a high-grade plastic explosive was used. All groups still retain access to a range of firearms and explosive materials.

Although in recent years there have been no terrorist bomb attacks linked to ETA, their logistical apparatus may still be operational. A number of ETA explosives caches were discovered in France and Spain in 2015. They contained large quantities of weapons and home-made explosives (HMEs), along with explosive precursors and other bomb-making materials.

Extremist groups in **Greece** mainly carried out attacks using flammable liquids, IEDs and improvised explosive-incendiary devices (usually ignited by a flame). During one investigation, Greek authorities discovered clandestine storage containing substantial quantities of firearms, explosive ordnance (rocket launchers), commercial explosives, HMEs, explosive precursors and bomb-making materials, ready to be used in an attack.

Anarchist groups in Italy predominantly carried out arson attacks using flammable liquids and improvised incendiary devices (IIDs). In addition, some terrorist attacks were conducted in which the perpetrators sent postal IEDs filled with a low-explosive charge. **All of these improvised devices were constructed using commercially available materials.**

Home-made explosives

Home-made explosives (HMEs) remain the most commonly used explosives in IEDs. Notwithstanding the easy access to bomb-making instructions on the internet, there is evidence that more expert knowledge is likely to have been transferred to terrorists through direct contact and experience. The transfer of knowledge to the EU has been facilitated by the phenomenon of foreign terrorist fighters and returnees. There are indications that some of the fighters in the conflict zones have received advanced training in manufacturing and using HMEs in IEDs. Moreover, recent investigations show that certain terrorist groups continue to establish large stockpiles of explosive precursors in the EU in order to manufacture HMEs.

Military explosives

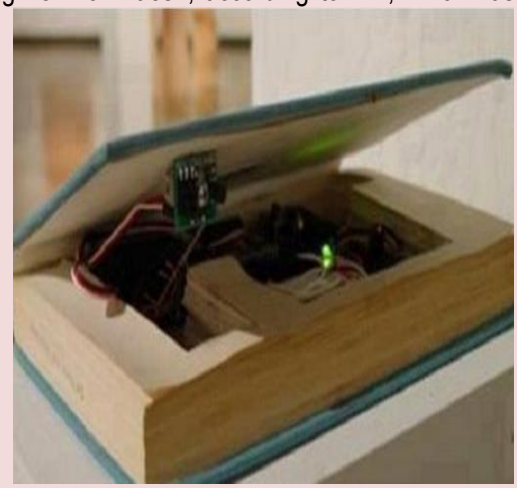
Explosive remnants of war (ERW) and illicit trafficking in explosives from former conflict areas present a significant threat to the EU. A number of large shipments of illegal military-grade firearms and explosives, mostly from the Western Balkan countries, were seized in organised crime investigations in 2015. Terrorists are known to have acquired hand grenades, rocket launchers, and high-grade plastic explosives and detonators from organised crime groups.
Explosive ordnance has also been acquired via theft from military explosive storage facilities and the illegal collection of ERW and unexploded ordnance (UXO) from former battle zones.

Commercial explosives
The threat posed by the misuse of commercial pyrotechnics and gunpowder endures, although they have generally been employed as sources of explosive compounds in smaller IEDs that did not result in casualties. Commercial explosives have rarely been used in IEDs to conduct terrorist attacks, due to the manufacture, storage, sale and use of such explosives being strictly regulated.
However, there have been reported incidents of burglary and the theft of explosives from storage facilities. In one case, a mining company employee was able to appropriate more than 500 kg of explosives and 150 electric detonators, which he subsequently attempted to sell on the black market.

Daesh Plants Bombs in Copies of Quran Near Mosul

Source: https://sputniknews.com/middleeast/201612061048202312-daesh-bombs-copy-quran-mosul/

Dec 06 – Islamic State terrorists have planted bombs in copies of the Quran before leaving them on the streets and in front of houses in Kan'ous, a village close to the Iraqi city of Mosul, the Iran Front Page has reported. Resorting to guerilla deception is nothing new for Daesh, according to IFP, which has



targeted Sunnis, Shiites, Kurds, Christians, and many others. The village of Kan'ous has since been liberated by the Iraqi army, according to reports.
Earlier Monday, the US-led coalition against Daesh conducted five airstrikes to soften the terror group's forces near Mosul, according to an announcement from the Operation Inherent Resolve joint task force. The Mosul strikes reportedly eliminated seven mortar systems, four Daesh-held buildings, two vehicles, and a front-end loader while engaging four tactical units, according to the news release. The airstrikes also damaged 31 supply routes.
"Coalition military forces conducted 10 strikes coordinated with and in support of the Government of Iraq using attack, fighter, and remotely piloted aircraft," against Daesh targets in Iraq, the report added. Over the weekend, the coalition of over 60 nations also launched 11 airstrikes on strategic targets in Syria, destroying oil assets, mortar systems, and a weapons production facility.
In Aleppo, Moscow officials have said that rebel shelling of a Russian mobile hospital has resulted in the deaths of two Russian nurses and eight civilians, with others in critical condition.

Cairo Cathedral explosion: 25 dead and 50 worshippers injured in blast at seat of Egypt's Orthodox Christian church

Source: http://www.mirror.co.uk/news/world-news/cairo-cathedral-explosion-22-dead--9434974

Dec 11 – An explosion at a cathedral in Cairo has killed at least 25 people - with at around 50 mostly Christian worshippers and other bystanders injured, according to Egyptian state television.

The blast happened near the St Mark's Coptic Orthodox Cathedral in the Abbassia district - with some suggestions it happened at a 100yr-old church within the complex called al-Botrosiya.

It is being reported that many of the victims were women and children - yet to be confirmed.

Amid panic at the scene, Daily News Egypt reported that families are desperately trying to enter the cathedral to check on relatives.

Armed forces have been deployed to the scene as 14 ambulances carry away the dead and injured.

Locals claimed the explosion occurred during prayers - and terrorists are being blamed by social media users although there is yet to be any official confirmation it was a bomb.

Egypt's official Mena news agency said an assailant lobbed a bomb into a chapel close to the outer wall of St Mark's Cathedral - seat of Egypt's Orthodox Christian church and home to the office of its spiritual leader, Pope Tawadros II.

Other local media is claiming an as yet unidentified woman placed an improvised explosive device (IED) containing 6kg of explosives inside the building before remotely detonating it - yet to be confirmed.

There have been no immediate claims of responsibility for the explosion - which is yet to be confirmed as a bomb - which occurred at around 10am local time (8am UK time).

Experts are speculating on social media that the large death toll suggests it could be the work of a suicide bomber - either just outside the door or inside the building.

The explosion comes 48 hours after two roadside bombs killed six policemen at the Great Pyramids in nearby Giza - about seven miles from the scene of today's blast.

That attack had previously been blamed on a group suspected by authorities of links to the outlawed Muslim Brotherhood.

UPDATE 1 (Dec 12): President Abdel-Fatah al-Sisi named a 22-year-old, Mahmoud Shafik Mohamed Mostafa, as the alleged perpetrator of the suicide attack.

UPDATE 2 (Dec 15): **Daesh took responsibility of the attack**

Greece – controlled explosion at Ministry of Labor

Source: Greek media

Dec 12 – Early hours of Monday, a car stopped and a man hanged a backpack on the door of the main entrance of the Greek Ministy of Labor (29 Stadiou Avenue, Athens downtown). At 01:20 a man made a telephone call at the Editors' Newspaper and informed that a powerfull IED was about to explode in 40 minutes. Athens EOD Squad crews arrived immediately on site and cordoned the area. By 06:30 three

controlled explosions were heard. Police authorities speculate that terrorists might belong to Revolutionary Struggle or the Popular Fighters Group or the Revolutionary Self-defense Group that, in November 2017, attacked the French Embassy in Athens. Explosive mechanism was iconnected to a 5L ANFO container. Either the detonation mechanism did not work or it was an "experimental" attack.

Netherlands explosion: Two SWAT team officers injured after massive blast

Source:http://www.dailystar.co.uk/news/latest-news/570061/Spaarndam-explosion-SWAT-team-officers-police-car-Netherlands

Dec 14 – Major explosion injures two police officers and leaves one in critical condition A Police SWAT team has been seriously injured after an explosion took place next to their car. The pair were in their police car when the explosion went off in Spaarndam, in the Netherlands at about 6.30pm. Both were badly

injured, with one in a serious condition in hospital, local media said.
A police spokesman said both officers were taken to hospital. He added they explosion may have taken place after the SWAT team's own device went off.
UPDATE Dec 15: Police confirm the **explosion was the result of ammunition in the police car**.

12-year-old attempted to bomb Christmas market in south Germany: prosecutors

Source: http://www.thelocal.de/20161216/12-year-old-attempted-to-bomb-christmas-market-report

Dec 16 – A young boy tried to set off a nail bomb at a Christmas market in Ludwigshafen, but the device failed to detonate, prosecutors have confirmed.

The boy, a German citizen of Iraqi heritage, attempted to blow up the device at the Ludwigshafen Christmas market on November 26th. When the device failed to detonate he gave up, before trying again on December 5th, prosecutors said on Friday.
This time he took the explosive device, hidden in a rucksack filled with nails, and placed it in a bush near the town hall.
Fortunately a pedestrian spotted the bag and alerted police, who then had specialists carry out a controlled explosion, Focus magazine reported on Thursday, citing security sources.

The 12-year-old, born in the town in Rhineland-Palatinate in 2004, had been radicalized and was encouraged to carry out the attack by an as-yet unknown member of the Isis terror group, according to Focus.
According to an earlier report by police investigators, the powder in **the homemade bomb had been created out of the ingredients of fireworks and sparklers and was flammable but not explosive.**
Because the boy is under 13 he cannot be tried for a crime. Instead youth workers have been assigned **to care for him**.
Federal prosecutors are however investigating the possibility that a terror network supported the attempted attack.

Syria: 9-year-old girl blows herself up near Damascus police station

Source: http://www.dnaindia.com/world/report-syria-explosion-heard-near-damascus-police-station-2283593

Dec 16 – Syrian state news agency *SANA*, quoting a Damascus police source, said on Friday there were reports of an explosion in a police station in the Midan neighbourhood of Damascus.
Syrian state television said a young girl of about nine years of age blew herself up on Friday in a police station in the Midan neighbourhood of Damascus.

State-run Ikhbariya news channel showed blurred images of what looked like a blackened girl's head in a blanket, and scenes of destruction inside what it said was the police station.

A witness in the area of the blast said a young girl entered the police station and, after asking to go to the toilet, blew herself up.

She asked to go to the bathroom of the police station because she has been lost…

Observatory head Rami Abdel Rahman told *AFP* that one woman was killed in the blast, but it remained unclear whether she was a suicide bomber or a bystander. Although rebel groups have fired rockets and mortar rounds into the capital, explosions inside the city itself are rare.

According to pro-government daily *Al-Watan*, the blast left "the female suicide bomber dead and wounded three police officers from the station".

In early 2012, a suicide bomber killed 26 people when he blew himself up in Midan. More than 310,000 people have died since Syria's conflict broke out in 2011.

Turkey – new terrorist (VBIED) attack against bus with soldiers

Source: http://www.reuters.com/article/us-turkey-blast-idUSKBN14605H?il=0

Dec 17 – **Thirteen soldiers were killed and 48 (update: 55 – 12 in critical condition) more were injured when a car bomb hit a bus transporting off-duty military personnel in the central Turkish city of Kayseri on Saturday, one week after a twin bombing targeted police in Istanbul.**

The blast is likely to further anger a Turkish public frustrated by a string of deadly bombings this year, several of which have been claimed by Kurdish militants, including last week's, which killed 44 and wounded more than 150.

There was no immediate claim of responsibility, but Deputy Prime Minister Veysi Kaynak likened the attack to last Saturday's dual bombings outside the stadium of Istanbul soccer team Besiktas, later claimed by an offshoot of the militant Kurdistan Workers Party (PKK).

"The car bomb attack resembles the Besiktas attack in terms of its style," he told a group of reporters, adding the incident would not put Turkey off of its goal of fighting militancy.

The military confirmed 13 personnel were killed and 48 wounded and said civilians may also have been injured in the attack. The wounded were transported to hospital for care, it said.

The bus was stopped at a red light near the campus of Erciyes University in Kayseri when a car approached it and then detonated, broadcaster NTV said.
Kurdish militants have previously targeted buses carrying military or security forces.

Defence Minister Fikri Isik said on Twitter that Turkey would redouble its efforts to fight militancy. "We will fight these cowards with a national mobilisation," he said, without elaborating.
Turkey faces multiple security threats including spillover from the fight against Islamic State in northern Syria, where it is a member of a U.S.-led coalition against the militant group.
It also faces regular attacks from Kurdish militants, who have been waging a three-decade insurgency for autonomy in largely Kurdish southeast Turkey.

Berlin attack: security intelligence has limits in preventing truck-borne terror

By John Blaxland
Source: http://www.homelandsecuritynewswire.com/dr20161221-berlin-attack-security-intelligence-has-limits-in-preventing-truckborne-terror

Dec 21 – The Christmas market truck assault in Berlin, which has left twelve dead and dozens injured, is a disturbing echo of the truck-borne attack on Bastille Day celebrants on the Nice promenade in July.
How could such events be allowed to happen? Why weren't intelligence agencies in Germany and France able to stay one step ahead of the perpetrators?
After all, we have become used to hearing stories of "increased chatter" and "high alerts." Does that not mean intelligence agencies should know enough to prevent such attacks?
Several trends are emerging that help explain the latest phenomenon and the limits of the security and intelligence agencies. These include:

- a sense in the security and intelligence business of being overwhelmed by having to trawl through a massive volume of data on potential hostile acts
- the trend towards greater disaffection among those feeling disempowered; and
- a heightened degree of disaggregation in terrorist activity.

A more complicated monitoring challenge

"High alerts" have become all too commonplace. Reports of "increased chatter" are either hard to discern from the background noise (which has grown exponentially in volume) or simply not heard as frequently or as clearly as before, thanks to greater security consciousness among would-be perpetrators.
In the post-Snowden era, the general awareness of security and intelligence agency monitoring has increased dramatically.
Arguably, the secret of success in the security intelligence business is keeping one's successes secret. But now that many of the intelligence successes of the recent past are common knowledge thanks to Edward Snowden's and other revelations, monitoring such plans and intentions has become incalculably more difficult. This has meant, for instance, that would-be terrorists and criminals have dramatically altered their online profile to evade detection.
This heightened level of awareness among would-be perpetrators of such acts has generated a far more complicated monitoring challenge.

Increasing levels of disaffection

The problem is made worse by heightened levels of disaffection.
The trend for violent extremists today is to draw inspiration from material online and through media coverage of the sensational acts of violence – be these in Brussels, Nice, Berlin, Aleppo, or Mosul.

The suffering and injustices continue to mount, providing ample sources of inspiration for acts of retaliation.

So a small number of young, often marginalized and disaffected migrants or their first-generation descendants seek to lash out in part against the apparent excess and indifference of the West to their circumstances, and in part out of misplaced zeal for a religious extremist cause.

Actors acting alone

Disaggregation – the fact many would-be terrorists operate alone and not as part of a wider cell – is a key concern.

In all likelihood, there was no direct connection between the perpetrators of the Berlin and Nice attacks that intelligence agencies might otherwise have been able to monitor. Instead, those in the truck in Berlin may have drawn inspiration from the truck attack in Nice: essentially perpetrating a copycat act. This suggests the hierarchical and networked nature of terrorist groups of the past is less relevant today.

Demagogues leading extremist Islamist groups, for instance, are less directly involved in prompting and facilitating such acts. With so many ideas and instructions available online, there is little need to establish the types of direct linkages once considered the norm.

As a consequence, identifying the relatively small number of such seriously disaffected people is a massive challenge that goes beyond the traditional technology-oriented solutions favored by security and intelligence agencies. In the social media age the task of monitoring for indicators of such behavior has become harder as the volume of data passed over the internet has gone from an emergent flood to an overwhelming deluge.

In countries like France, Belgium and Germany, where the number of disaffected and mostly migrant youth has been growing, the challenges are stretching the security and intelligence agencies to breaking point.

The expectation is these agencies must get better at their jobs. But, in reality, there are significant limits on what can be expected from them.

What now?

What is needed now is a new social compact that goes beyond reliance on security and intelligence agencies. We all have a role to play in preventing the fabric of society from tearing further.

The role of the security and intelligence agencies to remain vigilant and seek to monitor extremist elements will undoubtedly endure. The secret of their success will continue to be keeping their successes secret.

However, this does not absolve the rest of society from remaining engaged in community, by being inclusive, welcoming, and helpful, while also maintaining a level of vigilance many had come to associate with a bygone era.

John Blaxland *is Professor, Strategic and Defense Studies Center Australian National University.*

The new hacking game...

Russian gov. hackers may disrupt Germany's 2017 elections: Germany's intel chief

Source: http://www.homelandsecuritynewswire.com/dr20161129-russian-gov-hackers-may-disrupt-germany-s-2017-elections-germany-s-intel-chief

Nov 29 – The Russian government's broad hacking campaign to undermine Hillary Clinton's presidential bid and help Donald Trump become the U.S. next president may well be the template Russia is following in the run-up to next year's German general election. Russia has actively – both overtly and covertly — supported right-wing, ethno-nationalist, populist, and proto-Fascist parties like Front National in France, Golden Dawn in Greece, Ataka in Bulgaria, and Jobbik in Hungary. These parties share not only anti-immigrant policies – but they are also fiercely anti-EU and want to distance their countries from NATO. One of the major themes in the public rallies – and political platform – of the German far-right, anti-Muslim, anti-immigrant Pegida movement is that the influence of President Vladimir Putin's Russia in Germany would be a welcome alternative to the imperial designs of the United States and Brussels.

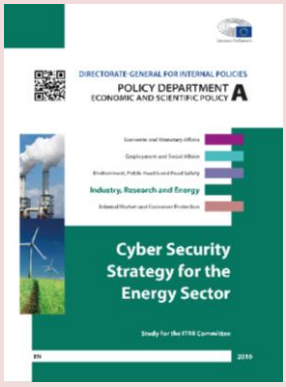
Cyberwar: Growing worries about Russia hacking, disrupting the U.S. election

Source: http://www.homelandsecuritynewswire.com/dr20161104-cyberwar-growing-worries-about-russia-hacking-disrupting-the-u-s-election

Nov 4 – The U.S. government is worried that Russian government hackers may try to hack and disrupt the upcoming presidential election. The U.S. intelligence community, DHS, and private cybersecurity experts have already identified a broad and sustained hacking effort by hackers working for two Russian government agencies aiming to undermine the campaign of Hilary Clinton and help Donald Trump. The United States has privately warned Russia in no uncertain terms that any attempt to manipulate vote counts would result in serious breaches — still, federal and state officials are focusing on five possible ways Russia may hack the election. Experts warn that Russia's long-term goal is to undermine the American political system by disrupting and discrediting the election process, sowing doubts and suspicion, and providing "proof" for the conspiratorial beliefs about a corrupt political system in which the electoral process is "rigged" and where "international bankers" are conspiring to "steal" the election.

Cyber Security Strategy for the Energy Sector

Source:http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

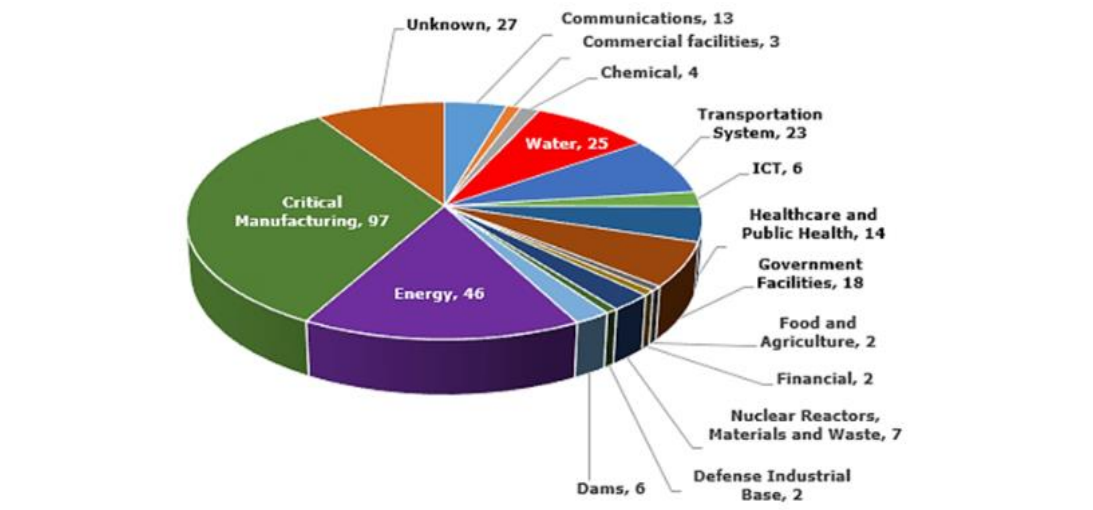


Dec 05 – This study is provided by the Policy Directorate at the request of the ITRE Committee. The EU energy infrastructure is transitioning into a decentralised, digitalised smart energy system. Already, energy operations are increasingly becoming the target of cyber-attacks with potentially catastrophic consequences. Development of energy specific cyber security solutions and defensive practices are therefore essential. Urgent action is required, including empowering a coordination body, to promote sharing of incident information, development of best practice and relevant standards.

One of the most recent publicised cyber security breaches within the electricity sector was the Ukraine power grid cyber-

attack on 23 December 2015. In this attack, three of the regional electricity distribution companies (known locally as 'Oblenergos') in Ukraine were

Figure 3: ICS-CERT logged security incidents by sector



Source: [https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf]

the subject of a co-ordinated series of cyber-attacks implemented over a 30-minute period. The attackers gained unlawful access to and control of the distribution companies' computer and SCADA systems affecting 110kV and 35kV substations. This resulted in outages which lasted several hours, and affected approximately 225 000 people in these regions.Once they were able to restore electrical

Figure 4: Overview of the Cyber Attack on the Ukraine Power Grid

1. Spear phishing to gain access to the business networks of the Oblenergos
2. Theft of administrative credentials from the business networks
3. The use of virtual private networks (VPNs) to enter the ICS network
4. The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator Human Machine Interface (HMI).
5. Serial-to-Ethernet communications devices impacted to prevent access to the compromised SCADA systems. Utilizing UPS systems to impact connected load with a scheduled service outage
6. Telephone denial-of-service DDoS attack on the call centre to ensure customers could not report outages

Source : [https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf]

service, the Oblenergos continued to operate their distribution systems in an operationally constrained mode.

The cyber-attacks in Ukraine are very significant because these are the first publicly acknowledged incidents of an attack against OT systems in a nation's CI resulting in a power outage.

New Botnet is Attacking the US West Coast with Huge DDoS Attacks

Source: https://www.hackread.com/new-mirai-like-botnet-ddos-attack/

Dec 06 – In a blog post by CloudFlare, it has been revealed that the US West Coast is likely to become the target of yet another huge DDoS attack but this time it will be conducted with a different botnet than Mirai that was using during Dyn DNS attack which forced sites like Twitter, Amazon, PayPal etc to go offline for hours.

The content delivery network states in the blog post that the company has been observing the overflow of traffic from about two weeks. It seems to be coming from a single source. Seemingly, someone was firstly testing their abilities with a 9-to-5 attack schedule and then the attack pattern was shifted to 24 hours. **This new botnet is either equal or superior to the Mirai botnet.**

When Terror Meets Technology

Source: http://www.cxotoday.com/story/when-terror-meets-technology/

Dec 12 – **Technology is indeed a double edge sword, its pros and cons highly depend on the user. While technology helps mankind to lead a better life, it can sometimes become an instrument to cause harm to humanity.** The technology proficiency of terror outfits is on a swift rise in recent years. Today, terrorists are harnessing Hi-tech tools and digital platforms to propagate radicalization. Unfortunately, counter terrorism agencies are not yet successful in cracking down the rampant use of technology for terror plots.

The United Nations and Tech giants, including Microsoft and Google discussed the increasing use of social media and technology among terror outfits in the UN Security Council meet recently. The body noted the urgent need to understand that how the terror outfits such as ISIS, Boko Haram and Al Qaeda are leveraging on the internet to propagate radicalism. The Security Council also voiced a need to develop a counter narrative campaign to amplify active denouncers of these groups.

Unfortunately, it is quite difficult to refrain anybody from exploring digital platforms. Microsoft pointed out that technology companies face a daunting challenge in stopping

terrorists from accessing online platforms, as the company needs to respect free-speech rights. Since there is no universal definition of 'terror outfit', technology giants find it difficult to differentiate between the hate speech and free speech. The growing use of exception tools is also an obstacle in identifying dedicated social media accounts of terrorist outfits.

Terrorists Embrace Technology

Gone are the days when guns and ammunition were the only weapons of terrorists. The terror outfits today are backed by high end technology tools, dedicated social media handlers and an army of hackers. Terror outfits such as the Islamic State of Iraq and Syria (ISIS), Boko Haram, Al-Qaeda has emerged as the most high-tech terror organizations. Using technology as a weapon to promote radicalism, these outfits have laid the foundation of virtual terrorism.

The outfit also has a dedicated army of cyber terrorists who are far ahead of counter terrorism agencies. ISIS rise in the virtual world clearly shows that the technology proficiency of terror outfits is on a swift rise. According to Ghost Security Group, the ISIS has developed an Android mobile app called Amaq Agency to share radical content and recruiting material. The app was also reportedly advertised on Telegram groups and Twitter. Though many sources are unavailable but it is still possible to find the app and download it. Terrorists are even equipped with the self-destructing software.

Experts also fear their hacking capabilities that could be used to attack a critical infrastructure to sabotage, or IT Infrastructure of federal governments to steal sensitive data. The ISIS is trying to recruit hackers and experts around the world to involve them in hacking campaigns. They are offering hackers handsome packages up to $10,000 for every successful cyber-attack. Over 30,000 youngsters have allegedly been in contact with the Daesh wing of ISIS.

Social Media: Essence Of Cyber Terrorism

Social media is an essential element of modern terrorism. These powerful digital platforms allow terrorists to communicate, to make propaganda and recruit new sympathizers. Outfits like ISIS have penetrated deep into the virtual world by using the platforms like Twitter, Facebook, Instgram, YouTube, WhatsApp, Telegram etc. through which the outfit instigates radical forces. ISIS has also created its own social network called "Kilafahbook".

Apart from digital platforms, terrorists also make a large use of mobile applications for communications.

Security experts have uncovered a number of websites offering pro-jihad content designed using a 'comic-style' and high impact Videos and Animations. Experts have also discovered documents containing the training material, including manuals for the preparation of chemical weapons and bombs. ISIS has allegedly launched a magazine titled Kybernetiq that instructs militants about technology. According to DigitaShadow, Ghost Security Groupclaimed to have taken down 149 Islamic State propaganda sites, 110,000 social media accounts, and over 6,000 propaganda videos so far.

Encryption Continue To Be A Thorn

While encryption will continue to be a thorn in the side of counter terrorism agencies, the extremist group continues to exploit the Internet in an overt, not covert, method with little resistance. Web Intelligence firm Recorded Future published a research on the use of encryption made by Al-Qaeda after the Snowden leaks in 2014. The study reported that members of Al-Qaeda were developing a series of new encryption software in response to NSA surveillance. According to reports, Al-Qaeda groups have developed several encryption tools such as Mujahideen Secrets, Tashfeer al-Jawwal, Asrar al-Ghurabaa, Amn al-Mujahid etc. to protect online and cellular communications. Considering the ongoing misuse of encryption, both federal governments and social media giants needs to find the middle path to stop terrorists from using the tool.

With terror outfits expanding their wings in the virtual world, both the counter terrorism agencies and tech companies need to collaborate to fight against these radical forces. It is not possible to ban terror outfits from using technology, but the collaborative efforts of all the federal governments, tech giants and international counter terrorism agencies can certainly help to combat radical forces.

Malaysia to Establish Cybersecurity Academy

Source: http://www.infosecurity-magazine.com/news/malaysia-to-establish/

Dec 05 – **The Malaysian Digital Economic Corporation (MDEC) and Protection Group International (PGI) have signed an agreement to work together to develop a cybersecurity academy in Malaysia.**

It will be known as the **UK-APAC Centre of Security Excellence** and will see PGI and MDEC collaborate, generate and formulate awareness and strategies to regularly promote bilateral cybersecurity research and investment opportunities. PGI will provide strategic advice on the design of the academy's cybersecurity courses, infrastructure and resources. PGI will also draw on its curriculum of UK Government Communication Headquarters (GCHQ) Certified Training courses, materials and expert trainers to conduct pilot programs and oversee the development of local trainers for continuous learning at the academy.

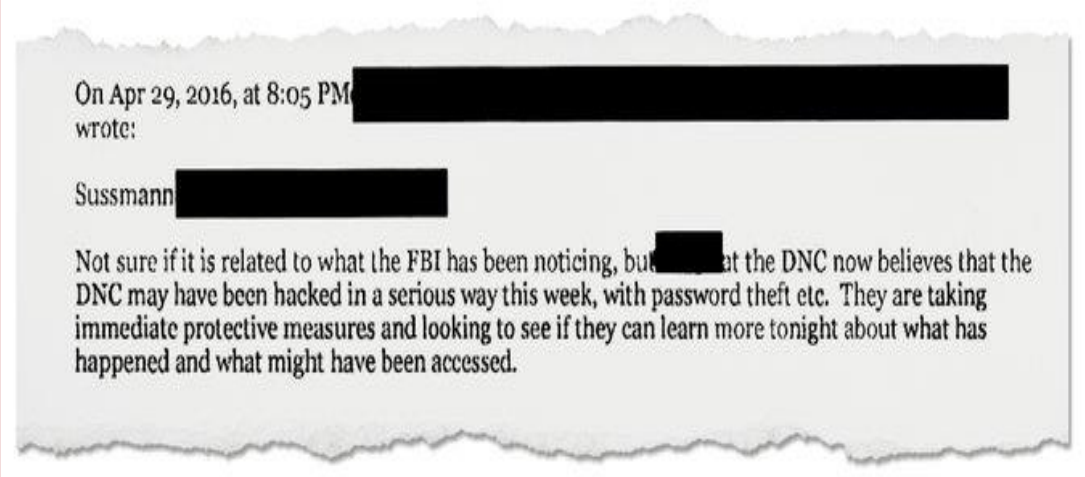
"Studies show that up to 2 million cybersecurity jobs will be unfilled by 2019 unless there is a step change in the numbers of new people entering the cyber security profession," said Barry Roche, CEO of PGI. "PGI set up its Cyber Academy to play a leading role in identifying and training new entrants, reskilling those seeking to change careers into cyber, and continuing the professional development of the cyber security workforce. We are delighted to have demonstrated our expertise in these areas to MDEC and to offer our services in creating a new Academy for the Asia Pacific region."

PGI was opened in September 2014 by the Rt. Hon Karen Bradley MP, now the Secretary of State for Culture, Media and Sport in the UK, to help tackle the global cyber-skills shortage. Since then, **PGI has trained over 1,000 cyber specialists from 21 countries**, and developed tailored courses and programs for government, police and armed forces clients, as well as senior management, mainstream IT specialists and entire workforces, from corporate to critical infrastructure clients. PGI's immersive courses are powered by its training infrastructure, which offers students realistic scenarios on up to 3,600 virtual machines.

"Seeing PGI's workforce conversion training in action has been extremely interesting and insightful," said Yasmin Mahmood, CEO of MDEC. "Learning from their ability to convert IT staff into frontline cyber security professionals will be pivotal to our cyber-development. We are looking forward to harnessing PGI's expertise to ensure that the UK-APAC Centre of Security Excellence can play a similar role in creating much-needed cyber security professionals in Malaysia and the broader Asia-Pacific region."

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

Source 1: http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html
Source 2: http://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html


On Apr 29, 2016, at 8:05 PM [redacted] wrote:

Sussmann [redacted]

Not sure if it is related to what the FBI has been noticing, bu[redacted]t the DNC now believes that the DNC may have been hacked in a serious way this week, with password theft etc. They are taking immediate protective measures and looking to see if they can learn more tonight about what has happened and what might have been accessed.

Michael Sussmann, a Washington lawyer and former cybercrime prosecutor at the Justice Department, received an email in late April confirming that the D.N.C.'s computer system had been compromised.

▶ **Read full articles in sources' URL.**

The Year of the Railway Station

Source: https://www.domesticpreparedness.com/preparedness/the-year-of-the-railway-station/

Dec 21 – The year 2017 should be a great year for mobility and infrastructure in the United States. All signs are pointing to a robust economy, and policymakers are looking favorably on transportation projects – road, rail, air, public, private, and in between. In particular, the upcoming year will see a number of passenger rail projects moving forward.

Significant and highly visible high-speed intercity passenger train projects are in the planning stages in Florida, California, Texas, and states in the Northeast. There is even a proposed magnetic levitation train in the Northeast Corridor. These projects are not going to magically appear in a protective bubble, however. Threats are real and documented, and 2017 may be the year when international terrorism retools for U.S. passenger rail.

Warnings With Cyber & Physical Attacks

Vulnerabilities abound within the passenger rail sphere. Cybersecurity events such as the November 2016 hacking of the San Francisco Municipal Light Rail System that forced Muni to suspend charging for rides, and transitional periods like the implementation by commuter railroads of positive train control suggest areas for attention by security interests, as do systems increasingly dependent on electric grids and electronic backends like passenger ticketing. Trains in transit have been platforms for onboard terrorist efforts like the August 2015 foiled armed attack on the French TGV as well as attempts to attack the right of way and blow up the rails (TGV in 1995), some successful (Muniguda, Munikhol, and other incidents in India in 2015).

Perhaps the best case to be made for 2017 is for a focus security efforts at stations, where there will be large masses of people. For example, the Texas Central project calls for eight-car trains carrying 200 people with rush-hour departures every 30 minutes. Terrorists could exploit such station vulnerabilities – for example, a coordinated knife attack inside the Kunming station (China) in 2014 killed 29 civilians and injured more than 140. Twenty people died in the bomb attack on the Maelbeek Metro station in central Brussels in March 2016. A 2011 Inspector General's report criticized how Amtrak and the Department of Homeland Security were spending security money, concluding, "The traveling public remains at risk for a potential terrorist attack at Amtrak's high-risk stations."

Decisions & Innovative Thinking Going Forward

Yet, there is little indication that high-speed train stations – "Palaces of Transport," according to the U.S. High Speed Rail Association, and "iconic structures" per the Texas Central Railroad – are benefitting from innovative thinking when it comes to security. California High-Speed Rail's Request for Qualifications for the High-Speed Rail Systemwide Vision Plan for Stations of 2015 talks about world-class sustainable public places, but does not mention safety or security. Texas Central held a design competition in 2016 among university architecture, engineering, and transportation programs, with judging based on programming, urban connectivity, use of local materials, environmental sustainability, and customer focus. Security was nowhere in the mix.

There is a continuing debate about the relative merits of airline-style security measures (landside/airside separation, personal and baggage screening, metal detectors, and radiation devices) as opposed to current practices for surface transportation like rail and bus. Even so, there are generally accepted approaches, some as an outgrowth of incidents like the Tokyo (Japan) sarin gas attack of 1995 – adding surveillance cameras, revising training and response protocols, removing trash cans where bombs can be hidden, controlling access to secured areas, providing two-way communication through public address systems and call boxes, intrusion

detectors, and so forth. Advocates for both sides argue the relative merits of multilayer security, level of separation from vehicle side and groundside, and level of identification with boarding passes, as well as whether security queues and baggage checks are even realistic for train operations.
It is time to wrap up these conversations and move forward with innovation in station design. Hopefully, 2017 will be remembered as the year that new, secure stations were planned from the ground up.

Steven Polunsky *is a research scientist with the Texas A&M Transportation Institute's Policy Research Center. He previously directed legislative committees overseeing transportation, homeland security, and regulatory policy where he led an award-winning technology initiative that saved thousands of taxpayer dollars. Prior service includes director of research and planning for the Texas High-Speed Rail Authority and legislative policy analyst for the Texas Department of Transportation. He has an MPA from the LBJ School of Public Affairs as a Robert Strauss Fellow and an MA in Security Studies with Distinction from the Naval Postgraduate School.*

"Bugs" to Assist First Responders

Source: http://i-hls.com/2016/12/first-responders-new-little-helpers/

Dec 03 – An original technology allows the use of unmanned aerial vehicles (UAVs) and insect cyborgs, or **biobots**, to map large and unsafe zones, like cities shortly after an earthquake. This combination of software and hardware has been developed by researchers at North Carolina State University.

"The idea would be to release a swarm of sensor-equipped biobots into a collapsed building or other dangerous, unmapped area," Edgar Lobaton, an assistant professor of electrical and computer engineering at NC State and co-author of two papers describing the work, told eurekalert.org.

Once the program receives enough data to map the defined area, the UAV moves forward to hover over an adjacent, unexplored section. The biobots move with it, and the mapping process is repeated. The software program connects the findings to a previous, existing map. This can be repeated until the entire region or structure has been mapped; that map could then be used by first responders or other authorities.

The biobots would be allowed to move freely within a defined area and would signal researchers via radio waves whenever they got close to each other. Custom software would then use an algorithm to translate the biobot sensor data into a rough map of the unknown environment.

"This has utility for areas where GPS can't be used," Lobaton says. "A strong radio signal from the UAV could penetrate to a certain extent into a collapsed building, keeping the biobot swarm contained. And as long as we can get a signal from any part of the swarm, we are able to retrieve data on what the rest of the swarm is doing. Based on our experimental data, we know you're going to lose track of a few individuals, but that shouldn't prevent you from collecting enough data for mapping."

"We had previously developed proof-of-concept software that allowed us to map small areas with biobots, but this work allows us to map much larger areas and to stitch those maps together into a comprehensive overview," Lobaton says. "It would be of much more practical use for helping to locate survivors after a disaster, finding a safe way to reach survivors, or for helping responders determine how structurally safe a building may be".

New Medical Disaster Drone for Audience of Homeland Security, Global Health Organizations

Source: http://www.hstoday.us/single-article/new-medical-disaster-drone-for-audience-of-homeland-security-global-health-organizations/70e79cf7acf0eab3197121549daad4bc.html

Dec 07 – Two new disaster drones delivered telemedical packages to victims and rescue personnel in a simulated mass casualty event Tuesday at John Bell Airport in Bolton, Mississippi as a demonstration of the Telemedical Drone Project, known as HiRO (Health Integrated Rescue Operations), which was developed by Dr. Italo Subbarao, senior associate dean at William Carey

University College of Osteopathic Medicine, and Guy Paul Cooper Jr., a fourth year medical student at WCUCOM.

Experts from Hinds Community College, in collaboration with Subbarao and Cooper

designed and built both disaster drones, which are capable of carrying telemedical packages in adverse conditions.

"These drones have impressive lift and distance capability, and can be outfitted with a variety of sensors, such as infrared, to help locate victims," said Dennis Lott, director of the unmanned aerial vehicle program at Hinds Community College. "Working together, we're able to develop, test, and bring this technology to the field. It is just a matter of time before the drones are universally adopted for emergency and disaster response toolkits."

The HiRO technology was debuted before an audience which included Mississippi Governor Phil Bryant and representatives from the Department of Homeland Security (DHS), federal law enforcement agencies and the United Nations.

"Reaching the victims is the critical challenge in these situations. As an osteopathic physician, my goal was to find ways to help save lives," and, "A medical drone is the bridge that delivers life-saving treatment directly to the victims, giving remote physicians eyes, ears and voice to instruct anyone on site," said Subbarao, a nationally recognized expert in disaster and emergency medicine.

According to the announcement, "The concept arose when the two studied the medical response to the devastating EF-4 tornado that struck Hattiesburg, Mississippi in February 2013. In the past two years, they've developed multiple prototypes to support rural and wilderness medical emergencies, including the two newest iterations: ambulance drones

designed to support victims and rescue personnel during mass shootings, bombings or other terrorist attacks."

During the demonstration, two new telemedical packages were deployed, one for a severely injured victim and the other for a mass casualty setup capable of treating up to 100 people with significant to minor injuries. Both kits incorporated DHS recommendations provided through the "Stop the Bleed" initiative.

"The two highly advanced mobile telemedical kits provide immediate and secure access to a provider on the other end of the screen," Cooper said, noting, "**The package was designed for use in the chaos and confusion where guidance must be simple, direct and user**

friendly. We feel that the features in these kits empower the provider and bystander to save lives."

According to the announcement, "When the critical care kit opens, the physician appears on video and can direct treatment. **The kit includes Google Glass, which allow the wearer to be hands free and to move away from the drone while maintaining audio and visual contact with the physician**."

Remote-control skillful rescue robot demonstrated

Source: http://www.homelandsecuritynewswire.com/dr20161215-remotecontrol-skillful-rescue-robot-demonstrated

Dec 15 – A group of Japanese researchers developed a prototype construction robot for disaster relief situations. This prototype has improved operability and mobility compared to conventional construction machines.

As part of the Impulsing Paradigm Challenge through Disruptive Technologies Program (ImPACT)'s Tough Robotics Challenge Program, a group of research leaders at Osaka University, Kobe University, Tohoku University, the University of Tokyo, and Tokyo Institute of Technology developed construction robots for disaster relief in order to solve various challenges of conventional construction machines used in such situations. Using a prototype machine with elemental technologies under development, verification tests were performed on places that represented disaster sites, and a certain level of performance was confirmed. Osaka U says that this **prototype looks like an ordinary hydraulic excavator, but, specifically, has the following elemental technologies:**

- Quickly and stably controlling heavy power machines with high inertia by achieving target values regarding location and speed through fine-tuning and by controlling pressures on a cylinder at high speeds.
- Estimating external load of multiple degree of freedom (DOF) hydraulically driven robot from oil pressure of each hydraulic cylinder. The estimated force will be used for force control or force feedback to the operator of tele-operated rescue robots.
- Measuring high frequency vibration by a force sensor installed at the forearm of the robot and giving the operator vibrotactile feedback.
- Flying a multi-rotor unmanned aircraft vehicle UAV ("drone") to the place of the operator's choice and obtaining image information. Long flights and pin-point landing of the drone are available due to power supply through electric lines and a power-feeding helipad for tethering the drone.

- Presenting the operator images of an overhead view from an arbitrary place by using 4 fish-eye cameras mounted on the robot in real time so that the operator can assess the area surrounding the robot.
- Using a far-infrared ray camera capable of viewing with long-wavelength light so that the operator can operate the robot while assessing the situation even under bad weather conditions like fog.

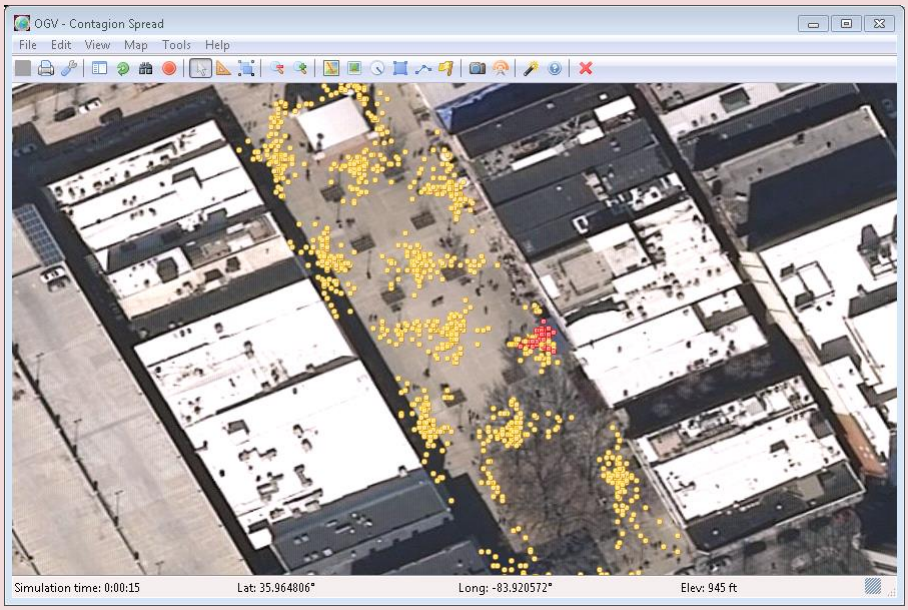
In addition to the above-mentioned technologies, this group is developing several useful elemental technologies and making efforts to improve their technical performance. They are also developing new robots with a double rotation mechanism and double arms with the purpose of achieving higher operability and terrain adaptability.

New incident management planning tool for first responders

Source: http://www.homelandsecuritynewswire.com/dr20161221-new-incident-management-planning-tool-for-first-responders

Dec 21 – A suspicious package is found in a public park. An unattended bag is found by a trash can at the metro or a street corner. A person with a weapon is reported at a school or mall or other public location. Unfortunately, these are not uncommon occurrences, and responder agencies – from small towns to big cities – must all know how to respond and work together. That requires training, technology, tools, and time. The Department of Homeland Security Science and Technology Directorate (S&T) Explosives Division (EXD) has a solution.

S&T says that EXD has funded research at the Oak Ridge National Laboratory to continue development of the Incident Management Preparedness and Coordination Toolkit (IMPACT), a geospatial tool designed to enhance situational awareness, communication, and collaboration during and for security events. This tool was originally funded by the DHS Office of Bombing Prevention to help bomb squads assess impacts from improvised explosive devices (IEDs). Since its original release, IMPACT has expanded its capabilities to provide tools to assist in active shooter planning, downwind hazards from the release of dangerous chemicals, large stadium evacuation and casualty simulations, security surveys, and monitoring large event social networks for emergency response support.



A built-in contagion spread model can be used for mass gathering events.

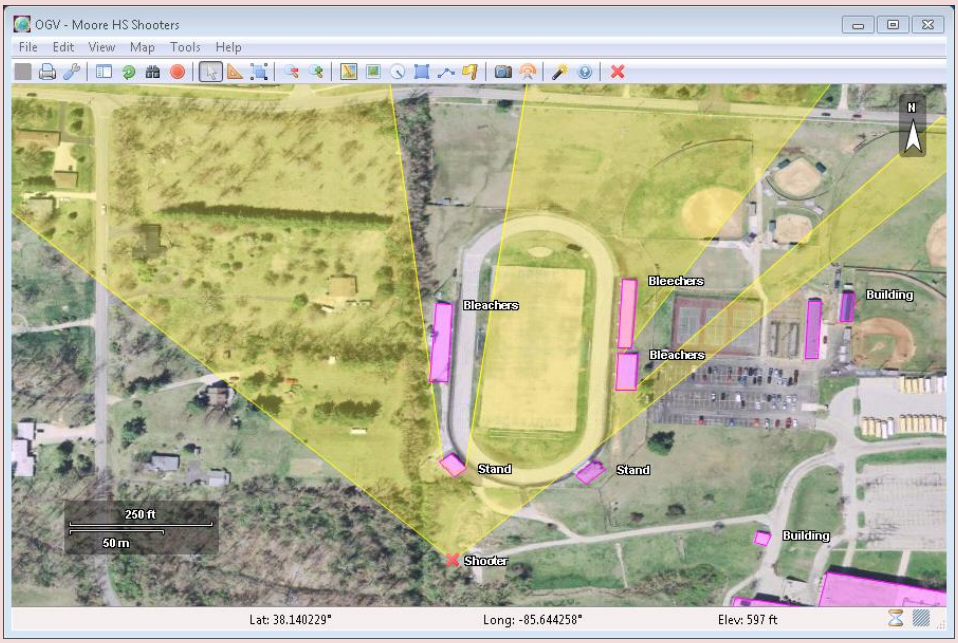
"IMPACT is a free, all-hazards planning tool for first responders, emergency managers, and other security professionals. It combines simulation, visualization, and mapping into an integrated user interface similar to a smart phone or tablet," explained S&T Program Manager Elizabeth Obregon. "First responders can use it for planning, situation awareness, and response to natural and man-made disasters. It uses common data formats to easily exchange data with other map-based tools."

IMPACT is currently being used and evaluated by more than 400 agencies at the federal, state, and local levels including the Transportation Security Administration, the Federal Emergency Management Agency, the Centers for Disease Control and Prevention, and police departments at the state and local levels.

The only Geographic Information System tool specifically tailored for counter-improvised explosive devices, homemade explosives, active shooter responses, and first responder

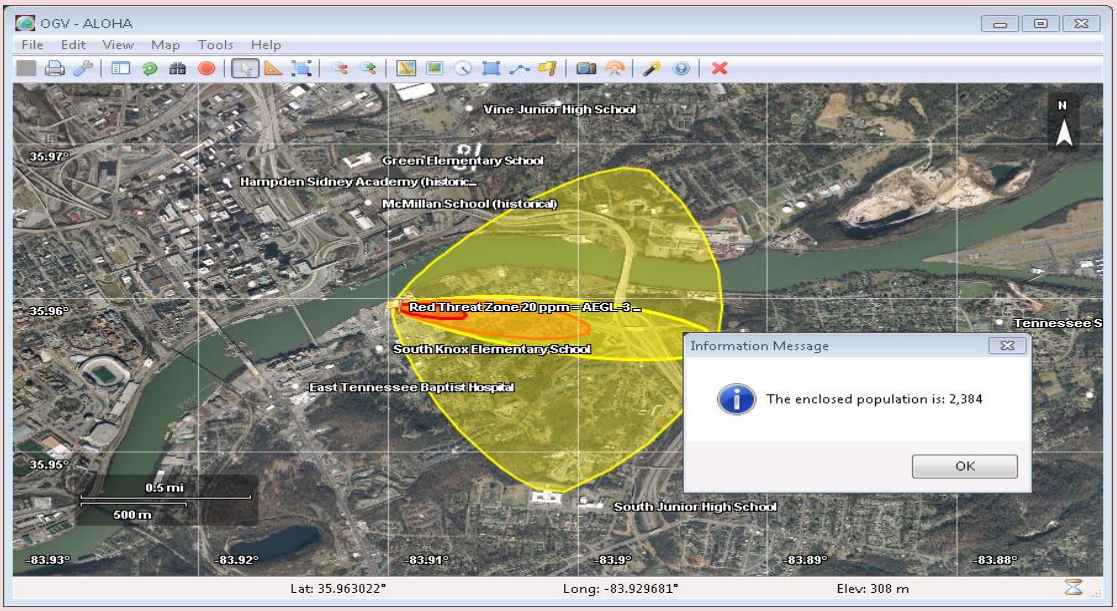
use, IMPACT allows responders to conduct both live and table top exercises for simulated active shooter and IED attacks, Obregon explained.

Repeatedly tested in the field by numerous law enforcement and first responder organizations, IMPACT has been successfully used to mitigate real world incidents. It was briefed to the United States Capitol Police immediately after a March 2016 incident in which live shots were fired at the Capitol Visitors Center. Since that briefing, USCP has become a growing end user of the tool and plans to use it for a number of upcoming gatherings in 2017. In addition, table top exercises generated by IMPACT were credited with mitigating an active shooter event at a school in Louisville, Kentucky, in September 2014. The tool is Section 508 compliant, enabling it to be used across the federal government and by its mission partners.



A built-in wizard calculates active shooter line-of-sight overlays.

S&T was interested in developing this tool as it gives first responders a free, easy to use capability to conduct better organized and more efficient exercises, provide for facility protection, and plan for major public and security events, Obregon said. IMPACT can be considered a success as many organizations that have been briefed on the tool, including the Secret Service, Capitol Police, Washington Metropolitan Area Transit Authority, the Transportation Security Administration, and others, have expressed interest in adopting the tool and are currently in the process of doing so. In addition, IMPACT has provided hundreds of agencies at the federal, state, and local level with an exercise, protection and planning capability that they did not have before but urgently needed.



ALOHA can produce a KML plume file and imported into IMPACT where the population can be calculated.

VR Technology to Help Train Military Units and First Responders

Source: http://i-hls.com/2016/12/vr-technology-help-train-military-units-first-responders/

Dec 15 – YDreams Global, the creative and technical supplier for brands such as Cisco, Qualcomm, Intel as well as the Government of Rio de Janeiro, has recently announced that it has signed a contract to use its Virtual Reality (VR) technology in the United States.

The company helps create digital experience combining both Augmented and Virtual Reality technologies, design, and intelligence.

The first project sold in the United States will be released in the second week of December.

VR Chinook training

According to the company's press release, YDreams Global plans to create a virtual reality platform to be used by the military and other government agencies such as police departments, fire departments and emergency medical services that could use VR as a training experience. By using this technology for training, for example, the military, police and fire services would be able to experience accurate real-life situations that would be impossible to replicate in physical world exercises.

The company will create a lifelike experience and improve military technique, according to finance.yahoo. Marcos Alves, Director of YDreams Global products division said: "VR is emerging as a technology that can improve the way we learn and experience stressful situations in a safer environment".

By using VR simulations, it is possible to optimize training budget while simultaneously increasing the number of scenarios. "YDreams is setting out to offer VR training techniques to thousands of military, police, and other agencies in this space. By bringing VR technology into their training routine, a new era of military training may be possible, increasing safety for both sides: the police force and the general population. The defense sector has a massive market and we feel that YDreams has a distinct advantage to develop VR techniques for this sector," declared the CEO of the Company, Daniel Japiassu.

"Our goal for 2017 is to accelerate our virtual reality growth strategy in North America, focusing on our fortune 500 relationships in place already," he added

Very few companies in the world provide this technology and YDreams Global's goal is to expand through commercial partners in North America, South America. and Europe, to offer this platform to military and civilian defense forces.

YDreams Global anticipates that the working version will be available in the second quarter of 2017, a project which involves partnerships with several hardware companies.

Syrian crisis altered region's land and water resources

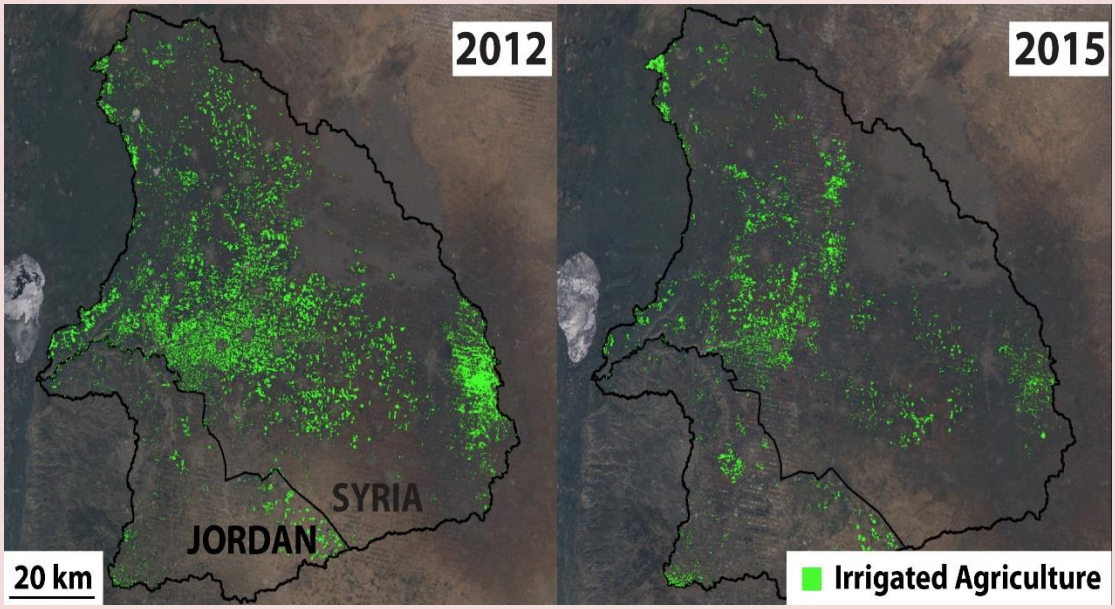
Source: http://www.homelandsecuritynewswire.com/dr20161206-syrian-crisis-altered-region-s-land-and-water-resources

Dec 06 – The Syrian civil war and subsequent refugee migration caused sudden changes in the area's land use and freshwater resources, according to satellite data analyzed by Stanford researchers.

The findings, published in the 5 December issue of *Proceedings of the National Academy of Sciences*, are the first to demonstrate detailed water management practices in an active war zone. Using satellite imagery processed in Google Earth Engine, Stanford researchers determined the conflict in Syria caused agricultural irrigation and reservoir storage to decrease by nearly 50 percent compared to prewar conditions.

"The water management practices in Syria have changed and that's visible from space," said study co-author and principal investigator Steven Gorelick, the Cyrus Fisher Tolman Professor in Stanford's School of Earth, Energy & Environmental Sciences. "The Syrian crisis has resulted in a reduction in agricultural land in southern Syria, a decline in Syrian demand for irrigation water and a dramatic change in the way the Syrians manage their reservoirs."

Stanford U says that the study focuses on impacts from 2013 to 2015 in the Yarmouk-Jordan river watershed, which is shared by Syria, Jordan, and Israel. Study co-author Jim Yoon, a Ph.D. candidate in Earth system science at Stanford, thought of the idea to study the Syrian war's impact on water resources when he noticed an increase in Yarmouk River flow based on streamflow data from Jordan's Ministry of Water and Irrigation.



Irrigated land area decreased by 50 percent in the Yarmouk Basin during the Syrian civil war. (Image credit: Landsat 7)

"The big challenge for us was that it was going to be next to impossible to get on-the-ground data in Syria," Yoon said. "We couldn't really close the story without this information in Syria – that was what led us to use remote sensing data."

Using composite images of the eleven largest Syrian-controlled surface water reservoirs in the basin, researchers measured a 49 percent decrease in reservoir storage. Irrigated crops are greener than natural vegetation during the dry summer season. This characteristic was used to show Syria's irrigated land in the basin had decreased by 47 percent.

Gorelick and his team looked at water management and land use on the Jordanian side of the Yarmouk basin and in Israel's Golan Heights as a baseline for understanding areas unaffected by the refugee crisis.

New precedent

"It's the first time that we could do large-scale remote sensing analysis in a war zone to actually prove a causal relation between conflict and water resources," said lead author Marc Muller, a postdoctoral researcher in Gorelick's lab. "With these new tools, you can do analysis and iterate very quickly – the effects were so strong, it was really easy to see right away."

The research sets a precedent for using remote sensing data to understand environmental impacts in war zones or other areas where information otherwise could not be collected.

"To be able to get this type of detailed information about a region where data on the ground are scarce is an important contribution," said Gorelick, who is also a senior fellow at the Stanford Woods Institute for the Environment. "This shows in the extreme case how relevant information can be obtained in an efficient and scientifically valid manner."

Refugees in Jordan

Syria's abandonment of irrigated agriculture, combined with the region's recovery from a severe drought, caused increased Yarmouk River flow to downstream Jordan, one of the most water-poor countries in the world. However, Jordan has absorbed hundreds of thousands of refugees from Syria since 2013.

"It's slightly good news for Jordan, but it's not a big bonus compared to what Jordan has had to give up and sacrifice for the refugees," Gorelick said. "Even in terms of providing water for the refugees, this transboundary flow is not compensation."

Despite this unexpected result, Jordan's flow from the Yarmouk River remains substantially below the volume expected under bilateral agreements with Syria, a result of legal and illegal reservoirs built in Syria, according to Gorelick.

The Jordan Water Project

Gorelick and his team have cooperated with Jordan on water management research since 2013 through the Jordan Water Project (JWP), a National Science Foundation-funded international effort to analyze freshwater resource sustainability. While experts speculate climate change can lead to conflict, Yoon said it was interesting to examine Syria from a different perspective.

Renewable internal freshwater resources per capita (m3)		
	1997	2013
Israel	129	93
Jordan	153	106
West Bank & Gaza	300	195
Syria	471	327
Water scarcity level	1,000	
Iraq	1,636	1,042
Lebanon	1,552	1,068

"In the past few years, there's been increasing focus on how climate change and drought influences conflict, but there hasn't been as much research on how conflict can actually lead to impact on the environment and water resources," Yoon said.

Ranked as one of the world's top three water-poor countries, Jordan faces serious potential impacts from climate change. One of the key goals of the JWP is to develop an integrated hydro-economic model of the Jordanian water system in order to explore policy interventions.

Gorelick also directs the Global Freshwater Initiative at Stanford and runs the Hydrogeology and Water Resources Program at Stanford's School of Earth, Energy & Environmental Sciences.

— Read more in Marc François Müller et al., "Impact of the Syrian refugee crisis on land use and transboundary freshwater resources," Proceedings of the National Academy of Sciences (5 December 2016).