International CBRNE Institute

CBRNE NEWSLETTER TERRORISM

November 2016

E-Journal for CBRNE & CT First Responders

www.cbrne-terrorism-newsletter.com

Suspension of U.S.-Russia plutonium disposal agreement a setback: Expert

Source: http://www.homelandsecuritynewswire.com/dr20161025-suspension-of-u-s-russia-plutonium-disposal-agreement-a-setback-expert

Oct 25 – **Earlier this week the lower house of the Russian parliament approved President Vladimir Putin's decree on suspending the U.S.-Russian Plutonium Management and Disposition Agreement (PMDA), which requires each nation to dispose of thirty-four metric tons of plutonium from its dismantled nuclear weapons and military stockpiles.** Edwin Lyman, a senior scientist at the Union of Concerned Scientists (UCS), answers questions about the agreement and the ramifications of the Russians' recent action.

Q: What is your take on Russia's suspension of the Plutonium Management and Disposition Agreement?

A: It is very unfortunate that Russia has decided to suspend the PMDA. The PMDA is a very important measure that would provide assurances to the international community that the United States and Russia are disposing of plutonium stockpiles that neither country needs any more for nuclear weapons. In addition, the PMDA helps reduce the possibility that terrorist groups could steal separated plutonium. This is a very real concern in both countries. Moving forward with the agreement is in the interest of both parties.

Q: Russia has claimed that the United States is violating the agreement by changing its disposition method from irradiating the plutonium as mixed-oxide (MOX) fuel for commercial nuclear reactors to a process called dilute and dispose. Isn't Russia therefore justified in suspending the agreement?

A: The United States has not violated the terms of the PMDA by proposing that it change its plutonium disposition approach from irradiation of MOX fuel in light-water reactors to dilution and geologic disposal. The PMDA allows either party to change its approach provided that both sides agree in writing — and that has happened before. **In 2010, the United States allowed Russia to change the disposition method it had committed to when the agreement was originally signed in 2000.** The United States and Russia had begun discussions on the proposed new U.S. method, but formal negotiations have not taken place. Meanwhile, work on the U.S. MOX fuel fabrication plant is continuing until the viability of the alternative approach can be fully demonstrated.

UCS has concluded that the dilute-and-dispose method would render U.S. plutonium sufficiently inaccessible to satisfy the intent of the PMDA. Also, the method could be implemented much more quickly than the MOX approach. Plutonium would be diluted to a low concentration with materials that would make it difficult — although not impossible — to chemically extract the plutonium. **This mixture would be placed in small quantities — about 300 grams, or 0.66 pounds, of plutonium — in large waste drums. The drums would be placed nearly half a mile underground in the Waste Isolation Pilot Plant (WIPP), a U.S. government geologic repository for nuclear waste. Over time, the salt caves where the waste is buried would collapse over the waste, rendering it irretrievable. In any case, the PMDA allows for the possibility of international monitoring.** Any attempt by the United States to recover the plutonium would take a significant amount of time and would be easily observable by inspectors.

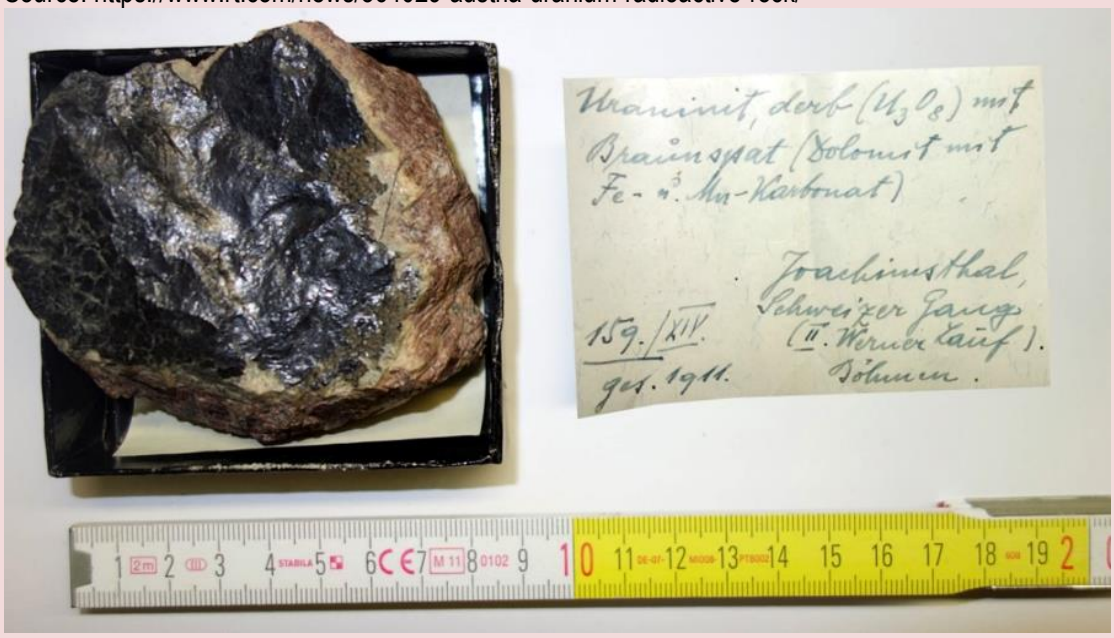
Russia has raised the concern that unlike reactor irradiation, the dilute-and-dispose method does not change the isotopic composition of plutonium from weapons-grade to reactor-grade. This is not a significant issue because the United States — and presumably Russia — can use reactor-grade plutonium to make nuclear weapons. However, to alleviate Russian concerns, the United States could obtain reactor-grade plutonium from another country, such as Japan, and blend it with U.S. weapons-grade plutonium before disposing of the mixture at the WIPP site.

Q: How will Russia's decision to suspend the PMDA affect its relations with the United States?

Russia's decision will have less of an impact than the other disputes that are causing friction between the United States and Russia. The half-life of plutonium-239 is more than 24,000 years, which should allow sufficient time for relations between the United States and Russia to improve. Both countries likely will proceed with plutonium disposition, anyway. The difference will be that there will be no verification regime. Regardless, the United States, as a good-will gesture, should invite both Russia and the International Atomic Energy Agency to observe its plutonium disposition activities. The United States can and should provide sufficient information to convince Russian experts that dilute-and-dispose is an acceptable approach.

Radiation alert: Discovery of uranium rock in Austrian school triggers evacuation

Source: https://www.rt.com/news/364029-austria-uranium-radioactive-rock/



Oct 25 – **A science class meeting with an anti-nuclear activist at an Austrian school ended in an evacuation, after a radioactive uranium rock was found on display in the classroom.** The incident led to a city-wide check which found at least 11 other schools had radioactive rocks.

The discovery was made as anti-nuclear campaigner Thomas Neff was giving a lecture at the Missionaries of the Sacred Heart School in Salzburg, the fourth-largest city in Austria, local media reported earlier in October.

Neff brought along a wristwatch from the 1960s with dials covered with a substance containing radium-226, which makes the numerals glow in the dark. He was planning to use the timepiece as an example of the dangers of radiation, of which little was known half a century ago.

"I brought the old watch from the 60s which lights up brightly at night because of the radiation," Neff said, as cited by Austrian media. He added that the watch was carefully sealed and didn't emit any radiation.

Even before Neff had got the watch out, however, his Geiger counter began to show that there was a source of radiation in the room. It displayed 1,200 counts per minute, some 20-25 times higher than the normal value.

Neff inspected the room to find the source of the radiation, and as he was walking past a collection of rocks, the Geiger counter jumped to over 102,000 counts per minute.

The classroom was immediately evacuated, with experts later discovering that one of the rocks on display was in fact a lump of uranium.

"If you had this rock the whole year in your bag, you would get around 210 millisievert exposure. The exposure to radiation from natural sources is only 2.8 millisievert in a whole year in Austria," Neff said.

The discovery triggered mass checks across schools in Salzburg. The Radiological Laboratory of Salzburg (RMLS) soon released a report, saying that it had inspected at least 336 schools in the Salzburg region and that in 73 of them the inspection had discovered a collection of rocks. Radioactive rocks were found in 11 of these schools. All in all, 38 pieces of uranium rocks were found during the 'anti-nuclear' checks.

In the meantime, a radiological laboratory in Austria said that schools were ignoring the dangers of radiation. *"The radioactive screening and the risk assessment show a basic risk potential in Salzburg schools in case of improper storage,"* Central European News cited the laboratory statement as saying, as reported by the Local.

Leak at nuclear reactor in Norway is contained

Source: http://www.reuters.com/article/us-norway-accident-nuclear-idUSKCN12P13Y

Oct 25 – **A leak at a small nuclear reactor in Norway has been contained, with no injuries sustained and no expected environmental damage outside the facility**, the reactor's operator and the country's Radiation Protection Authority (NRPA) said on Tuesday.

The leak at the research reactor operated by the Institute for Energy Technology, **located in a mountain cave in the middle of Halden** in southern Norway, began on Monday at 7.45 a.m. ET but the regulator said it was not alerted until Tuesday.

The crew of the reactor was evacuated after the leak was detected but some staff later returned to assess the cause and extent of the accident, the NRPA said. Its operator said the reactor was isolated and the leak contained.

"We will investigate how this (leak) could happen and why we were not warned until the following day," the regulator said in a statement.

A senior official at the regulator told Reuters the incident would "maybe" be rated a 1 on an International Nuclear Event Scale ranking from 1 to 7, where 1 is an anomaly and 7 is a major accident, such as Chernobyl or Fukushima.

"We need to gather more information ... But we are not happy with the situation, that we were not warned immediately. We will investigate further," Per Strand, the head of safety, preparedness and environment at the NRPA, told Reuters.

The reactor's operator said the leak had been contained and there had been no injuries. "The reactor is shut. The leak is contained," Atle Valseth, research director at the Institute for Energy Technology told Reuters.

He did not know how many staff were present when the leak occurred but said up to eight persons are allowed during this type of operation.

"There is no danger to health. The radioactive dosage they have received is low," he said, adding the crew had not received hospital treatment.

Close to Sweden

The reactor is close to the border with Sweden but the Swedish Radiation Safety Authority says it had not detected any radiation as result of the incident and did not expect to do so based on the low levels of radiation in Halden.

The reactor was built in the late 1950s in a mountain cave in Halden, some 120 km south of Oslo. Norway does not have nuclear power stations but operates two small research reactors that study nuclear safety issues. The Halden reactor can produce up to 25 megawatts, a fraction of what nuclear reactors in neighboring Sweden can produce. Mark Foreman, a nuclear expert at the Chalmers University of Technology in Sweden, said iodine was mainly a by-product of nuclear fission in the reactor. "Almost all the iodine is trapped inside the fuel, in a ceramic material. That is inside a metal tube that is welded shut. That is then inside the reactor - it would then have to leak out of the reactor to enter the reactor hall," he said. There were also small amounts of iodine from other sources, such as in water used to cool the reactor, he said.

New Hand Held Radiation Detector for First Responders

Source: http://www.hstoday.us/single-article/new-hand-held-radiation-detector-for-first-responders/f461fb584fe2631b0aae6388b6f42ef3.html

Security professionals seeking reliable radiation detection and identification for remote locations can now use a pocket-size search-and-find detector that is designed for high-sensitivity and accuracy. Because the new detector combines gamma and neutron detection, first responders and strike teams can now quickly locate a wide range of radioactive materials with a single device.

The Thermo Scientific RadEye SPRD-GN (spectroscopic personal radiation detector – gamma neutron) builds upon the family of RadEye personal radiation detectors. It is designed for use in both dynamic monitoring and isolated settings, including rural borders, on boats and on foot, that are not conducive to larger, fixed detection systems. The RadEye SPRD-GN incorporates a highly sensitive, dual sensing gamma and neutron detector. The advanced natural background rejection (NBR) technology continuously analyzes the radiation field and easily differentiates between artificial or natural radiation.

The RadEye SPRD-GN is the first handheld PRD to incorporate pulse shape discrimination (PSD), which separates real neutrons from high energy particles in the background. PSD allows the RadEye SPRD-GN to meet the strict ANSI N42.32-2006 standard for time to alarm, alarming within two seconds. Additionally, it is the first radiation detector to integrate a spectroscopic-capable CLYC (cesium lithium yttrium chloride) crystal. This technology allows for more reliable detection by measuring both neutron pulse height and shape.

"We designed our newest handheld radiation detector with ease of use in mind, so that chemical, biological, radiological and nuclear defense specialists, border inspectors and other first responders can minimize the size and number of tools required in the field," said Scott Masiella, portables and applications product manager, radiation measurement and security instruments, for Thermo Fisher Scientific. "The RadEye SPRD-GN complements our existing line of dependable personal detectors. It is a compact device designed for rugged environments to ensure that security professionals and the public remain safe from radiological threats."

In addition to introducing the RadEye SPRD-GN, new features have also been added to the existing Thermo Scientific RadEye SPRD. The RadEye SPRD, designed for mass deployment by police officers and other first responders in large events, now includes:

- An intuitive on-screen interface that guides users toward fast, accurate results;
- An automatic identification mode designed to provide the isotope and class of artificial radiation within seconds of an alarm; and
- Intuitive, audible tones and vibration patterns that deliver the radiation location and type without the need to view the display.

Immobilizing radioactive waste in glass for millions of years

Source: http://www.homelandsecuritynewswire.com/dr20161104-immobilizing-radioactive-waste-in-glass-for-millions-of-years

Nov 04 – **How do you handle nuclear waste that will be radioactive for millions of years, keeping it from harming people and the environment?**

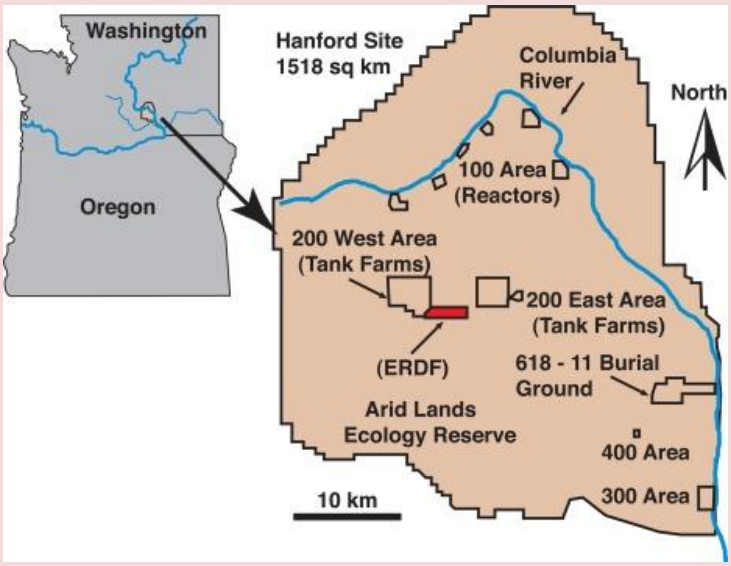
It is not easy, but Rutgers researcher Ashutosh Goel has discovered ways to immobilize such waste – the offshoot of decades of nuclear weapons production – in glass and ceramics.

Rutgers says that Goel, an assistant professor in the Department of Materials Science and Engineering, is the primary inventor of a new method to immobilize radioactive iodine in ceramics at room temperature. He is also the principal investigator (PI) or co-PI for six glass-related research projects totaling $6.34 million in federal and private funding, with $3.335 million going to Rutgers.

"Glass is a perfect material for immobilizing the radioactive wastes with excellent chemical durability," said Goel, who works in the School of Engineering. Developing ways to **immobilize iodine-129, which is especially troublesome**, is crucial for its safe storage and disposal in underground geological formations.

The half-life of iodine-129 is 15.7 million years, and it can disperse rapidly in air and water, according to the U.S. Environmental Protection Agency. If it is released into the environment, iodine will linger for millions of years. Iodine targets the thyroid gland and can increase the chances of getting cancer.

Among Goel's major funders is the U.S. Department of Energy (DOE), which oversees one of the world's largest nuclear cleanups following forty-five years of producing nuclear weapons. The national weapons complex once had sixteen major facilities that covered vast swaths of Idaho, Nevada, South Carolina, Tennessee, and Washington state, according to the DOE.



The agency says the Hanford site in southeastern Washington, which manufactured more than twenty million pieces of uranium metal fuel for nine nuclear reactors near the Columbia River, is its biggest cleanup challenge.

Hanford plants processed 110,000 tons of fuel from the reactors. Some 56 million gallons of radioactive waste – enough to fill more than 1 million bathtubs – went to 177 large underground tanks. As many as 67 tanks – more than one third – are thought to have leaked, the DOE says. The liquids have been pumped out of the 67 tanks, leaving mostly dried solids.

The Hanford cleanup mission commenced in 1989, and construction of a waste treatment plant for the liquid radioactive waste in tanks was launched a decade later and is more than three-fifths finished.

"What we're talking about here is highly complex, multicomponent radioactive waste which contains almost everything in the periodic table," Goel said. "What we're focusing on is underground and has to be immobilized."

Goel, a native of Punjab state in northern India, earned a doctorate in glasses and glass-ceramics from the University of Aveiro in Portugal in 2009 and was a postdoctoral researcher there. He worked as a "glass scientist" at the Pacific Northwest National Laboratory in 2011 and 2012, and then as a senior scientist at Sterlite Technologies Ltd. in India before joining the Rutgers faculty in January 2014.

The six projects he is leading or co-leading are funded by the DOE Office of River Protection, National Science Foundation and Corning Inc., with collaborators from Washington State University, University of North Texas and Pacific Northwest National Laboratory.

Rutgers notes that one of his inventions involves mass producing chemically durable apatite minerals, or glasses, to immobilize iodine without using high temperatures. A second innovation deploys synthesizing apatite minerals from silver iodide particles. He's also studying how to

immobilize sodium and alumina in high-level radioactive waste in borosilicate glasses that resist crystallization.

At the Hanford site, creating glass with radioactive waste is expected to start in around 2022 or 2023, Goel said, and "the implications of our research will be much more visible by that time."

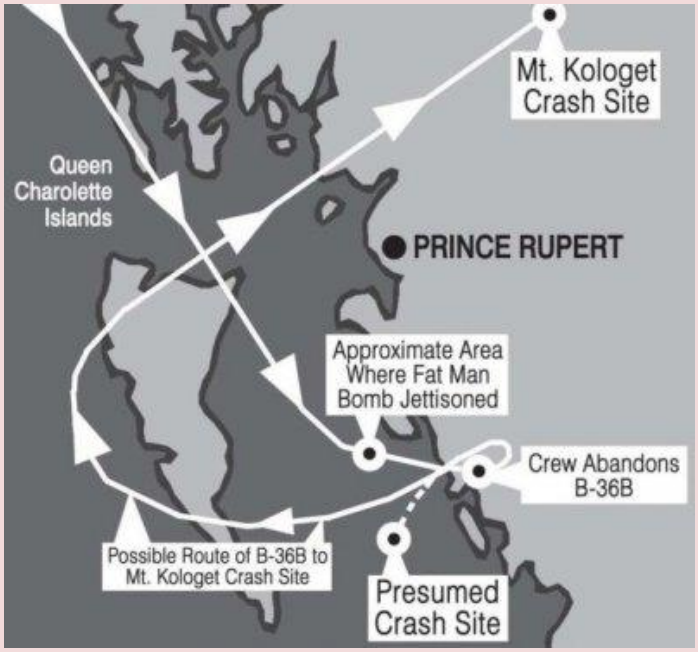
The research may eventually help lead to ways to safely dispose of highly radioactive spent nuclear fuel that is stored now at commercial nuclear power plants.

"It depends on its composition, how complex it is and what it contains," Goel said. "If we know the chemical composition of the nuclear waste coming out from those plants, we can definitely work on it."

Canada to investigate object that could be a nuke lost in 1950

Source: http://www.homelandsecuritynewswire.com/dr20161107-canada-to-investigate-object-that-could-be-a-nuke-lost-in-1950

Nov 07 – **The Royal Canadian Navy is to investigate an object found by a diver off the coast of Queen Charolette Islands, suspecting it could be a "lost nuke" which was lost off the coast of Canada since 1950.**



The BBC reports that Sean Smyrichinsky discovered it while fishing near Haida Gwaii, British Columbia. Experts say it could be a **dummy nuclear bomb – likely still loaded with TNT –** lost after the crew of a training flight encountered mechanical problems and ditched the bomb into the sea before crashing.

"I found something that I'd never ever seen before," Smyrichinsky told the CBC. "It resembled, like, a bagel cut in half, and then around the bagel these balls all cut into it, molded into it… It was the strangest thing that I had ever seen."

Smyrichinsky sketched what he saw on a napkin, and initially thought it could have been a UFO. When he mentioned it to an old fisherman from the area, that fisherman said it could be a bomb that went missing more than five decades ago.

The BBC says that on 13 February 1950, three of the engines of a U.S. Air Force B-36 bomber aircraft caught fire while flying from Alaska to Texas. The plane was on a training mission, planning to carry out a simulated nuclear attack on San Francisco.

Its payload was a Mark IV nuclear bomb, weighing nearly five tons. It had a lead core instead of plutonium, and was thus

unable to cause a nuclear explosion, but it was still a real device loaded with explosives.
The co-pilot of the flight explained in a 1998 interview why this was done: "Without a real bomb the support systems could not be tested. There were some dummy bombs made of concrete that were used for load testing, but we weren't carrying one of those.
"This mission was to be as real as it gets short of war…The large amount of TNT in the bomb could have caused major damage where it would have impacted."
The crew decided to drop the bomb into the Pacific Ocean before bailing out because they were unsure of how close they were to populated areas.
When Smyrichinsky returned home, he researched the story of the downed B-36 and nuclear weapons of the time. He saw one photo of the Fat Man bomb, which looks a bit like a blimp, in several pieces before being assembled.
"It was a piece that looked very much like what I saw," he told CBC. "The plane that was carrying the bomb, it crashed fifty miles south of where I found that object."
Smyrichinsky contacted the Canadian Department of National Defense, which said the discovery had their "collective attention." Defense officials said the department would be dispatching a ship carrying a team of nuclear weapons specialists to the area in November.

US floating SBX radar spent month spying on N.Korea nukes – reports

Source: https://www.rt.com/news/364991-radar-us-north-korea/

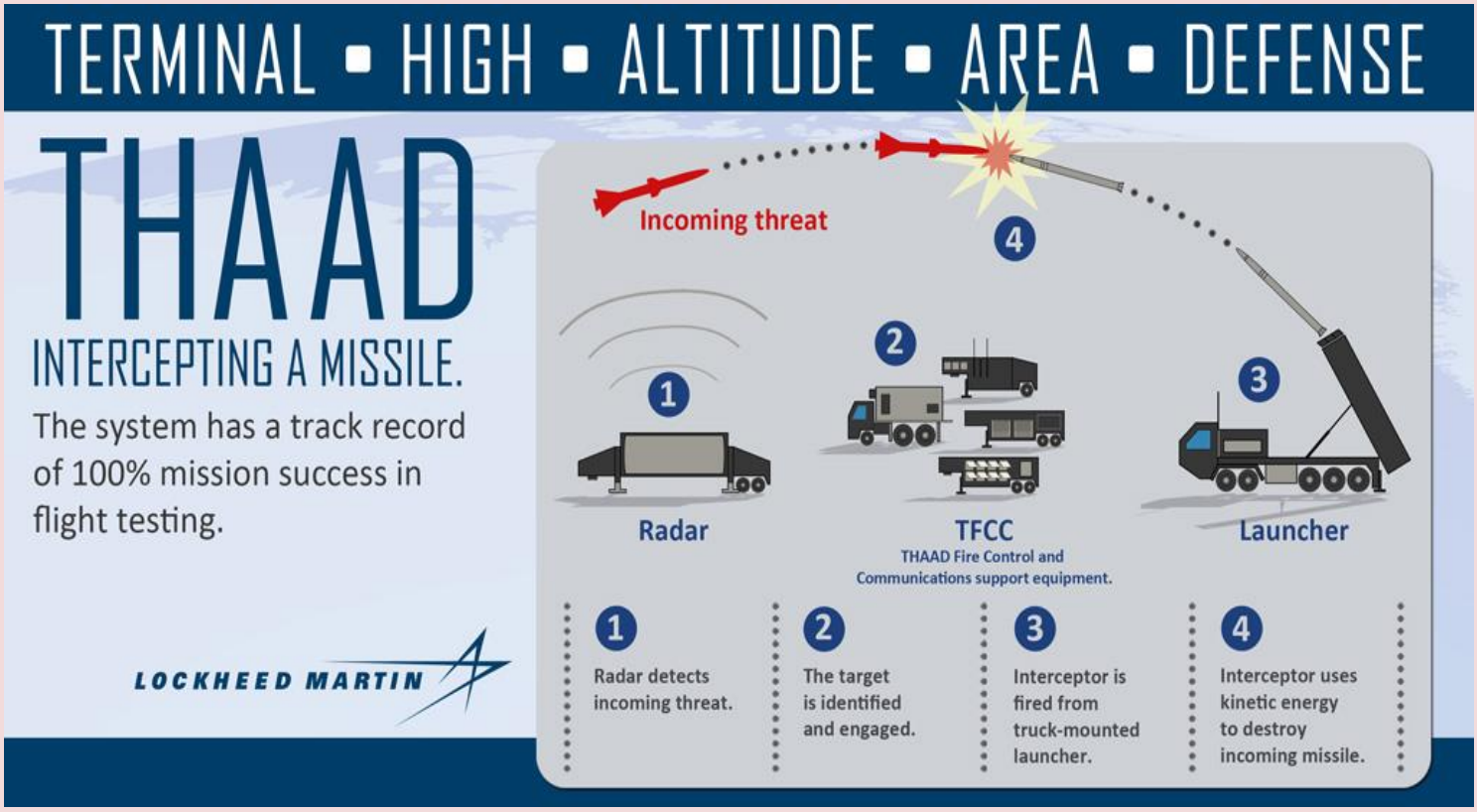
Nov 01 – **"The US sea-based X-Band (SBX) radar was sent to an undisclosed location off the Korean Peninsula for a one-month deployment after departing Hawaii in late September. It sailed back to its home port in late October,"** a South Korean military official told Yonhap news agency on Tuesday.

He did not provide details about the mission and the radar's route, nor did he specify the purpose of the deployment, citing security reasons, Yonhap noted.
According to South Korean broadcaster KBS, citing military and government sources, the radar was dispatched to the waters near the Korean Peninsula to monitor possible long-range ballistic missile launches by North Korea.
So far, the US government has not officially confirmed the radar deployment, although several media outlets reported that SBX did in fact leave its home port in Hawaii at the end of September, citing local residents who witnessed its departure.
The SBX is a floating, mobile, active early-warning radar station. It has a 116 meter by 85 meter radar system installed on its deck, which is capable of detecting a missile fired

upwards from a range of up to 2,000 kilometers. Its aim is detecting and tracking long-range ballistic missiles and rockets, as well as determining their properties to help defend against them. The radar is said to be so accurate it could detect a baseball over San Francisco from the other side of the continent. The project has cost the US Pentagon some $10 billion, but according to media reports, it reportedly proved less effective than expected.

Tensions on the Korean peninsula have been running high since the beginning of 2016, as North Korea has started conducting nuclear and ballistic missile tests in violation of UN resolutions.

The situation has worsened since Washington's recent decision to deploy sophisticated nuclear-capable bombers at its base on Guam in the western Pacific, and the announcement of the deployment of **THAAD missile systems** in South Korea.



The US and South Korea insist that THAAD will keep North Korean nuclear ambitions at bay, disregarding Russian and Chinese concerns over security in the region. The two states repeatedly condemned Pyongyang for threatening the security of the region through its policies, but also criticized Washington for interfering.

Chinese Defense Minister Chang Wanguan said in early October that *"some countries seek absolute military superiority, ceaselessly strengthen their military alliances, and seek their own absolute security at the costs of other countries' security."*

The US has recently been actively displaying its military presence in the Korean peninsula. Just this week, US ballistic-missile submarine 'USS Pennsylvania' has arrived in Guam. Last month, the US deployed a 3,500-strong armored brigade to South Korea for a nine-month *"rotational deployment."*

Pyongyang repeatedly warned it is ready to battle the US *"with nuclear hammers of justice"* and that the North has all the resources necessary to battle US *"nuclear hegemony."*

No money, no iodine pills for all Belgians

Source:http://www.hln.be/hln/nl/6756/Kernenergie/article/detail/2957649/2016/11/03/Geen-geld-dus-geen-jodiumpillen-voor-alle-Belgen.dhtml (in Dutch)

Bathroom air freshener triggers emergency response at nuclear weapons complex

Source: http://www.homelandsecuritynewswire.com/dr20161111-bathroom-air-freshener-triggers-emergency-response-at-nuclear-weapons-complex

Nov 11 – An air freshener caused quite a scare last week at the Savannah River Site (SRS).
Late in the afternoon on Wednesday of last week officials at the nuclear weapons complex declared an emergency after finding what they regarded as a suspicious device in a bathroom at the Savannah River National Laboratory, a research area at SRS. Emergency teams treated the item as potentially explosive.

The *Miami Herald* reports that the emergency teams determined that the item was an air freshener wrapped in paper towels with a flashing light on it. Site spokesman Jim Giusti said the facility quickly declared the item "non-threatening'' and returned operations to normal.

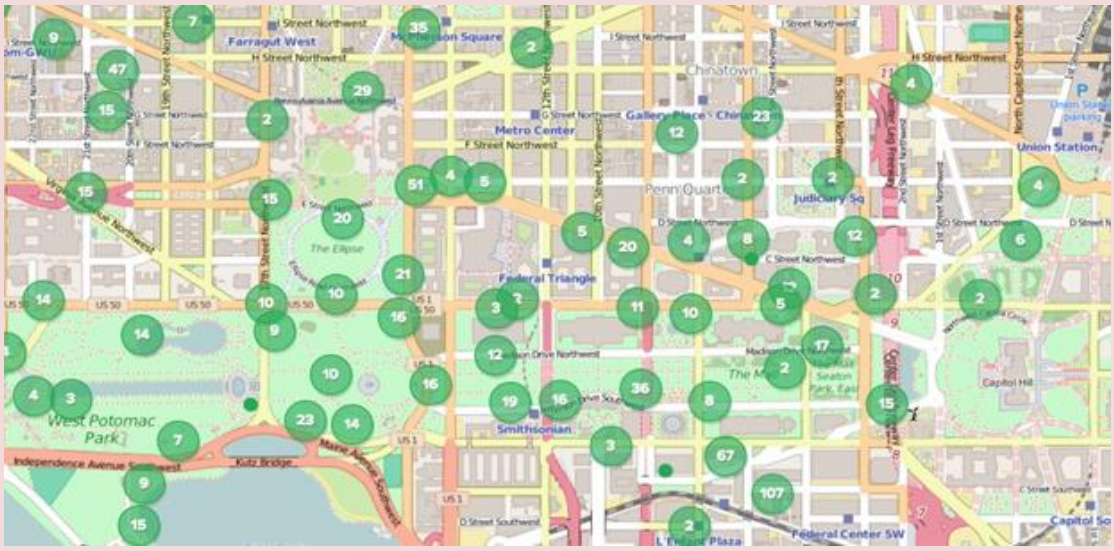
Giusti, who is with the U.S. Department of Energy, said SRS is trying to determine why the air freshener was displayed that way.
"People reported a suspicious object and we responded based on all our training,'' Giusti said. "It is a standard type of air freshener we use in the building. We don't know why it was wrapped in paper towels. That's going to be an ongoing issue for us to evaluate tomorrow when we talk to people.''
The Savannah River Site is a heavily guarded atomic weapons complex near Aiken in western South Carolina. The 310-square miles site contains large amounts of nuclear material. Much of the site is now undergoing post-Cold War cleanup.
"The All-Clear has been given at SRS,'' a 5:40 p.m. agency news release said. "A suspicious item was discovered at the Savannah River National Laboratory which prompted the emergency response activities. After thorough investigation, the suspicious item was determined to be non-threatening and the site has been returned to normal operations.''

First large-scale, citywide test of advanced radioactive threat detection system

Source: http://www.homelandsecuritynewswire.com/dr20161111-first-largescale-citywide-test-of-advanced-radioactive-threat-detection-system

Nov 11 – On a recent sunny fall day in the nation's capital, several hundred volunteers — each toting a backpack containing smartphone-sized radiation detectors — walked for hours around the National Mall searching for clues in a "whodunit" scavenger hunt to locate a geneticist who had been mysteriously abducted. The geneticist and his abduction were fictitious. But the challenge this scavenger hunt was designed to address is real: The need to detect even small quantities of radioactive material that terrorists might try to bring into an urban area with the intent of detonating a "dirty bomb," or worse. By getting volunteers to walk all day looking for clues, the DARPA-sponsored exercise provided the largest test yet of **DARPA's SIGMA program**, which is developing networked sensors that can provide dynamic, real-time radiation detection over large urban areas.
DARPA says that akey element of SIGMA, which began in 2014, has been to develop and test low-cost, high-efficiency, radiation sensors that detect gamma and neutron radiation. The detectors, which do not themselves emit radiation, are networked via smartphones to provide

city, state, and federal officials real-time awareness of potential nuclear and radiological threats such as dirty bombs, which combine conventional explosives and radioactive material to increase their disruptive potential. Following a demonstration earlier this year with the Port Authority of New York and New Jersey involving more than 100 SIGMA sensors, the 1,000-detector deployment in Washington, D.C. marked the largest number of SIGMA mobile detectors ever tested at one time and was a demonstration of the program's ability to fuse the data provided by all those sensors to create minute-to-minute situational awareness of nuclear threats.



A map of the National Mall in Washington, D.C., shows the location of the SIGMA mobile radiation detectors as deployment participants moved around the city. DARPA's SIGMA program is developing networked sensors that can provide dynamic, real-time radiation detection over large urban areas.

"The SIGMA system performed very well, and we collected and analyzed a huge amount of streaming data as we watched in real-time as participants covered a large portion of D.C.," said Vincent Tang, DARPA program manager. "The data collected is already proving invaluable for further development of the system, and we're excited that SIGMA is on track to provide U.S. cities an enhanced layer of defense against radiological and nuclear threats."

Orchestrating a large event involving hundreds of people in the heart of the Capital required months of planning and coordination with multiple D.C. and federal agencies, as well as soliciting and registering volunteer participants. The University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) — a performer on the SIGMA program — was a prime player in successfully staging the day-long deployment. START recruited several hundred ROTC cadets from universities in the National Capital Region and midshipmen from the U.S. Naval Academy to participate in the event. A number of DARPA and other government personnel volunteered as well.

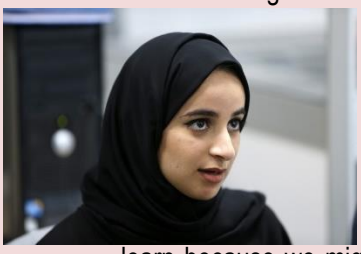
To get volunteer participants to move widely around the downtown area with their detector-packed backpacks, the START team developed an intriguing spy-thriller scavenger hunt scenario that required participants to collect clues and perhaps ultimately solve the mystery of what had become of a scientist who had been dramatically abducted by masked men. That allowed the SIGMA research team to evaluate how well the devices functioned as mobile nodes on a network that stretched to about five square miles. A number of SIGMA performers — Invincea Labs with 3Pillar Global, Eucleo, and Berkeley Applied Analytics; Kromek Group plc; TRX Systems Inc; Physical Sciences Inc. with Lawrence Berkeley National Laboratory; and Lawrence Livermore National Laboratory — played key roles in ensuring the event's success. That included everything from preparing the detectors, packaging them into hundreds of backpacks, coordinating the detector tracking and data monitoring, and performing the analyses to help further refine the algorithms that will be integrated into an operational version of the SIGMA software.

Next steps in the SIGMA program include continuing to test full city- and regional-scale, continuous wide-area monitoring capability in 2017 and then transition the operational system to local, state, and federal entities in 2018.

Nuclear empowerment for women

Source 1: http://www.thenational.ae/business/energy/nuclear-empowerment-for-women -meet-four-emirati-trailblazers#3
Source 2: http://www.thenational.ae/uae/uae-portrait-of-a-nation-the-emirati-born-to-work-in-nuclear-energy
Source 3: http://www.thenational.ae/uae/power-of-emirati-women-growing-in-the-uaes-nuclear-industry

May 2016 – We profile some of the women recently hired by the Federal Authority for Nuclear Regulation (Fanr), which is increasing its recruitment of Emirati staff.
Today, 61 per cent of the authority's staff is Emirati compared to 48 per cent six years ago. More than half of them are women. Although 36 of the 80 jobs held by Emiratis in the authority's operations division belong to women, the hope is to increase that number further.



Fatima Al Muhairi: the nuclear industry was initially considered an unconventional choice for women
"My family was scared at first because they wanted to know if it was safe and secure," said the 23-year-old, originally from Abu Dhabi. "They wanted to know if it was OK for a woman to work here. But I explained to them that it was, I am not the only woman here so they accepted it and they support me."
"I think nuclear energy is the future, it's interesting and something we have to learn because we might depend on it in the future," the mechanical engineer from Khalifa University, said.

Amal Bin Lootah: national importance of the nuclear sector means more Emiratis are needed

"I went to South Korea as part of a youth ambassador programme which made me interested in the nuclear industry," the 23-year-old civil engineer from Dubai, said.
"When you study it, you realise that nuclear is safe and you get more radiation when you travel on a plane. But people get scared."

Huda Al Tamimi: every Emirati has a role to play
"We are here to serve our country," said the 23-year-old mechanical engineer from Ras Al Khaimah.
"I got the chance so why not? Fanr has the vision that I am looking for, which is protecting the environment and people from radioactive material and the threat from any nuclear misuse. We're still not operating but I'm very excited to be a part of it because it's my role to clear up the messed up ideas about nuclear to the public."

Amal Al Saleem: the most challenging part is the responsibility

"My goal was always to find a place for myself to be a part of the UAE's development," said the 24-year-old mechanical engineer from Abu Dhabi who interned at Airbus in Toulouse, France.
"I don't want to be useless to the country and the nuclear industry will definitely be needing national engineers, which is what motivated me to join Fanr and the nuclear field."

Salama Al Ketbi is the senior project engineer the power plant site in Barakah in the Western Region.

Al Blooshi: As both of Hasna Al Blooshi's parents were in the energy industry it was perhaps natural that she, too, should eventually work in the field.
"My father served at the Abu Dhabi Company for Onshore Petroleum (Adco) for 40 years and my mother for 27 years," she says."So, I grew up in a house where we talked about science, technology and new projects that Adco was going through. We were so familiar with the industry because my parents were so involved in it," says Ms Al Blooshi, 36.
After acquiring a higher diploma in health information management at the Higher Colleges of Technology, Ms Al Blooshi went on to work at the Abu Dhabi National Oil Company while studying for a bachelor's degree in health information management in the evenings.

She worked for Adnoc's medical services for almost six years, then moved to the Health Authority Abu Dhabi's regulatory sector for another six.
When the UAE launched its nuclear programme she was keen to become involved as the director for nuclear performance improvement at the Nawah Energy Company.
The number of Emiratis working in nuclear-related projects has increased by more than 100 in the past year and more than 700 since 2010. More than 2,700 work in the nuclear sector.
Mr Alkaabi attributed the increase to greater interest across the country.
"Our objective is to increase knowledge and awareness."
In a first, the IAEA's International Conference on Nuclear Power, which takes place every four years, is to be held in Abu Dhabi next year.
"It provides a platform for government officials and policymakers to discuss trends, outlook and contribution of nuclear power globally," Mr Alkaabi said.
"Choosing the UAE to host such a conference is a high recognition of the country's efforts and contribution to the responsible development of nuclear power globally. It also demonstrates the confidence of the IAEA member states in UAE capabilities to conduct such a high level conference successfully. It is timely for the UAE as we are progressing very well."

Erdogan: We can purchase 3-5 Nuclear warheads from Pakistan

Source 1: http://www.f-16.net/forum/viewtopic.php?f=37&t=52504
Source 2: http://www.haberandum.com/gundem/pakist ... h4704.html

AYNI ZAMANDA CUMHURBAŞKANI RECEP TAYYIP ERDOĞAN YAPTIĞI AÇIKLAMADA, "PAKISTAN'DAN NÜKLEER SILAH ALABILIRIZ. 3-5 TANE YETER" ŞEKLINDE KONUŞTU.

Nov 18 – Turkish media is going crazy over a very public statement made by the Turkish President yesterday during a visit to Pakistan.
Erdogan stated as follows: "We can purchase 3 to 5 nuclear weapons (high yield) from Pakistan and this will be enough".
If this is true and Turkey does in fact purchase 3 to 5 high yield nuclear warheads from Pakistan, how will this change the geopolitical scene? Besides economic sanctions and the embargo on any F-35 sale to Turkey. In fact, the EU is already discussing sanctions but what other geopolitical ramifications could this have?
Ankara's response to the EU threat about economic sanctions was: "go shove your EU membership" and "hurry up and cancel our EU candidacy. You are far too late". So it begs me to ask what is Turkey's plan? Shanghai Cooperation Organisation?

Pakistan's Evolving Nuclear Weapons Infrastructure

By Hans M. Kristensen
Source: https://fas.org/blogs/security/2016/11/pakistan-nuclear-infrastructure/

Pakistan's tactical NASR nuclear-capable mobile rocket launcher now appears to be deployed.

Nov 16 – In our latest Nuclear Notebook on Pakistani nuclear forces, Robert Norris and I estimate that Pakistan has produced an estimated stockpile of 130-140 nuclear warheads for delivery by short- and medium-range ballistic missiles, cruise missiles, and fighter-bombers.

Pakistan now identifies with what is described as a full-spectrum nuclear deterrent posture, which is though to include strategic missiles and fighter-bombers for so-called retaliatory strikes in response to nuclear attacks, and short-range missiles for sub-strategic use in response to conventional attacks.

Although there have been many rumors over the years, the location of the nuclear-capable launchers has largely evaded the public eye for much of Pakistan's 19-year old declared nuclear weapons history. Most public analysis has focused on the nuclear industry (see here for a useful recent study). But over the past several years, commercial satellite pictures have gradually brought into light several facilities that might form part of Pakistan's evolving nuclear weapons launcher posture.

This includes 10 facilities, including 5 missile garrisons (soon possibly 6) as well 2 (possibly 4) air bases with fighter-bombers.

Pakistan's nuclear weapons related infrastructure includes at least 10 major industrial facilities and about 10 bases for nuclear-capable forces. Click map to view full size.

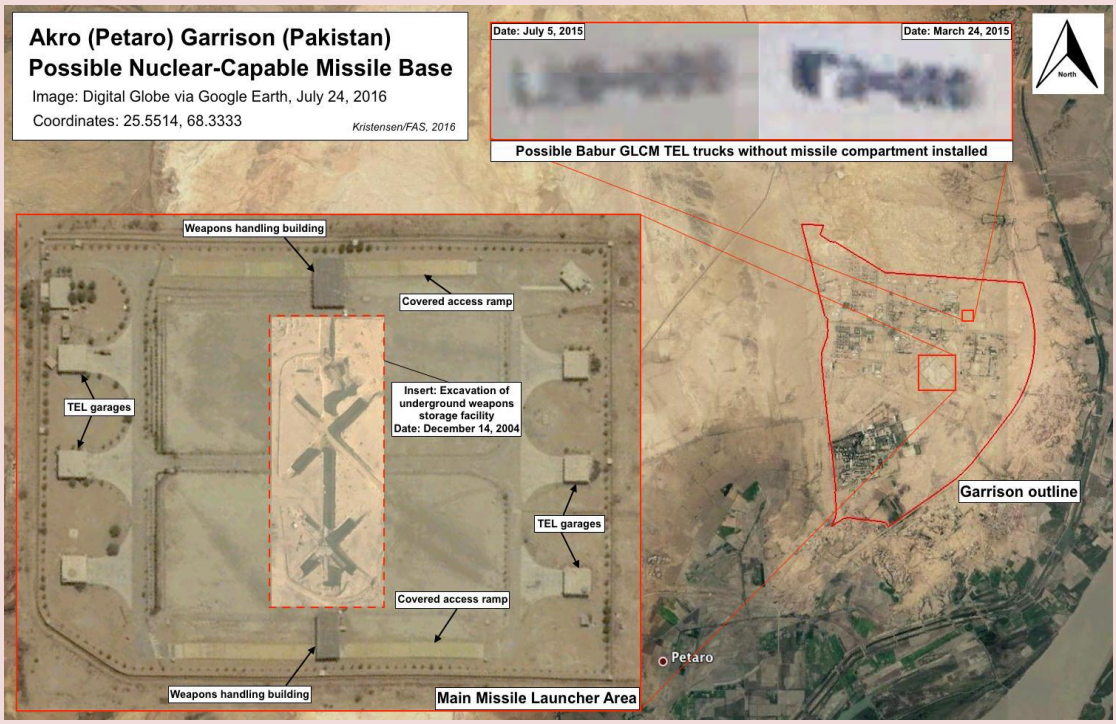
The nuclear warheads that would arm the launchers are thought to be stored at other secure facilities that have not yet been identified. In a crisis, these warheads would first have to be brought to the bases and mated with the launchers before they could be used.

Security at these and other Pakistani defense facilities is a growing concern and many have been upgraded with additional security perimeters during the past 10 years in response to terrorist attacks.
There are still many unknowns and uncertainties about the possible nuclear role of these facilities. All of the launchers are thought to be dual-capable, which means they can deliver both conventional and nuclear warheads. So even if a base has a nuclear role, most of the launchers might be assigned to the conventional mission. Further analysis in the future might disqualify some and identify others. But for now, this profile of potential road-mobile launcher garrisons and air bases are intended as a preliminary guide and accompany the recent FAS Nuclear Notebook on Pakistani nuclear forces.

Nuclear-Capable Road-Mobile Missile Launcher Bases

The total number and location of Pakistan's nuclear-capable missile bases is not known. But analysis of commercial satellite photos has identified features that suggest that at least five bases might serve a role in Pakistan's emerging nuclear posture. This includes army garrisons at Akro (Petaro), Gujranwala, Khuzdar, Pano Aqil, and Sargodha. A sixth base at Bahawalpur (29.2829, 71.7955) may be under construction. There is also a seventh base near Dera Ghazi Khan (29.9117, 70.4922), but the infrastructure is very different and not yet convincing.
An obvious difficulty in identifying nuclear missile bases is that the infrastructure is not yet publicly known, that commercial satellite photos do not have sufficient resolution to positively identify nuclear-capable launchers with certainty (especially smaller shorter-range types), that all launchers are dual-capable (not all bases with a certain launcher may have a nuclear role; and not all nuclear-capable launchers at a particular base may be assigned nuclear warheads), and that Pakistan (like other nuclear-armed states) most likely is engaged in considerable efforts to conceal and confuse identification of nuclear launchers.
With these caveats, here is a description with images of what we consider to be the five primary nuclear-capable bases and the primary TEL (Transporter Erector Launcher) production facility in Pakistan:

Akro Garrison: This base is located (25.5483, 68.3343) approximately 18 km (11 miles) north of Hyderabad between Akro and Petaro in the southern part of the Sindh Province approximately 145 kms



(90 miles) from the Indian border. The garrison covers an area of 6.9 square kms (2.7 square miles) and has been expanded significantly since 2004 (the base was first pointed out to me by Martin Bulla, a German amateur satellite imagery enthusiast). The Akro Garrison includes **a unique underground facility** located under what appears to be a missile TEL garage complex. The underground facility consists of two star-shaped sections located along a central corridor that

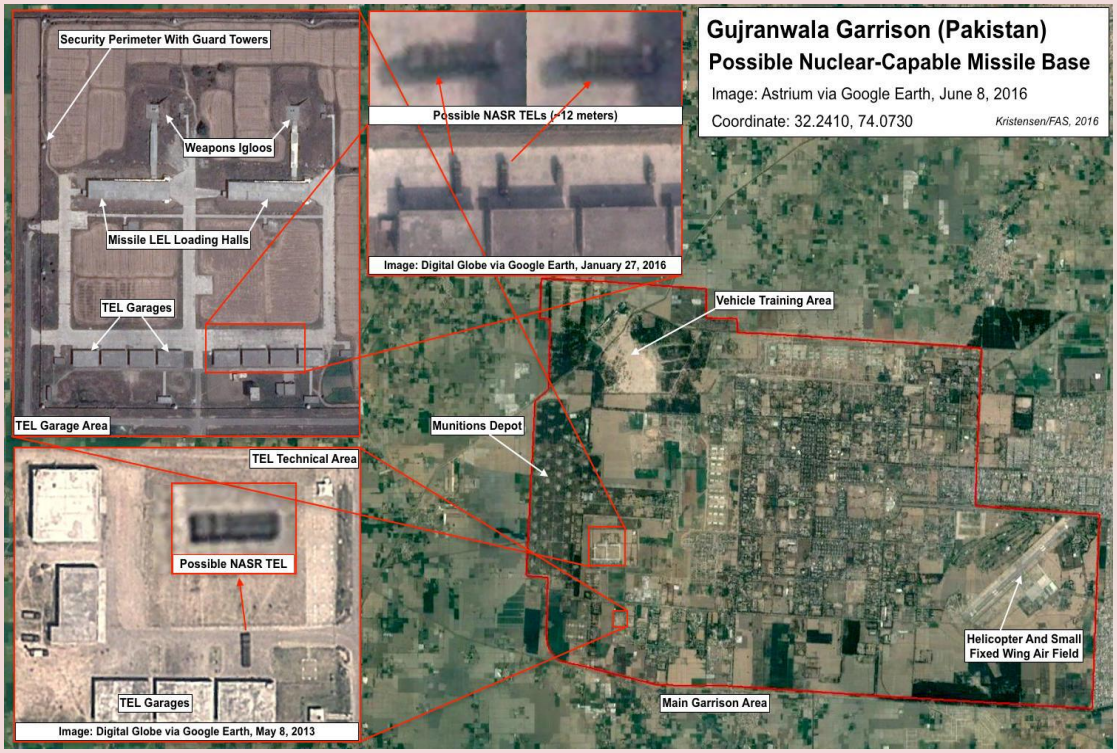
connects to two buildings with covered access ramps. **The six TEL garages appear to be designed for 12 launchers.**

The Akro Garrison has a TEL area with unique underground facility. Click image to view full size.

It is not possible to identify the suspected launchers in the TEL complex from the available photos. But analysis of a vehicle training area in the northeast corner of the garrison shows what appears to be five-axel TELs for the Babur cruise missile weapon system.

In a hypothetical crisis the launchers presumably would load their complement of missiles at the base and disperse outside to predetermined launch locations in the region. The range of the Babur is uncertain; NASIC reports it as 350 km (217 miles) while the Pakistan government claims a range of more than 500 kms (373 miles), sometimes as much as 700 kms (435 miles). The Akro unit would be able to defend all of the southeastern part of Pakistan, including Karachi.

Gujranwala Garrison: This sprawling base complex covers an area of approximately 30 square kms (11.5 square miles) and is located (32.2410, 74.0730) in the northeastern part of the Punjab Province approximately 60 kms (37 miles) from the Indian border. Since 2010, the base has added what appears



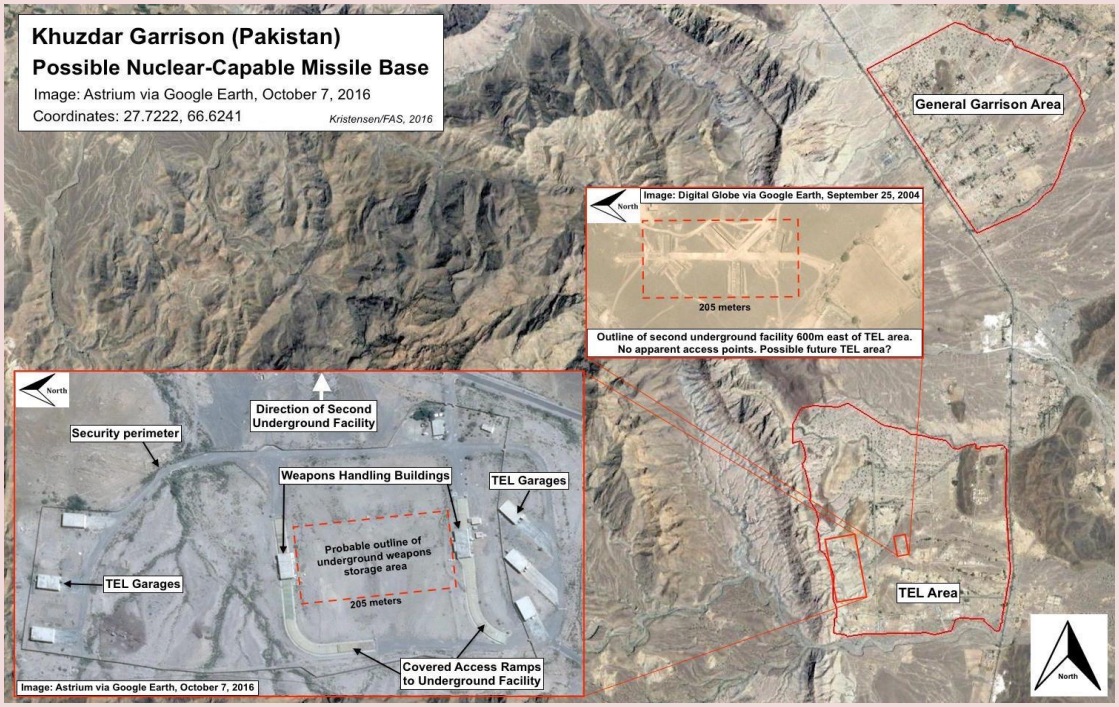
to be a TEL launcher area in the western part of the complex. There is also what appears to be a technical area for servicing the launchers. The TEL area became operational in 2014 or 2015. The TEL area appears to be made up of two identical sections (each consisting of launcher garages, a weapons loading hall, and a weapons storage igloo), each similar in design to the TEL area at Pano Aqil. The security perimeter appears to have room for a third TEL section. (This and other facilities have also been spotted by https://twitter.com/rajfortyseven.)

The Gujranwala Garrison appears to be a base for the NASR tactical nuclear-capable launcher.

Several trucks have been seen on the satellite pictures that strongly resemble the NASR short-range missile launcher. It is impossible to identify the launchers with certainty due to the relatively poor quality of the pictures (the launchers could potentially also be multiple rocket launchers), but the resemblance is strong with a drivers cabin, a power and hydraulics unit, and a twin box launcher seen on NASR test launch photos published by the Pakistan military. The range of the NASR is equal to the base's distance from the Indian border.

Khuzdar Garrison: Of the missile garrisons located so far, the Khuzdar Garrison some 220 kms (136 miles) west of Sukkur in south-east Balochistan Province is the one located (27.7222, 66.6241) the farthest from the Indian border (295 kms or 183 miles). The base is split in two sections: a northern section and a southern section (where the TELs are based).

Possible launchers have not been seen and identified in Khuzdar photos, but the TEL garages are longer than at all the other bases except the Sargodha Garrison. This could **potentially be a base for Shaheen-2 medium-range missile launchers.**

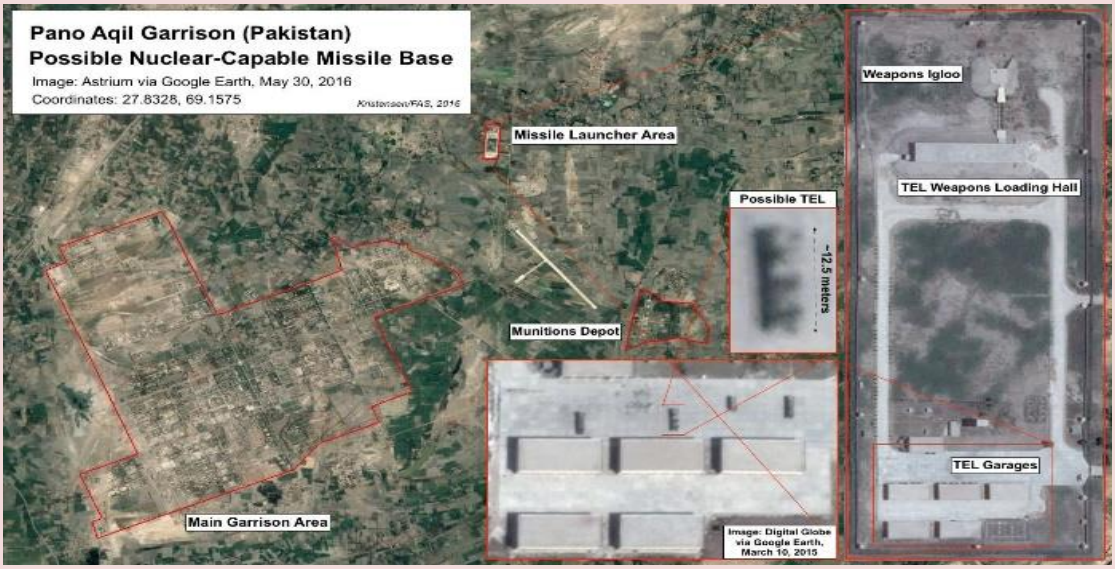


The Khuzdar Garrison might deploy Shaheen-2 launchers.

The TEL area includes what appears to be an underground facility similar to the one identified at the Akro Garrison. It consists of two buildings on covered access ramps that probably provide TEL access to an underground weapons storage and handling facility.

Khuzdar appears to also have a **second underground facility** approximately 600 meters (1,800 feet) east of the TEL area. This facility has roughly the same overall dimensions as the suspected underground facility between the access ramps inside the TEL area, but the second facility has no TEL facilities on top of it and does not appear to have clear access points. One potential possibility is that this facility may be intended for a second TEL area in the future.

Pano Aqil Garrison: The Pano Aqil Garrison is split up in several sections that cover a combined area of nearly 20 square kms (7.7 square miles). This includes the main garrison area, a TEL area (27.8328,



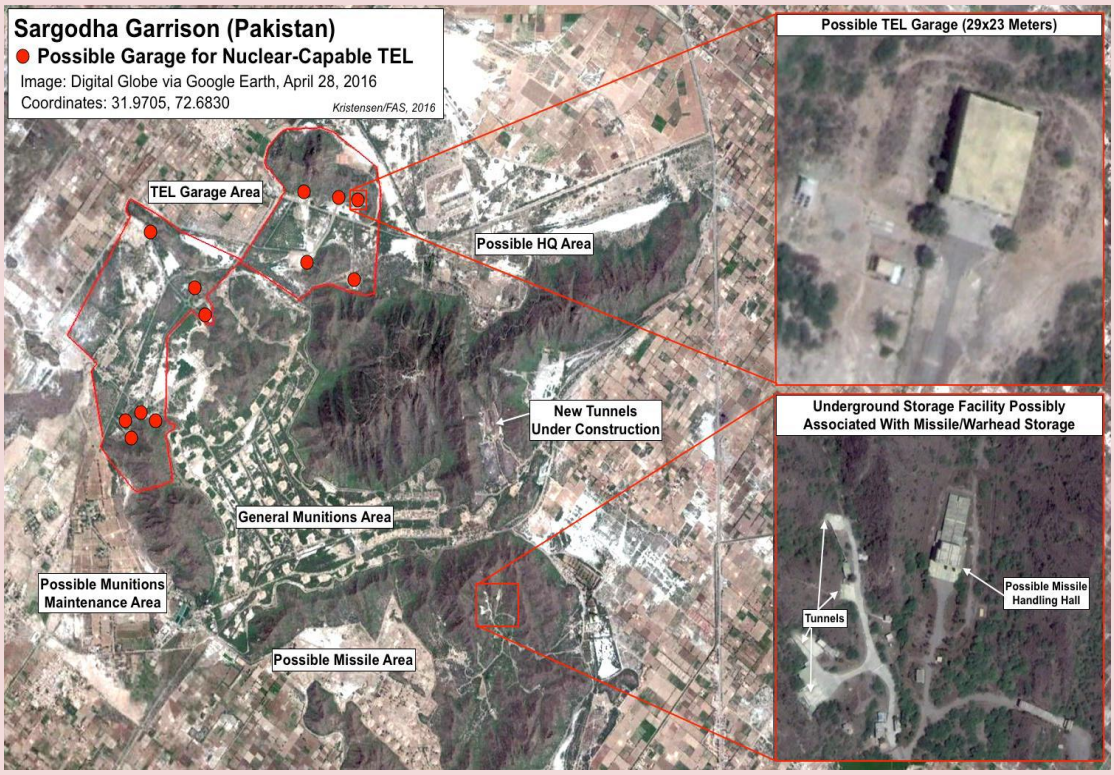
69.1575), a munitions depot, an airfield, and a shooting range. The base is located approximately 80 kms (50 miles) from the Indian border in the northern part of the Sindh Province.

The TEL area is located 1.8 kms (1.2 miles) northeast of the main garrison and includes five TEL garages (a sixth is under construction) and a service building. At the north end of the facility are located a weapons storage igloo and a weapons handling hall. The layout of the TEL area is similar to the Gujranwala Garrison (which appears to have twice the capacity). The five TEL garages can potentially hold 25 TELs although some of the spaces are probably used by support vehicles.

The Pano Aqil Garrison has a remote TEL area.

Identification of TEL type is difficult due to the relatively poor quality of the satellite pictures, but it could **potentially be NASR, Shaheen-1 or Ghaznavi short-range missile launchers.**

Sargodha Garrison: The large munitions storage depot at Sargodha has long been rumored to include TEL garages. The facilities date back to the mid-1990s when Pakistan was first reported to have acquired M-11 missiles from China (DF-11 or CSS-7), which was used to produce what is now known as Pakistan's Ghaznavi and Shaheen-1 short-range ballistic missiles. But the garages (31.9722, 72.6838) at Sargodha are nearly twice the size that would be needed by short-range Ghaznavi and



Shaheen-1 launchers and seem better sized for medium-range Ghauri or Shaheen-2 launchers. There appear to be 10 TEL garages plus two garages with different dimensions that might be used for maintenance.

Yet the Sargodha complex has less of the type of infrastructure seen at other potential TEL bases. Much of the infrastructure seen might be used by personnel that maintain the large weapons depot itself. Whatever the large garages are used for, they are currently being upgraded and additional infrastructure is being added.

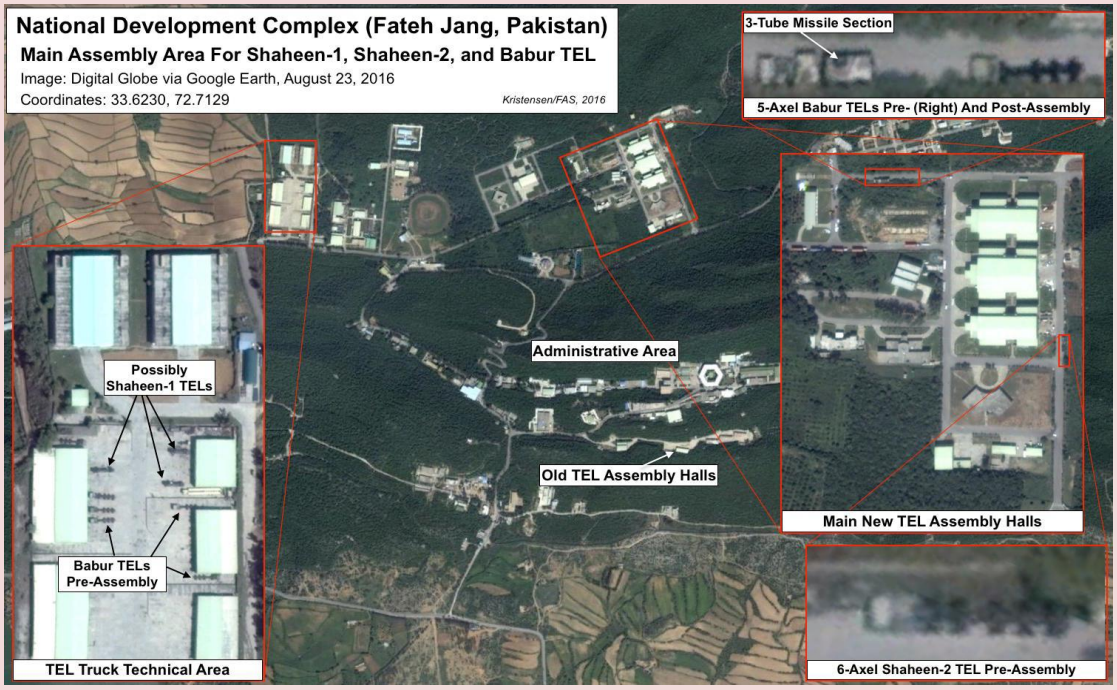
The Sargodha Garrison has large garages and underground facilities.

The Sargodha complex also includes several underground facilities, including a section with two large buildings that could potentially be missile handling halls. Additional tunnels are under construction.

National Development Complex: Several of the TEL types seen or suspected at the different missile garrisons are assembled at the National Development Complex (sometimes called National Defense Complex), or NDC. It consists of a string of facilities scattered across the Kala-Chitta Mountain Range west of Islamabad. But the heart of the complex is the TEL assembly section north of Fateh Jang (33.6292, 72.7106). NDC reportedly emerged in the mid-1990s to produce Gazhnavi and Shaheen-1 short-range ballistic missiles based on technology supplied by China.

Since then NDC has expanded considerably to include facilities west and east of the central TEL assembly area. The central area has expanded considerably since 2003, with the addition of a TEL truck assembly facility as well as three large high-bay TEL assembly halls for

mounting missile compartments onto TEL trucks. **For the past ten years, these facilities have been busy producing Shaheen-2 medium-range ballistic missile launchers and Babur ground-launched cruise missile launchers.**

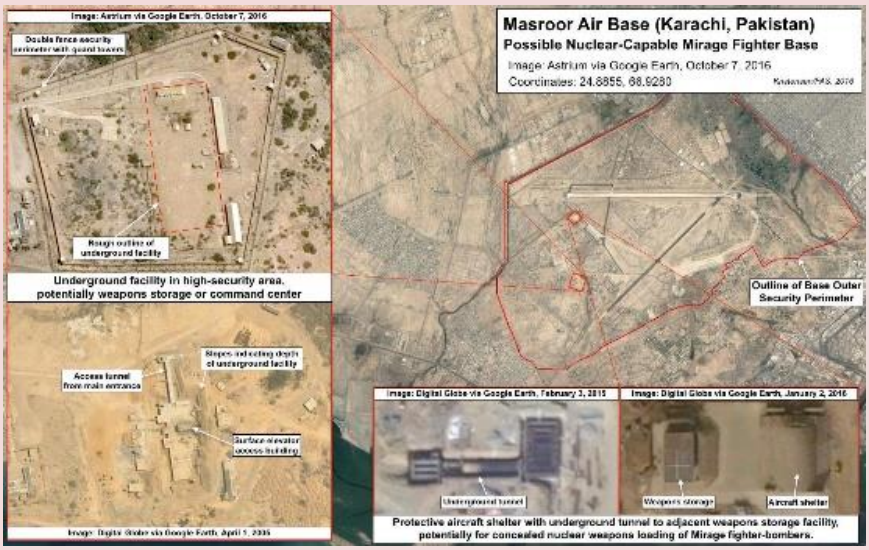


The National Development Complex assembles Shaheen and Babur missile launchers.

Satellite pictures give an example of the flow of production of different TEL types at NDC and also provide valuable reference points for comparing dimensions of TELs seen at individual missile garrisons. Several pictures from 2016, for example, show both 6-axel Shaheen-2 TELs and 5-axel Babur TELs, and possibly also 4-axel Shaheen-1 TELs, in the process of assembly or maintenance. The 8-axel Shaheen-3 TEL has not yet been seen as this weapon system is still very early in production and not yet operationally deployed.

Air Bases

Pakistan has a large number of air bases but only a small number is thought to be involved in the nuclear mission. This includes bases with Mirage and F-16 fighter-bombers. United States officials have stated that F-16s were sold to Pakistan on the conditions that they could not be uses to deliver nuclear weapons, but other sources have indicated that some of the planes were converted nonetheless. French-produced Mirage aircraft are widely assumed to be equipped to deliver the Ra'ad air-launched cruise missile.



Masroor Air Base: This base is located (24.8855, 66.9280) west of the city of Karachi and has long been suspected of serving a role in Pakistan's airborne nuclear deterrent. The base is home to the 32nd Fighter Wing with Mirage fighter-bombers and is located only 5 kms (3 miles) from a potential nuclear weapons storage site (24.9429, 66.9083).

Over the past decade, unique facilities have been construction at Masroor Air Base that might potentially form part of Pakistan's nuclear posture. This includes a large underground facility that is located inside a high-security area. The purpose of the facility has not been confirmed and could potentially also involve

command and control. Yet the facility is clearly unique compared with other Air Bases and might potentially serve as an underground nuclear weapons storage and handling facility. (Update: **the underground facility is possibly a command center**.)

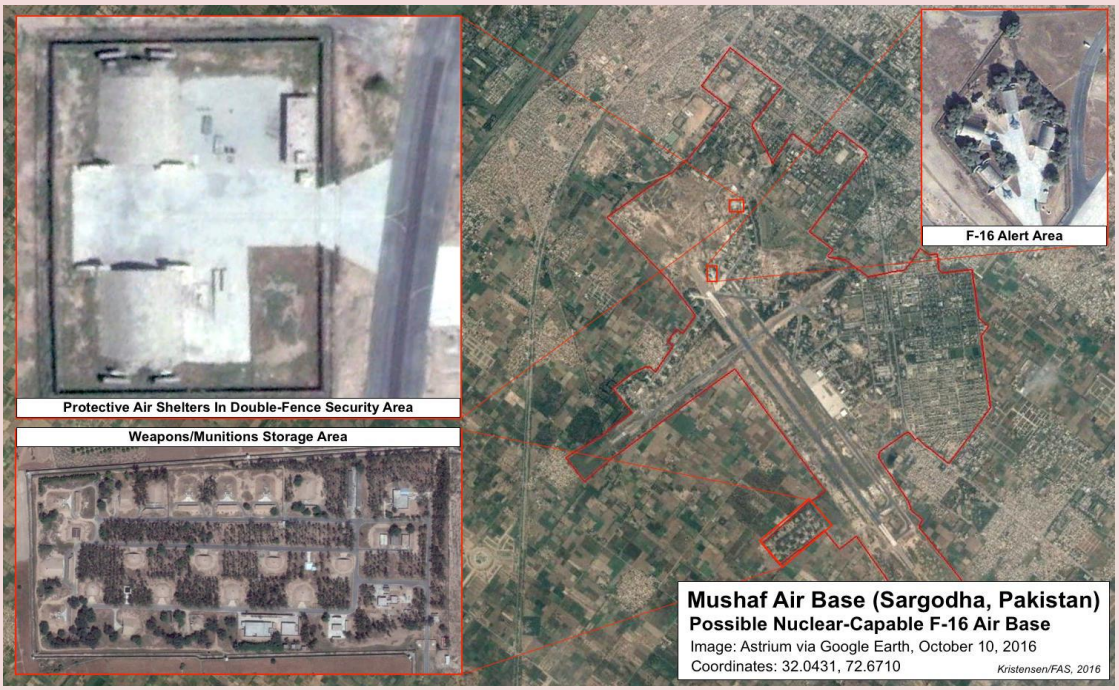
Masroor Air Base includes unique underground facilities.

Another unique facility at Masroor Air Base is a hardened aircraft shelter connected by an underground tunnel to what appears to be a weapons storage facility. The purpose of this facility (first spotted by https://twitter.com/rajfortyseven) is unknown but could potentially be designed to enable concealed nuclear weapons loading of Mirage fighter-bombers.

It should be emphasized that despite the interesting features of some of the facilities at Masroor Air Base, there is no official publicly available information that explicitly identifies them as nuclear.

Mushaf Air Base: One of Pakistan's oldest suspected nuclear-capable air bases is Mushaf Air Base located (32.0431, 72.6710) near Sargodha in the Punjab Province. The base is the home of the 38th Wing with F-16 squadrons that have long been suspected of forming part of Pakistan's air-borne nuclear deterrent.

One pair of hardened aircraft shelters at the base are located inside an area with additional security perimeter but there is little visible evidence of nuclear facilities at the base. The munitions storage area shows no unique structures that suggest a nuclear weapons storage role.



Mushaf Air Base has long been rumored to have a nuclear role. Click image to view full size.

Instead, nuclear bombs for the F-16s at Mushaf Air Base might be stored at the nearby Sargodha weapons storage facility less than 10 kms (6 miles) to the south.

Others Air Bases: There are a couple of other Mirage and F-16 Air Bases that could potentially also serve a role as part of Pakistan's airborne nuclear strike mission. This includes the Mirage-equipped base at Rafiqui (30.7580, 72.2822), which has been upgrade over the past three years. The F-16 base at Shahbaz (28.2825, 68.4506) has been upgraded considerably to accommodate the new F-16s (Block 52).

These and other bases could potentially serve a dispersal bases for Mirage and F-16 nuclear-capable bombers. But there is little visible physical evidence to suggest they serve a nuclear role. Likewise, **Kamra (Minhas) Air Base** (33.8697, 72.4004) has often been **suspected to have a nuclear role** but appears to serve as conversion facility for aircraft.

Conclusions and Implications

Commercial satellite pictures provide new information about Pakistan's emerging nuclear weapons posture that includes missile garrisons for short-range nuclear-capable missiles,

unique underground facilities potentially intended for nuclear weapons storage, and air bases with possible nuclear-related facilities.

The tactical nuclear-capable launchers do not present a strategic threat to India due to their short range, but their introduction into the Pakistani armed forces raises important questions about early dispersal of nuclear warheads and launch authority in a crisis as well as potential earlier use of nuclear weapons in a conflict with India.

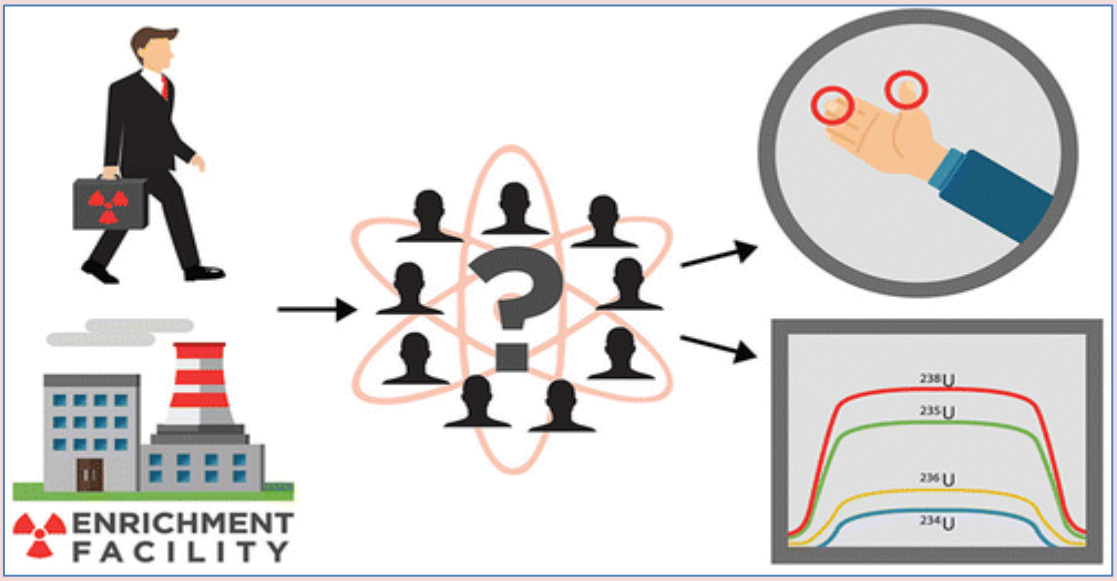
We estimate that Pakistan currently has a stockpile of 130-140 nuclear warheads and is building more. But we also take note of statements by some Pakistan officials that the country might not intend to continue to increase it arsenal indefinitely but may soon reach the goal for the size of its full-spectrum deterrent. Whether and when that will happen remains to be seen. For now the Pakistani arsenal is in a dynamic phase.

Hans M. Kristensen *is the director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons. Kristensen is co-author of the Nuclear Notebook column in the Bulletin of the Atomic Scientists and the World Nuclear Forces overview in the SIPRI Yearbook. The Nuclear Notebook is, according to the publisher, "widely regarded as the most accurate source of information on nuclear weapons and weapons facilities available to the public."*

Biological Screening to Prevent Nuclear Terrorism?

Source: http://i-hls.com/2016/11/biological-screening-to-prevent-nuclear-terrorism/

Nov 08 – The growing threat of nuclear terrorism by extremist groups, independent or supported by states, has been urging law enforcement agencies as academic researchers to develop advanced means for screening suspects exposed to nuclear materials.



National American defense agencies currently face the feat of determining if an individual has handled nuclear materials such as uranium or plutonium. Although uranium exposure is possible to find through a urine sample, urine is able to only identify those who have been recently exposed. **Scientists at the University of Missouri have developed procedures that will improve the ability to identify individuals exposed to uranium within a period of one year.**

"We are working to develop a tool that law enforcement agencies will be able to use and identify individuals who have handled special nuclear material," said John Brockman, associate professor of research in the MU Research Reactor Center. "The goal of our research was to determine

if hair, fingernail clippings and toenail clippings could be used to better detect uranium exposure."

"Our technique was not only able to determine uranium exposure, but also the specific isotopes the individual has handled within the last year," Brockman said. "We were able to identify exposure to enriched uranium, which is used to make both nuclear fuel and weapons, and U-236 which is suggestive of nuclear fuel reprocessing."

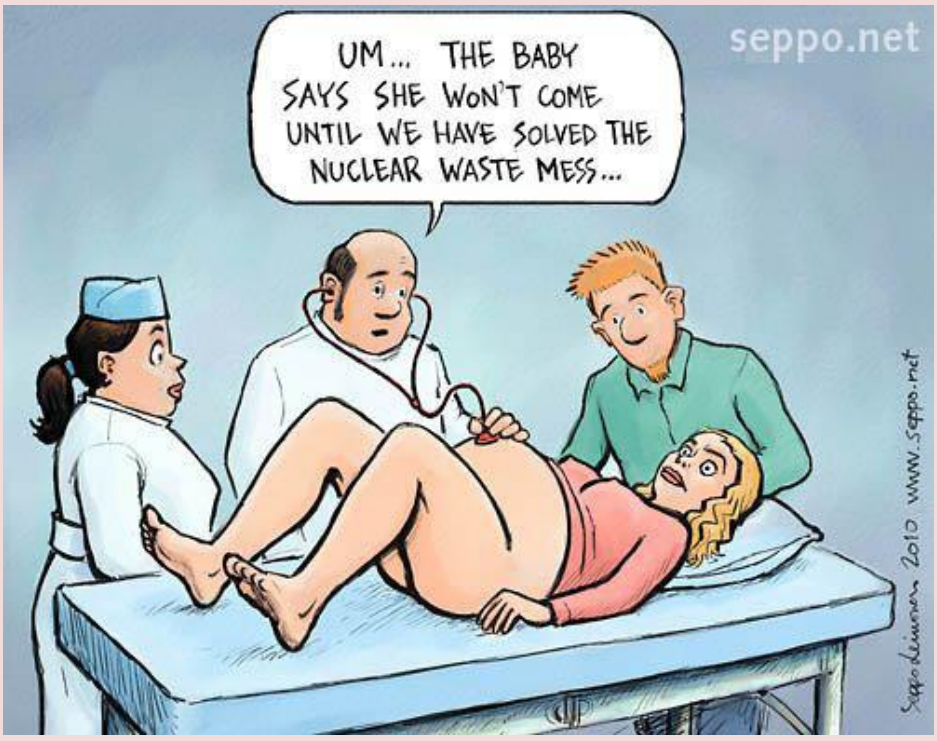
Brockman is looking to expand his analysis with the national human radiobiological tissue repository (NHRTR) to further provide insight on how hair and nail samples could be used to monitor exposure to special nuclear material.

According to the university's website, **the study "Measurement of Uranium Isotope Ratios in Keratinous Material: A Noninvasive Bioassay for Special Nuclear Material,"** recently was published in Analytical Chemistry and was funded by a grant from the Defense Threat Reduction Agency and a National Science Foundation grant.

ABSTRACT

Anal. Chem., 2016, 88 (17), pp 8765–8771

Hair, toenail, and fingernail are noninvasive, integrative biological monitors routinely used to assess mineral intake.1−4 In this study, we demonstrate the feasibility of distinguishing between exposure to natural, depleted, and enriched U by measuring the $^{235}U/^{238}U$, $^{234}U/^{238}U$, and $^{236}U/^{238}U$ ratios in the hair, fingernails, and toenails of occupationally exposed workers and control volunteers. The exposure history of cases and controls to non-natural U was assessed through voluntary self-reporting using a simple questionnaire. The measured U isotope ratios and U concentration in the hair, toenail, and fingernail of cases were compared to a nonexposed control group. No difference was observed in the uranium concentration between the two groups. Significant differences between the cases and the control group were observed in the $^{235}U/^{238}U$ and $^{236}U/^{238}U$ isotope ratios but not the $^{234}U/^{238}U$. This is the first time that hair, fingernail, and toenail have been demonstrated to be sensitive to occupational exposure to enriched and depleted U, a result with significant implications for proliferation compliance monitoring.



Off-road bomb squads: All-terrain vehicle turns bulky EOD specialists into speedy saviors

Source: http://www.washingtontimes.com/news/2016/oct/14/off-road-bomb-squads-new-all-terrain-vehicle-turns/

Oct 14 – A US company has largely turned the cumbersome suits and equipment of explosive ordinance disposal (EOD) personnel into a non-factor with its new off-road vehicle.

Alabama-based Torq Defense Systems has developed a buggy that can bring in EOD specialists, SWAT and HAZMAT teams in a hurry. Its Explosive Ordinance Disposal Light Tactical Electric Vehicle (LTEV) was specifically engineered around the bulky equipment first responders use to save lives.

"We designed this purpose-built LTEV with input from EOD and law enforcement industry" said Rick D'Andrea, director of Sales and Marketing in a Tuesday press release.

The product also impressed Popular Mechanics, which called the LTEV "a go-kart for the bomb squad" on Friday.

Some of the other features on the light-tactical vehicle include:

- A max speed of 30 miles per hour.
- An overhead operator protection system.
- All-wheel hydraulic disc brakes.
- Independent front and rear suspension.

"The open design of this lightweight and stealthy task oriented vehicle easily lends itself to situational customization for a wide array of narrowly defined missions and applications, TORQ Defense Systems President Steve Brown added in the company's press release.

Popular Mechanics noted that police departments have been keen to acquire such a vehicle, which may have been useful this summer when a bomb disposal robot was deployed in Texas to kill an active shooter.

Micah Johnson died July 7 after a Dallas massacre that killed five police officers and wounded nine others. His rampage also wounded two other civilians.

Homemade bomb 'could have been devastating'

Source: http://www.wellandtribune.ca/2016/10/19/homemade-bomb-could-have-been-devastating

Oct 19 – There'd likely be a crater where 79 Park St. now stands if one of those homemade bombs detonated during Sunday's fire, said Niagara Regional Police Det. Sgt. Wayne Genders.

And there were at least four improvised explosive devices found within the upper apartment, including one that incorporated a typical backyard barbecue propane tank.

Genders said Welland firefighters he spoke to described the devastation that could have been caused if just one of the bombs had exploded.

"If that would have blown it would have leveled the house and there'd be collateral damage to the surrounding homes," he said Wednesday, while providing details about his ongoing investigation into the startling discovery of explosives after Welland firefighters extinguished the blaze that started at about 1:38 p.m.

He said firefighters also faced a huge risk while extinguishing the fire.

"That could have been devastating. I could just imagine what could have happened there. Never mind property damage, the loss of life could have been huge."

Genders said there were about four or five bombs found within the apartment, although "there could be more."

The bombs were constructed out of various items, including the propane tank, aerosol cans, and ammunition from a gun.

"I don't have a total report, but that was some of the preliminary stuff," he said, adding he's hoping the report from the NRP's bomb technicians will provide more insight into how the materials could be incorporated to construct the bombs.

"I'm not a bomb-maker so I don't understand all this either, but I'm starting to get a sense of it."

While finding improvised explosive devices is unusual, fire Chief Brian Kennedy said most of the items used to make those devices "are common in every house."

"There was nothing in there that we don't encounter at every fire we go to. Your average garage fire has more hazardous things in it than people really realize," he said. "Aerosol cans, paint cans, propane tanks, they're all in our everyday fires. We have to be very careful when we approach these fires."

He recalled one garage fire "several years ago" where an acetylene tank exploded and its folded flat wreckage crashed down on the back of a fire truck.

"That's the backyard mechanic. Those kinds of people have all kinds of hazards in their just regular shops. It's something we encounter and have to think about at every call we respond to," he said.

In addition to threat commonly found within burning buildings, Kennedy said local firefighters have also responded to fires "where there have been intentional things done" to add significantly to the danger fire fighters face, such as propane tanks brought into a building.

"They're not normally there, and they shouldn't be there. But we've gone into fires and once the smoke clears then you see it – there's a propane tank on a table," he said. "Why is that? Clearly there's someone trying to do something."

A 41-year-old man who escaped the burning apartment through a second floor window during the fire remains in critical condition at a Hamilton hospital, being treated for severe smoke inhalation.

Genders said he has yet to interview the man, who has not been charged and his name has not been released.

But through his investigation, Genders hopes to determine who created the explosives and why, and if charges are warranted.

"There's still lots of work to do."

Genders said investigations involving homemade bombs are rare in Niagara.

He said the NRP's bomb technicians only see a couple calls a year like this. The most recent was earlier this year in Niagara Falls, involving an explosive made using chemicals.

"I've been here 32 years and I've never investigated one," he said.

At this time, he said police believe it was an isolated incident.

"There is nothing to lead us there (terrorism) at this point, so I'll just leave it there as that. I mean we can't say 100 per cent, but there is nothing to indicate that," Genders said.

Damage inside the building was not as severe as firefighters and police previously anticipated.

He said there were some rooms upstairs that were destroyed, but other rooms only have water and smoke damage.

Kennedy said that's one of the reasons the improvised explosive devices did not detonate.

The propane tank, for instance, was in an area where the fire had not spread yet, and other explosive devices were found on the floor, below the heat of the flames.

Kennedy said the Ontario Fire Marhal's office has concluded its investigation into the fire, and he's awaiting its report about the fire before he's able to comment on the cause.

"I think there was some clear evidence in there of what went on, but I haven't had a chance to sit down with anyone in there to get that information yet," he said.

K-P's bomb disposal robots out of order

Source: http://tribune.com.pk/story/1202749/dysfunctional-k-ps-bomb-disposal-robots-order/

Oct 19 – **Despite playing a vital role in countering terrorism and defusing over 6,000 improvised explosive devices and person-borne improvised explosive devices over the past eight years, Khyber-Pakhtunkwa's Bomb Disposal Unit is marred by lack of funds and equipment.**

The four robots donated to the bomb disposal unit in 2012 too have become partially dysfunctional due to lack of proper maintenance. The robots were donated by the British government to K-P police four years ago.

These robots were designed to scan suspicious vehicles or objects for explosives and upon detection defuse them. However, though the robots aimed to reduce the risk for BDU personnel, they were seldom brought to the field.

According to sources in the bomb disposal unit, the robot working in Nowshera is better in comparison with the one in Peshawar.

"We have twenty-five districts in the province and wish that the K-P government provide at least two robots for each one of them. We have demanded that Peshawar, which faces 50% of the attacks, must have at least five or six such robots to save maximum number of lives," K-P Assistant Inspector General Shafqat Malik of the bomb disposal unit told *The Express Tribune*.

AIG Malik confirmed that the gadgets had reached their expiry and stated that he had repeatedly requested the provincial government to acquire new robots to save the lives

While commenting on the issue, Advisor to Chief Minister on Information Mushtaq Ahmad Ghani said that the incumbent government spent around Rs30 billion and accepted that the department was facing problems. He added that the provincial government was working to improve the situation.

Smiths Detection's TRACE-PRO™ now identifies the explosive - TATP

Source:http://www.cbrneworld.com/news/smiths_detections_trace_pro_now_identifies_the_explosive_tatp#axzz4KVD9jSfC

Sep 14 – Smiths Detection's newly launched TRACE-PRO™, a non-radioactive, hand-held explosive threat detector, now has the additional capability to detect and identify TATP (Triacetone Triperoxide). This was the explosive substance used in the terrorist attack in Brussels in March 2016. This much-needed capability will enable users of TRACE-PRO to identify traces of TATP easily and aid covert operations or

security operators to screen people, objects and materials in any location.

Shan Hood, Vice President, Products & Technology, Smiths Detection said "We are very proud to announce the addition of TATP detection capability to TRACE-PRO™. This has been a priority for our customers. Due to its chemical makeup, TATP can be difficult to detect and TRACE-PRO™ now provides an easy to use solution to identify this challenging substance. Since TRACE-PRO's launch in November 2015 we have seen considerable interest in customers wanting to use this advanced technology for a wide range of applications, including the military, police, airports and hotels."

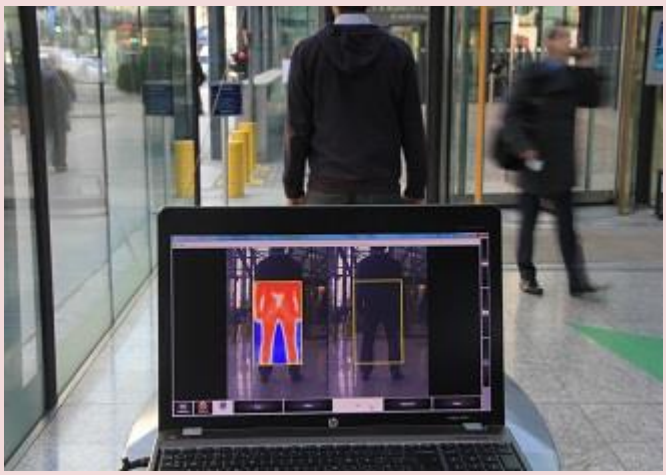
TRACE-PRO™ is a revolutionary hand-held detector for fast identification and evidence collection of common explosives and can deliver a result in less than 10 seconds. Swabs can be taken from people, objects and materials in any location and the in-built camera and GPS facilitate easy evidence collection – allowing the user to record and store data in the immediate location of the suspect substance.

TRACE-PRO™ is suited to a variety of environments and situations with its ruggedised exterior. It is **ergonomically designed, weighs just 1.7 kg and is the only detector that can be powered by AA commercial batteries.** It requires minimal user training due to its intuitive software and provides a low cost of ownership through its re-usable swabs and basic maintenance requirements.

Highly Sensitive Camera will Identify Explosives at Airports

Source: http://i-hls.com/2016/11/highly-sensitive-camera-will-identify-explosives-at-airports/

Nov 03 – A new technology that claims to be able to identify weapons hidden under people's clothing as they walk through checkpoints, is currently under trial at a handful of international airports. It is being used to provide an additional layer of security against landside attacks.



The new technology, ThruVis, developed by UK based

security technology company Digital Barriers, utilises a highly sensitive camera capable of detecting hidden objects such as weapons, explosives and drugs.

Its creators envisage two main ways of deploying Thruvis at airports – at entrances to terminal buildings to identify threats before passengers reach the traditional security checks and as a secondary check of airport staff when they pass in and out of secure areas, according to airportworld.com.

Digital Barrier's chief executive, Zak Doffman, says: "Our highly sensitive camera solution can be covertly deployed at airport entrances to spot items concealed under a person's clothing before they reach baggage points and security chokepoints.

"Once deployed, it will spot hidden explosives and liquids, with recent tests having a 100% success rate in identifying anyone carrying a hidden weapon or suicide vest. The solution does not replace an airport's existing security infrastructure; rather it acts as an additional protection that can extend the airport's secure zone as far as the terminal entrance."

ThruVis works on the TeraHertz frequency, meaning that unlike X-rays it has no harmful effects to the human body and does not reveal anatomical details.

The technology is currently being trialled at transport terminals in the US and the UK and is already in use in the Middle East and Asia.

Spinach effective in helping detect landmines, according to MIT field work

Source: http://en.mercopress.com/2016/11/01/spinach-effective-in-helping-detect-landmines-according-to-mit-field-work

Nov 06 – **Scientists have transformed the humble spinach plant into a bomb detector. By embedding tiny tubes in the plants' leaves, they can be made to pick up chemicals called nitro-aromatics, which are found in landmines and buried munitions. Real-time information can then be wirelessly relayed to a handheld device.**

The MIT (Massachusetts Institute of Technology) work is published in the Journal Nature Materials. The scientists implanted nano-particles and carbon nano-tubes (tiny cylinders of carbon) into the leaves of the spinach plant. **It takes about 10 minutes for the spinach to take up the water into the leaves.**

To read the signal, the researchers shine a laser onto the leaf, prompting the embedded nanotubes to emit near-infrared fluorescent light.

This can be detected with a small infrared camera connected to a small, cheap Raspberry Pi computer. The signal can also be detected with a smartphone by removing the infrared filter most have.

Co-author Prof Michael Strano, from MIT in Cambridge, US, said the work was an important proof of principle. "Our paper outlines how one could engineer plants like this to detect virtually anything," he told the BBC News website.

Prof Strano's lab has previously developed carbon nanotubes that can be used as sensors to detect hydrogen peroxide, TNT, and the nerve gas sarin.

When the target molecule binds to a polymer material wrapped around the nanotube, it changes the way it glows.

"The plants could be use for defense applications, but also to monitor public spaces for terrorism related activities, since we show both water and airborne detection," said Prof Strano.

"Such plants could be used to monitor groundwater seepage from buried munitions or waste that contains nitro-aromatics."

Using the set-up described in the paper, the researchers can pick up a signal from about 1m away from the plant, and they are now working on increasing that distance. (BBC).

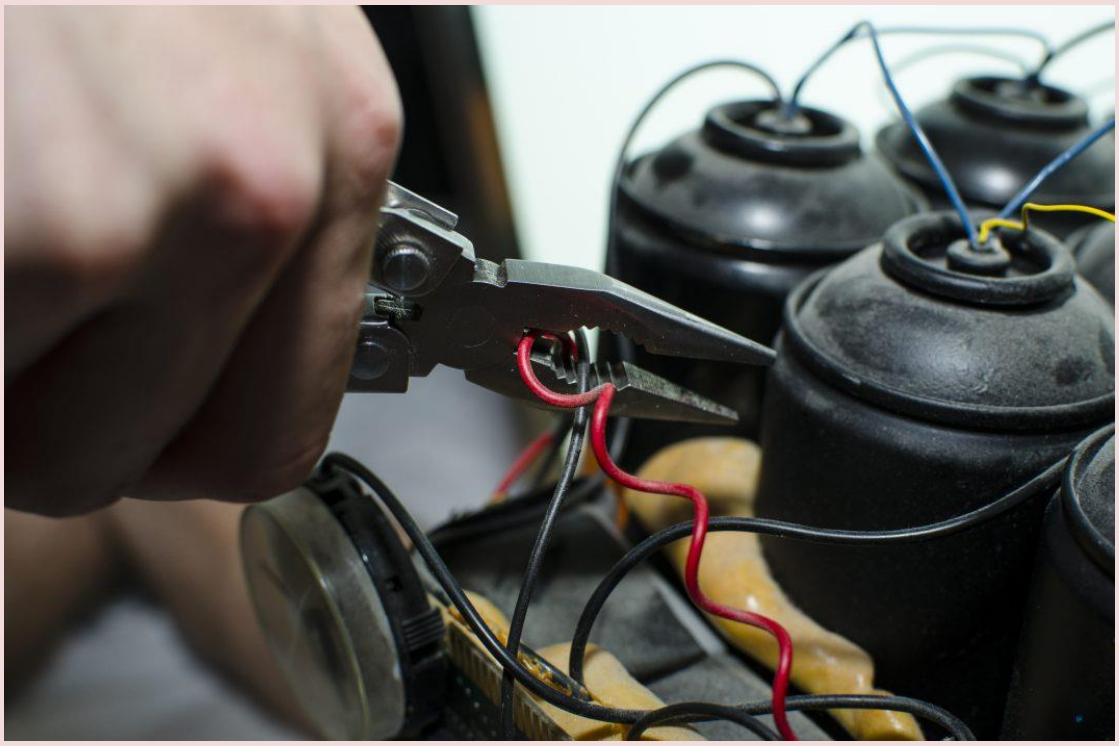
There's No Place Like Home: The Threat of HME and IEDs

By Frank G. Rando

Source: http://www.cbrneportal.com/theres-no-place-like-home-the-threat-of-homemade-explosives-and-ieds/

" Terrorism has become the systematic weapon of a war that knows no borders or seldom has a face." – Jacques Chirac

"This is not the end. This is not even the beginning of the end. This is just the end of the beginning." – Sir Winston Churchill



Oct 27 – Recently, the world has seen an increased use of homemade explosives (HME) and explosive devices to perpetrate acts of terror. This trend has been accentuated by the recent use of these devices on U.S. soil. On September 19, a homemade improvised explosive device (HMIED) in the form of a pipe bomb, detonated in New York City 's Chelsea section, injuring 29 individuals. A second pipe bomb device also exploded in Seaside Park, New Jersey without injuries. The Seaside Park device was positioned in an area proximal to where thousands of runners were due to partake in a 5,000 meter race to benefit U.S. Marines and sailors.

In addition, five suspect devices were discovered in a backpack placed in a waste disposal bin near the Elizabeth, New Jersey train station. A second unexploded device consisting of pressure cookers, a cellular "flip" phone and Christmas lights was discovered only a few blocks away from the West 23rd Street Chelsea location. The pressure cooker device was reminiscent of the Boston Marathon bombing incident and of other similar devices used in the Middle East. Tannerite, which is used in target practice and is readily available in sporting goods stores was the explosive used in the detonation in Chelsea and suspected to have been used in the unexploded device nearby.

HMEs/IEDs can be readily manufactured and constructed from instructions derived from the Internet and a variety of underground publications, such as The Poor Man's James Bond and The Anarchist's Cookbook. The perpetrator seeking to concoct a HME/IED can combine commercially available precursor materials or military or commercial explosives to create non-conventional improvised explosive materials. Terrorists may obtain materials and supplies via legal and illegal sources. Legally, perpetrators can obtain precursor materials through legitimate sources such as retail purchases made at beauty supply stores, hardware stores, grocery stores, home improvement outlets, swimming pool supply stores and other commercial establishments. These materials do not require special permits or authorization. Retail purchases do not have to be made in person – they can be obtained via online ordering and delivered via common carriers, such as FedEx, UPS and others, as these items are not classified as restricted commodities.

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

Frank G. Rando *possesses over 30 years of real world experience as a public safety professional, clinician, educator, emergency and crisis manager, author*

and consultant in the areas of tactical, disaster and operational medicine, weapons and tactics, law enforcement /criminal investigations, counterterrorism, hazardous materials management and emergency response, toxicology, environmental safety and health, and health care and public health emergency management.

Islamic State Calls for Vehicle Attacks

Source: https://pietervanostaeyen.files.wordpress.com/2016/11/rumiyah3en.pdf

On Friday (Nov 12, 2016), AlertsUSA subscribers were notified via SMS messages to their mobile devices of the release of a new issue of the Islamic State propaganda magazine known as ***Rumiyah (#3)*** which calls on Muslims to carry out vehicle attacks similar to that Bastille Day celebrations on July 16th in Nice France. The article goes into detail (pp.10-12) on selecting the ideal vehicle, suggests applicable targets such as large outdoor markets, conventions and celebrations, pedestrian-congested streets and parades, as well as provides guidance on preparation and planning.

Though being an essential part of modern life, very few actually comprehend the deadly and destructive capability of the motor vehicle and its capacity of reaping large numbers of casualties if used in a premeditated manner. This was superbly demonstrated in the attack launched by the brother Mohamed Lahouaiej-Bouhlel who, while traveling at the speed of approximately 90 kilometers per hour, plowed his 19-ton load-bearing truck into crowds celebrating Bastille Day in Nice, France, harvesting through his attack the slaughter of 86 Crusader citizens and injuring 434 more.

The method of such an attack is that a vehicle is plunged at a high speed into a large congregation of kuffar, smashing their bodies with the vehicle's strong outer frame, while advancing forward – crushing their heads, torsos, and limbs under the vehicle's wheels and chassis – and leaving behind a trail of carnage.

The publication suggests the Macy's Thanksgiving Day Parade as an "excellent target."

An excellent target

AlertsUSA again cautions readers that despite the overwhelming news coverage of the election and politics in general, it is important to keep in mind that the threat of terrorism in N. America and Europe is still extremely high and has not abated. The intelligence community is unanimous in their view that the tempo of attacks will increase as the Islamic State and al Qaeda continue to experience battlefield defeats overseas. As such, an increased level of situational awareness and vigilance is urged when out and about.

The Ideal Vehicle

- Load-bearing truck;
- Large in size, keeping in mind its controllability;
- Reasonably fast in speed or rate of acceleration (Note: Many European countries pre-restrict larger vehicles to specified speeds);
- Heavy in weight, assuring the destruction of whatever it hits;

- Double-wheeled, giving victims less of a chance to escape being crushed by the vehicle's tires;
- Possessing a slightly raised chassis (the under frame of the vehicle) and bumper, which allow for the mounting of sidewalks and breeching of barriers if needed;
- If accessible, with a metal outer frame which are usually found in older cars, as the stronger outer frame allows for more damage to be caused when the vehicle is slammed into crowds, contrary to newer cars that are usually made of plastics and other weaker materials.

Vehicles to Avoid

- Small cars, including larger SUVs;
- Slower vehicles that cannot exceed 90km per hour;
- Load-bearing trucks with load compartments that are not fixed to the cabin, which may cause loss of control and subsequent jackknifing, especially if driven erratically;
- Load-bearing trucks with excessively elongated trailer compartments, which can cause the driver trouble as he seeks to maneuver.

Preparation and Planning

- Assessing vehicle for roadworthiness;
- Filling vehicle with a sufficient amount of fuel;
- Mapping out the route of the attack;
- Surveying the route for obstacles, such as posts, signs, barriers, humps, bus stops, dumpsters, etc. which is important for sidewalk-mounted attacks, keeping in mind that more obstacles might be set up on the day of a targeted event, and doing the surveillance in an inconspicuous manner, specially if one suspects being monitored by an intelligence apparatus;
- If accessible, a secondary weapon should be attained (gun or knife).

Ambulance suicide bombings kill at least 24 in Iraq

Source: http://news.sky.com/story/ambulance-suicide-bombings-kill-at-least-24-in-iraq-10647391

Nov 06 – At least 24 people have died after ambulances loaded with explosives were detonated in two Iraqi cities.

The suicide attacks in Tikrit and Samarra come as Iraqi forces battle to clear areas taken from Islamic State around Mosul.

In Tikrit, a blast near an entrance to the city during the morning rush hour killed at least 13 people.

Meanwhile, at least 11 people died in an attack against Shia pilgrims in Samarra, about 60 miles north of Baghdad.

Ali al-Hamdani, spokesman for Salahuddin province, said a bomber parked an ambulance in the car park for a Shia shrine.

He walked up to pilgrims about 500 metres from the shrine, detonated his vehicle and then blew himself up, Mr al-Hamdani said.

Five female students, a woman and three policemen were among those killed, while up to 100 others were injured.

Islamic State has issued a statement claiming the bombings, which are the latest in a series of attacks during the three-week campaign to recapture Mosul.

EDITOR'S COMMENT: Take a note – AMBULANCES. They easily move around without raising suspicions and always have traffic priority… and they can be heavily loaded with everything!

Man injured after package explodes in Philadelphia

Source: http://6abc.com/news/man-injured-after-package-explodes-in-center-city/1619575/

Nov 22 – Philadelphia police explosive experts are on the scene after a package containing medicine exploded and injured a man in Center City Philadelphia.

It happened around 4 a.m. Tuesday inside an apartment on the 1800 block of Pine Street.

Police say a 62-year-old man received the package around 5 p.m. Monday.

When he went to **open the package containing some type of medicine** early Tuesday morning, it exploded.

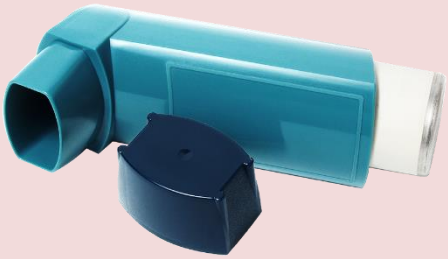
The man was taken to Thomas Jefferson University Hospital with chest and hand injuries. He is in stable condition.

Police say the explosion happened in the kitchen area and damaged the oven range.

The man's roommate told police **the victim does receive inhalers in the mail.** But it is still unclear what was in the package.

"It did explode," Philadelphia Police Chief Inspector Scott Small told Action News early Tuesday. "But at this time, they don't know whether or not this was an intentional explosion. In other words, we don't know if this was a bomb mailed to the house... or whether this was just some sort of freak accident where something like an inhaler just exploded." Police say there were no threats before or after the package exploded.

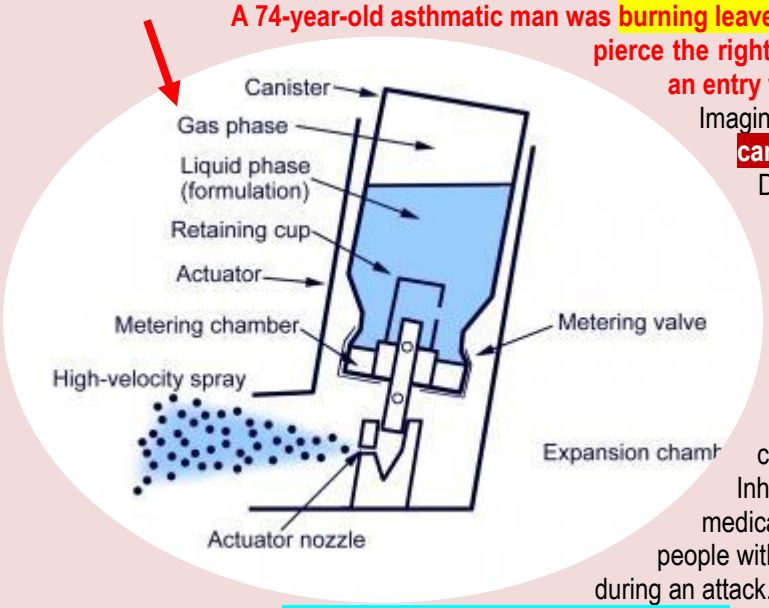
Asthma inhaler lodged in chest highlights importance of warning labels



Source: http://www.reuters.com/article/us-device-safety-asthma-idUSKBN0FE2D620140709

July 2014 - A new case report from France offers a reminder of why people who use medical devices like asthma inhalers should take warnings on the product label seriously.

A 74-year-old asthmatic man was burning leaves when he heard an explosion and felt something pierce the right side of his chest. At the hospital, doctors found an entry wound between his ribs, but no exit wound.



Imaging revealed what appeared to be a **nebulizer canister wedged between his liver and diaphragm.**

Doctors believe the man's inhaler fell from his pocket into the fire and exploded.

Dr. Stanislas Ledochowski of the Hospitalier Universitaire Lyons Sud, who examined the man, told Reuters Health, "Fortunately, it is to be considered as an exceptional event, and since it was the only described case in the medical literature, we thought describing such an occurrence could be of medical interest."

Inhalers, a portable form of nebulizer, turn liquid medication into a fine mist, which is the fastest way for people with asthma or other lung conditions to dose themselves during an attack.

But **the devices contain pressurized gas** along with medication, and canisters of albuterol, the drug the patient used, carry a warning to keep them away from flames or high heat.

The National Institutes of Health also warns that albuterol should be kept out of the reach of children, stored at room temperature and kept in its foil pouch until needed.

Ledochowski and his coauthors describe in the journal *Surgery* what they found when they went in to remove the foreign object. The burnt canister was lodged between the man's liver, which suffered no damage, and his diaphragm, which was slightly ruptured.

In some cases of chest trauma, they write, doctors decide that it would be better to leave the foreign object in place. But to avoid the risk of infection, Ledochowski surgically removed the canister.

About 25 million Americans have asthma, and according to the U.S. Centers for Disease Control and Prevention, that number increases every year.

"The general public should understand, that all medical devices and drugs are designed for a specific purpose and that their unreasoned use, voluntary or not, can have severe consequences," Ledochowski said.

"What was exceptional in this case report is the severity of the sustained trauma and the object responsible for the trauma," he said. "As with every domestic device that contains gas, the warning about not approaching these objects to a heat source has to be respected."

Black (medical) humor!

New cyber threat: Hacking 3D manufacturing systems

Source: http://www.homelandsecuritynewswire.com/dr20161020-new-cyber-threat-hacking-3d-manufacturing-systems

Oct 20 – **Researchers from three universities combined their expertise to demonstrate the first complete sabotage attack on a 3D additive manufacturing (AM) system, illustrating how a cyberattack and malicious manipulation of blueprints can fatally damage production of a device or machine.**

dr0wned – Cyber-Physical Attack with Additive Manufacturing

Sofia Belikovetsky	Mark Yampolskiy	Jinghui Toh	Yuval Elovici
Ben-Gurion University of the Negev	*University of South Alabama*	*Singapore University of Technology and Design*	*Ben-Gurion University of the Negev, Singapore University of Technology and Design*

In their paper titled "Dr0wned," researchers from Ben-Gurion University of the Negev (BGU), the University of South Alabama, and Singapore University of Technology and Design detail how to sabotage the quality of a 3D-printed functional part, which leads to the destruction of a device.

A proof-of-concept video shows how the researchers destroyed a $1,000 quadcopter UAV drone by hacking into the computer used to control the 3D printing of replacement propellers. Once they penetrated the computer, the researchers identified the propeller blueprint file and inserted defects undetectable by visual inspection. During flight tests, the sabotaged propeller broke apart during ascent, causing the drone to smash into the ground.

More than 100 industries, including aerospace, automotive and defense, employ additive printing processes. According to the *Wohlers Report*, the AM industry accounted for $5.165 billion of revenue in 2015. Furthermore, 32.5 percent of all AM-generated objects are used as functional parts.

"Imagine that an adversary can sabotage functional parts employed in an airplane's jet engines. Such an attack could cost lives, cause economic loss, disrupt industry, and threaten a country's national security," says Prof. Yuval Elovici. Elovici is a member of BGU's Department of Software and Information Systems Engineering, director of the Deutsche Telekom Innovation Labs @ BGU and the BGU Cyber Security Research Center (CSRC). The CSRC is a collaboration between the University and Israel's National Cyber Bureau, focused on advanced cyber security topics.

"With the growth of additive manufacturing worldwide, we believe the ability to conduct malicious sabotage of these systems will attract the attention of many adversaries, ranging from criminal gangs to state actors, who will aim either for profit or for geopolitical power," says Elovici. "'Dr0wned' is not the first article that raises this issue. However, all prior research has focused on a single aspect of a possible attack, assuming that all other attack elements are feasible," the researchers say. **"This is the first experimental proof of a complete attack chain initiated by sabotaging the 3D-printed propeller."**

The study addresses the consequences of cyberattacks, and proposes a systematic approach for identifying opportunities and a methodology for assessing the level of difficulty of an attack involving AM.

Terrorists could launch a cyber attack within three years, report warns

Source: http://www.smh.com.au/federal-politics/political-news/terrorists-could-launch-a-cyber-attack-within-three-years-report-warns-20161011-gs04qy.html

Oct 12 – **The government claims terrorists could be capable of launching a cyber attack on Australia "to destructive effect" within three years even though the threat of their capability is currently ranked as "low".**

The advice is contained in a new report by the Australian Cyber Security Centre (ACSC) to be released on Wednesday.

The collective of hackers known as Anonymous released a video the day after the terrorist attacks in Paris declaring it would retaliate with a new wave of cyberattacks on ISIS.

While Australia has never been the victim of a cyber attack, authorities have investigated 1095 cyber security incidents investigated over the past 18 months. These have been the work of hacktivists, cyber criminals and foreign state actors.

Writing in News Corp, the Minister Assisting the Prime Minister for Cyber Security Dan Tehan claimed terrorists would be soon capable of targeting Australia over the internet.

"The threat of a cyber attack from terrorists presently is ranked as low," he said.

"Islamic State is using social media for propaganda and recruitment but its skills to launch a genuine cyber attack are rudimentary."

"That won't always be the case and the ACSC estimates that within three years terrorists will have the ability to compromise a secure network with destructive effect."

The minister said that the national computer emergency response team (CERT Australia) had dealt with 14,804 cyber security incidents affecting Australian businesses in the last financial year.

He said 418 of those involved "systems of national interest and critical infrastructure."

While Islamic State has expressed a desire to venture into cyber attacks their ability to do so is considered remote and have been more successful in recruiting potential fighters online.

In September 2015, the Director of National Intelligence in the United States, James Clapper said while terrorist groups are experimenting with hacking, their sympathisers have so far only managed to conduct "low-level attacks," that has attracted more media attention than damage.

Alex Kassirer, a Flashpoint terrorism analyst, which monitors extremists' chatter on the dark web agreed that it was "laughable" to think Islamic State, which is in retreat in Iraq and Syria, could launch a cyber attack.

"They're incredibly unsophisticated in their cyber abilities," she said.

But she said the government warnings should be believed because terrorist groups are repeatedly expressing a desire to venture into cyber attacks.

"On this forum there was a recent conversation that discussed 'launching a hacking' and that just shows an interest and an aspiration amongst the group's supporters to learn how to hack and have some sort of cyber capability, so its definitely something they're trying to cultivate," she told Fairfax Media.

"I think it's inevitable that they're going to try their hand at it because they see it can be successful," she said.

She said she was hesitant to put a timeframe on it on how soon that might be.

"But I don't think [three years] seems incredibly overblown, especially given the fact they're talking about it on their forums, it's definitely seems like something on their radar at the very least."

But she said the more immediate threat of a cyber attack was from sophisticated foreign state actors and their success would inspire terrorist groups to innovate.

"I think the real danger of a terrorist group developing cyber ability is that they have no restraints…unlike state actors who have to operate in the international community."

The government is currently reviewing how Australia's intelligence agencies operate. Recently the agencies began a recruitment drive for hackers to test for potential holes in government systems.

Is someone really trying to find out if they can destroy the Internet?

By David Glance

Source: http://www.homelandsecuritynewswire.com/dr20161025-is-someone-really-trying-to-find-out-if-they-can-destroy-the-internet

Oct 25 – A prolonged Internet outage prevented access to major sites like Twitter, Netflix, Spotify, and the *New York Times* on Friday. The attack has commentators concerned that this is was a practice run for future, promising more frequent and widespread disruption of the Internet. The distributed denial of service attack (DDoS) targeted the dynamic domain name service provider Dyn and came in three waves during the day.

Dynce provides Internet address translation through DNS servers to take a name like www.nytimes.com and translate it into an address like 170.149.159.130. Denial of service attacks use a variety of techniques to keep the DNS servers busy. The attacks work by flooding DNS servers with millions of requests that seem legitimate but are for fake addresses, causing the DNS server to get overloaded. Real DNS requests from real users can't get through and so it appears that the site they are trying to get to, like www.netflix.com is down.

DNS attacks operate in a number of different ways but those that affected the Dyn servers were using a range of techniques that included sending requests for sites that had random characters attached to the start of a valid domain e.g. abcd123.nytimes.com. Because these addresses are essentially valid, the DNS server tries to look up the address but gets tied up because of the sheer volume of requests. The attacks are difficult to guard against because the requests are essentially valid.

The sheer volume of requests were being sent in part by the Mirai botnet of Internet of Things devices, mostly Internet-connected cameras and digital video recorders. This botnet has been in a previous attack this month on the website of a security reporter Brian Krebs.

These types of attacks have been occurring more frequently and because they involve pieces of Internet infrastructure, have a more widespread impact. Last month, security analyst Bruce Schneier wrote that he believed that state actors were increasingly probing for weaknesses in the basic infrastructure of the Internet in order to be able to mount large-scale devastating attacks. Because of the increase in number and intensity of DDoS type attacks in recent years, security analysts have theorized that some of the attacks are masking the probing of vulnerabilities.

A particular fear is that a DDoS attack could prevent people from voting online during the U.S. election on 8 November. Overseas military and citizens are allowed to vote online in several US states and everyone in Alaska can vote online. Russia has already been implicated in the hack of Democratic National Committee emails and organizing their release through WikiLeaks.

There is concern that the Russians will try and discredit the election process in whatever way they can and disrupting it through a DDoS attack on the day would be one way of achieving this.

The risk of this actually effecting the vote on the day has been dismissed however as the window for voting online in some of these situations is weeks before the election rather than on the day. When Alabama trialed online electronic voting during the primaries, their site was in fact attacked, but although it slowed down the site, it didn't prevent anyone from voting.

There is also the possibility that this attack was actually just hackers going after a particular site that happened to be using the Dyn service. The source code for the Mirai botnet was released on 1 October and since that time, other hackers have been using the code to expand the number of bots involved and create their own botnets. DDoS attacks may actually just be hackers testing out the power of their creations.

The Internet remains incredibly vulnerable to attacks on its infrastructure and right now, there are few ways of avoiding them.

Because Internet of Things devices like cameras, digital video recorders, and a whole range of other equipment are being used as vehicles to launch DDoS attacks, making sure that the devices are secure would be a priority. However, manufacturers are creating these devices in a way that doesn't allow for automated, un-monitored updates which is what is really required for security patches to be applied when they are discovered. Governments could potentially legislate that they should take all efforts to ensure their devices are secure before allowing the public to connect them to the Internet, but this would need all countries of the world to do this.

It does bring into question the ability of governments to put even more of its interface with the public online since as soon as it does, it becomes a potential target for malicious actors. Governments in particular need to become more adept at dealing with this possibility, especially after the Australian Bureau of Statistics demonstrated that it was unable to run an online census collection successfully in the face of relatively minor DDoS attacks.

***David Glance** is Director of UWA Centre for Software Practice, University of Western Australia.*

More Dangerous Than Boko Haram, Nigeria's New Biggest Terror Threat

Source: https://fronteranews.com/news/africa/dangerous-boko-haram-nigerias-new-biggest-terror-threat/

Oct 29 – The head of an international criminal network behind fraud totaling more than $60m was arrested in Nigeria in June 2016. The 40-year-old Nigerian male was found in Port Harcourt as the result of a global investigation led by Interpol.

Such crime "poses a significant and growing threat, with tens of thousands of companies victimised in recent years," Noboru Nakatani, executive director of the Interpol Global Complex for Innovation, warned in a statement.

Now viewed as a more serious security threat than even terrorism, **cyber attacks and data breaches are now considered the leading risk to businesses today.**

Nigeria's National Information Technology Development Agency (NITDA) estimates that the **local population lost $450 million to digital fraud in 2015. Meanwhile, cyber fraud attempts in the country in the first half of 2016 are reported to have increased by 1,000 times.**

Nigeria's cybercrime act was finally voted into law in May 2015, which defined the legal consequences faced by individuals and corporations found to be in violation of the law. However, many are questioning whether the government and corporations are doing enough to keep cyber threats at bay, and ensure the security of the population.

The website of the Independent National Electoral Commission (INEC) was hacked on the day of the 2015 presidential election. Then, the Lagos state government suffered a major breach in December 2015.

Tope Aladenusi, Partner at Deloitte Nigeria, says that the

cybercrime act "is a welcome development but many key stakeholders such as the judiciary and law enforcement agencies are yet to come up to speed in understanding and implementing the act."

Boasting the largest growth in Internet usage in Africa – from 23.9 million in 2008 to 82.1 million in 2015 – arguably no country on the continent is at greater risk than Nigeria. Aladenusi cautioned that, "the advent of cyber as a weapon of warfare is rapidly gaining momentum and Nigeria is not immune to such threats. It is only a matter of time before it becomes full blown."

Government policymakers and corporations worldwide by and large share these sentiments as threats increase in size and scope. On 8 October, the US formally accused Russia of hacking the Democratic Party's computer networks. Then on 21 October, a major DDoS cyber attack in the US caused outages on a slew of websites including Twitter, Spotify, Amazon, Reddit, Yelp, Netflix and The New York Times.

Recent major hacks on high profile companies including Yahoo, Sony Pictures Entertainment, and Vera Bradley have wreaked considerable damage on the corporate world resulting in heightened fears globally.

Commenting on the Yahoo attack that affected 500 million accounts – allegedly one of biggest thefts of online users' personal information ever – Michael Bittan, a risk manager at Deloitte, cautioned that it was "the biggest to be made public. There have possibly been others that were bigger".

A recent study by PwC found that the number of global cyber security incidents across all industries rose by 38% in 2015 – the biggest increase in the 12 years since the study was first published.

Spending on cyber security worldwide will rise from $73.7 billion in 2016 to $101.6 billion by the start of the next decade, according to new research released in early October by the International Data Corporation. **The US government alone currently spends about $10 billion a year on IT security, and is set to increase this substantially.**

The non-existence of a Nigerian national policy on information security or even guidelines on monitoring and censoring internet content will make cyber security a difficult task for both the local government and corporations to tackle in years to come.

What CSPs can learn from the latest DDoS attacks

Source: http://www.homelandsecuritynewswire.com/dr20161031-what-csps-can-learn-from-the-latest-ddos-attacks

Oct 31 – **On Friday, 21 October 2016, there was a major distributed denial of service (DDoS) attack that took down major US company's web sites, including Twitter, Paypal, the *New York Times*, Box, Netflix, and more.** The attack targeted managed DNS provider Dyn Inc., which hosts the authoritative DNS for these popular domains. The attack originated from a large number of compromised IoT devices, including Internet-connected cameras, routers and digital video recorders.

Around the world, communications service providers (CSPs) and subscribers were affected by the attack, making it virtually impossible to reach these popular Web sites for several hours. Although CSPs weren't targeted directly, they were still affected since the outages drove additional caching DNS traffic caused by the errors from failed DNS requests. This spike in traffic slowed overall network performance, likely driving up customer support call volumes from unhappy subscribers.

The attacks highlighted the easily overlooked — yet vital — role that DNS plays on the Internet. A lone attacker was able to prevent hundreds of millions of Internet users from accessing their favorite sites by targeting a single managed DNS provider. Given the growth in IoT devices, the scale and frequency of these types of attacks is likely to increase. Without question, CSPs must be prepared for the unfortunate day when their DNS—or one of their subscribers—is the intended target of an attack, so as to preserve both network and brand integrity.

Craig Sprosts, Vice President, Product Management & Strategy at Nominum, writes that afew key

steps CSPs can take to prepare for similar attacks in the future are outlined below.

1. Monitor DNS carefully

The Web site failures during the recent DDoS attack caused a surge in "SERVFAIL" errors as subscriber queries to these popular domains generated error responses. The chart below shows a surge in SERVFAIL errors from the attack, taken from a sample of Nominum CSP customers around the world. The yellow line represents the ration of "SERVFAIL" errors to total responses, which peaked at a remarkable 30 percent + of traffic on the day of the attack.

CSPs must have tools in place to monitor these common errors so they can quickly drill down and see the top clients and domains generating the errors. With proper monitoring and tools, Network Operations can identify root causes within minutes, at which point they can isolate the issue and provide accurate details to call center personnel about the sites affected, as well as to subscribers with misconfigured devices.

2. Design DNS architecture for Internet storms

When evaluating DNS software, network teams tend to look only at queries per second (QPS) as an indication of reliability, but these metrics can be misleading. Instead, network teams must evaluate how the DNS performs on the worst days when traffic patterns are highly unusual. Common DNS implementations have very simple rules that don't differentiate between legitimate and attack traffic. In the case of the latest attack, when the authoritative DNS servers were unable to respond to queries, the querying servers continued to flood the authoritative servers, waiting hopelessly for a response. This overwhelms the DNS server and slows DNS responses to all queries — both legitimate and malicious traffic — creating a major "traffic jam," which can bring the Internet to a halt.

Nominum's Vantio CacheServe, on the other hand, handled these errors smoothly, largely due to its "success-based rate limiting" feature. Success-based rate-limiting automatically detects non-responding authoritative DNS servers and immediately slows queries to these servers, substantially reducing attack traffic to the target sites, preserving the integrity of the network and ensuring the lowest possible latency for all queries.

3. Consider partnering with a secondary authoritative DNS & anti-DDoS vendor

Given the massive scale of attacks taking place today, it is difficult for CSPs to provision enough authoritative DNS capacity to address the biggest attacks on their own. There is now a mature industry with hosted authoritative DNS and anti-DDoS services that can be deployed to complement a service provider's authoritative DNS. Such services can be easily and securely configured to handle queries when the CSP's authoritative service becomes overwhelmed.

4. Enforce security best practices whenever possible

A significant portion of these attacks come from DVRs, webcams and other connected consumer devices, whose poorly configured security credentials allow them to be easily compromised. Any device managed directly by a service provider should follow strict security best practices. Such best practices require highly secure passwords before allowing the device to connect, use secure protocols such as HTTPs whenever possible and design devices to receive automated remote security updates without requiring user action.

5. Prioritize IoT security

There are now billions of connected IoT devices, most of which aren't controlled directly by the CSP, meaning there is only so much a service provider can do to enforce good security best practices. Many of these devices are inexpensive and don't offer strong security protections. In fact, Dyn reported that more than 10 million devices were used in this latest attack against them; additionally, Nominum has been tracking exponential growth in compromised IoT devices since the source code was released in early October.

Unfortunately, Nominum anticipates more IoT-based attacks in the near future. Our Data Science team has been monitoring malicious DNS queries from the Mirai botnet to these same domains and other popular domains for several weeks. While the exact reason for

this activity remains unknown, we suspect it was used as a test for executing larger DNS-based or other types of attacks such as cache poisoning.
DNS is a great place to invest in IoT security since compromised IoT devices are using DNS for legitimate purposes such as checking for software updates and malicious communications, including command and control and DNS-based DDoS attacks.
Last week's attack was a wake-up call that put a spotlight on the importance of DNS, and the impact of IoT-based attacks on the Internet and on CSPs. CSP security and operations teams should use this as an opportunity to evaluate their preparedness for an attack on their DNS, as well as on broader IoT-based attacks that originate on their network. Nominum is investing heavily in this area, designing products that work to prevent malicious attacks on DNS and IoT devices.

▶ There is more information and white papers on this topic here.
— Read more in Data Revelations: Nominum Data Science Security Report (Nominum, Fall 2016).

Detecting malicious Web sites before they do harm

Source: http://www.homelandsecuritynewswire.com/dr20161031-detecting-malicious-web-sites-before-they-do-harm

Oct 31 – **Malicious Web sites promoting scams, distributing malware, and collecting phished credentials pervade the Web.** As quickly as we block or blacklist them, criminals set up new domain names to support their activities. Now a research team including Princeton University computer science professor Nick Feamster and recently graduated Ph.D. student Shuang Hao has developed a technique to make it more difficult to register new domains for nefarious purposes.
Princeton University says that in a paper presented 27 October at the 23rd ACM Conference on Computer and Communications Security, the researchers describe a system called PREDATOR that distinguishes between legitimate and malicious purchasers of new Web sites. In doing so, the system yields important insights into how those two groups behave differently online even before the malicious users have done anything obviously bad or harmful. These early signs of likely evil-doers help security professionals take preemptive measures, instead of waiting for a security threat to surface.
"The intuition has always been that the way that malicious actors use online resources somehow differs fundamentally from the way legitimate actors use them," Feamster explained. "We were looking for those signals: what is it about a domain name that makes it automatically identifiable as a bad domain name?"

Feamster, the acting director of Princeton's Center for Information Technology Policy, will be participating in the upcoming fourth Princeton-Fung Global Forum, which is focused on cybersecurity. The event will be held 20-21 March 2017 in Berlin.
Once a Web site begins to be used for malicious purposes — when it is linked to in spam e-mail campaigns, for instance, or when it installs malicious code on visitors' machines — then defenders can flag it as bad and start blocking it. But by then, the site has already been used for the very kinds of behavior that we want to prevent. PREDATOR, which stands for Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration, gets ahead of the curve.
The researchers' techniques rely on the assumption that malicious users will exhibit registration behavior that differs from those of normal users, such as buying and registering lots of domains at once to take advantage of bulk discounts, so that they can quickly and cheaply adapt when their sites are noticed and blacklisted. Additionally, criminals will often register multiple sites using slight variations on names: changing words like "home" and "homes" or switching word orders in phrases.
By identifying such patterns, Feamster and his collaborators were able to start sifting through the more than 80,000 new domains registered every day to preemptively identify which ones

were most likely to be used for harm.

Testing their results against known blacklisted Web sites, they found that PREDATOR detected 70 percent of malicious Web sites based solely on information known at the time those domains were first registered. The false positive rate of the PREDATOR system, or rate of legitimate sites that were incorrectly identified as malicious by the tool, was only 0.35 percent.

Being able to detect malicious sites at the moment of registration, before they're being used, can have multiple security benefits, Feamster said. Those sites can be blocked sooner, making it difficult to use them to cause as much harm — or, indeed, any harm at all if the operators are not permitted to purchase them. "PREDATOR can achieve early detection, often days or weeks before existing blacklists, which generally cannot detect domain abuse until an attack is already underway," the authors write in their paper. "The key advantage is to respond promptly for defense and limit the window during which miscreants might profitably use a domain."

Additionally, existing blocking tools, which rely on detecting malicious activity from Web sites and then blocking them, allow criminals to continue purchasing new Web sites. Cutting off the operators of malicious Web sites at the moment of registration prevents this perpetual cat-and-mouse dynamic. This more permanent form of protection against online threats is a rarity in the field of computer security, where adversaries often evade new lines of defense easily, the researchers said.

For the PREDATOR system to help everyday internet users, it will have to be used by existing domain blacklist services, like Spamhaus, that maintain lists of blocked Web sites, or by registrars, like GoDaddy.com, that sell new domain names.

"Part of what we envision is if a registrar is trying to make a decision about whether to register a domain name, then if PREDATOR suggests that domain name might be used for malicious ends, the registrar can at least wait and do more due diligence before it moves forward," Feamster said.

Although the registrars still must manually review domain registration attempts, PREDATOR offers them an effective tool to predict potential abuse. "Prior to work like this, I don't think a registrar would have very easy go-to method for even figuring out if the domains they registered would turn out to be malicious," Feamster said.

— Read more in Shuang Hao et al., "PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration" (DOI: http://dx.doi.org/10.1145/2976749.2978317) (paper presented at the 23rd ACM Conference on Computer and Communications Security, Hofburg Palace, Vienna, Austria, 24-28 October 2016).

Cybersecurity requires better collaboration between private, public sectors

Source: http://www.homelandsecuritynewswire.com/dr20161102-cybersecurity-requires-better-collaboration-between-private-public-sectors

Nov 02 – The U.S. government will always play an important role in cybersecurity, but it lacks the resources fully to defend the private sector in the digital realm, according to a new report from the GW Center for Cyber and Homeland Security.

The report, released Monday, offers a comprehensive assessment of the legal, policy, and technological contexts that surround private sector cybersecurity and active defense measures to improve the U.S. responses to evolving threats.

A key difference between cybersecurity threats and other security threats is the mismatch between public and private capabilities and levels of authority in responding to these threats, the report says. The lack of government resources to defend the private sector from digital threats places businesses on the front lines of the cyber conflict and can put national security, economic vitality, and privacy at risk.

"Given the scale and scope of the cyber threat, the digital equivalent of building higher walls and deeper moats alone is a reactive strategy doomed for failure," said Center for Cyber and Homeland Security

Director Frank Cilluffo. "Businesses cannot simply firewall their way out of this problem and must instead have greater leeway to more proactively respond to cyber threats."

GWU notes that the report calls for increased collaboration between the public and private sectors to use available tools more effectively to disrupt and deter cyber threats, noting the collaboration between the private sector and policymakers is long overdue.

The report recommends:

- Developing procedures for public-private coordination on active defense measures through existing industry-led cooperation.
- Amending the Computer Fraud and Abuse Act and the Cybersecurity Act of 2015 affirmatively to allow low- and medium-impact active defense measures.
- Developing C-suite level operational templates based on risk assessment, industry standards and best practices to integrate into broader cyber strategy and incident response protocols.

GWU says that the report draws on knowledge from an Active Defense Task Force of experts in the public and private sectors who are thought leaders in technology, security, privacy, law, and business. The task force examined current cybersecurity practices commonly found in the private sector and provided case studies that lay out the strengths and weaknesses of such practices in addition to less common, active defense measures.

The aim of the report is to help chart a constructive course forward through the complicated terrains of law, technology and policy as they relate to private sector active defense. The report also dissects the complex web of the legal gray areas of cyber defense that make it difficult for the private sector and policymakers to work together.

The report provides a new definition of active defense that reflects the evolution of cybersecurity capabilities and includes operation that will allow defenders to gather intelligence and policy tools aimed at deterring hacks. With proper balance, the private sector can be a vital player in ensuring the nation's economic and national security, the report finds.

The study differentiates between active defense and "hacking back," which refers to offensive cyber measures that are beyond the scope of what is defined as permissible activity in this report. It also balances the need to enable private sector active defense measures with other important considerations such as the protection of individual liberties, privacy and risks of collateral damage when implementing active defense.

"The framework that we provide in this report offers a sustainable path forward for responsible private sector active defense," said Deputy Director of the GW Center for Cyber and Homeland Security Christian Beckner. "An informed and equipped private sector, supported by this framework, is necessary to improving America's cybersecurity posture moving forward."

— Read more in Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats (GWU, Center for Cyber and Homeland Security, October 2016).

The risk of cyber 9/11 or cyber Pearl Harbor exaggerated

Source: http://www.homelandsecuritynewswire.com/dr20161102-the-risk-of-cyber-9-11-or-cyber-pearl-harbor-exaggerated-expert

Nov 02 – Prof. Jon Lindsay of the Munk School of Global Affairs at the University of Toronto, discussed cybersecurity and the future of warfare at an event organized by the Mario Einaudi Center for International Studies at Cornell University.

Lindsay, addressing the implications of cybersecurity threats for the stability of international world order, acknowledged that states will find it difficult to maintain cybersecurity in an increasingly porous and congested cyberspace, but said that cyber-experts exaggerate the threat to essential state infrastructures.

"Deception [using cyber security] on a large scale are very rare, because you need to manage all the information channels … these kinds of large scale gambits are more likely to fail," he said. "When we focus on the low end of the attacks, we do see a great deal … **But when we look at the most worrisome scenarios, cyber 9/11, digital Pearl Harbor,**

we see strategic disincentives and operational barriers in actually getting something done."

Lindsay said that exclusively focusing on the technological weaknesses of state infrastructure leads to an over-evaluation of cyberthreat. He urged a more nuanced approach to cybersecurity, one which considers "technological plausibility along with political utility."

"It's not enough to say, 'Given the present infrastructure with these vulnerabilities, X might happen.' That's the realm of technological plausibility," he said. "You need to be able to take that plausibility and be able to weaponize it. There's got to be a story of what kind of political or economic gain is going to be realized from that particular attack."

Lindsay noted the attribution of cyberattacks to highlight the importance of considering technology and politics side by side. While it can be difficult to determine who is responsible for a cyberattack, he said technological vulnerability does not translate into political weakness, because attacks do not necessarily threaten the most critical government infrastructure.

"Ironically, while attribution is difficult in the low end, where people are not motivated to work through vast number of potential attackers, at the high end there is a limited number of perpetrators and more motivation on the political side to do it," he said. "And if attribution is feasible, so is deterrence."

Lindsay also said that an interdisciplinary approach to cybersecurity creates a paradox. The current international order, which disincentivizes the use of military force, has encouraged states to instead wage low intensity, high frequency conflicts in cyberspace. In other words, the historical stability and peacefulness of the current international order can be said to have contributed to the proliferation of cyberattacks.

"The increasing perplexity and danger of the cyber domain is happening in a world … that is becoming less dangerous, where war is less likely," he said. "The half empty glass part is, yes, cyber security is dangerous. It is going to be a problem difficult to solve. But the half full part is, it's predicated on things going pretty well on a civilizational time scale. We got conflict looking more complex but not necessarily more dangerous."

The SCADA Syndrome: Addressing the Threats and Challenges of Protecting Critical Infrastructure

Source: http://www.hstoday.us/single-article/special-the-scada-syndrome-addressing-the-threats-and-challenges-of-protecting-critical-infrastructure/fef5be3ead21dc8df0d8b6cff3c5cb6d.html

Oct 31 – **SCADA (supervisory control and data acquisition) is a true battleground in the war against cyber attacks.** It's become one of those innocuous acronyms for what is now the most crucial of analytic tools, the ones which keep countries and businesses secure by ensuring our nuclear power plants, our airports and our weapons caches continue to run smoothly.

A SCADA network is a type of industrial control system (ICS), which uses multiple hardware and software elements to perform key functions in the delivery of essential services and commodities in the real world, such as water and power, transportation services, and other utilities. SCADA systems are distinguished from other ICS systems by their size and magnitude; typically, a SCADA system spans multiple sites over very long distances. While SCADA systems have many applications, they are especially popular in the utility industry because they allow workers to control and monitor utility equipment from remote locations.

SCADA systems use a series of codes to relay messages from sensors to central terminals when a fault occurs, and ensure the fault is analyzed immediately.

Many of these SCADA systems were built decades ago when cyber security was not really an issue. They were built to maximize functionality, efficiency, and safety – but not cybersecurity.

There is also widespread myths that SCADA networks do not "need" information security because they already enjoy "security through obscurity." But here's the fear factor - they are being hacked with increasing regularity. In essence, whoever hacks a SCADA system literally can have their finger on the button of the nukes.

Many SCADA systems use proprietary interfaces and specialized protocols that aren't widely known, but obscurity does not equal security. All it takes is one malicious insider – or unsuspecting victim – to hand system credentials and protocols over to a hacker. An attack on a Ukraine power company's SCADA network last December, which took 30 substations offline and left 230,000 residents without power for hours, had its genesis in a spear-phishing attack targeting system administrators and IT employees at power companies throughout Ukraine.

Other SCADA systems are not connected to the Internet and use private physical network links or satellite connections to transmit data. It is widely believed that this "segregation" provides immunity to breaches, but no twenty-first century network is truly completely segregated and private networks and satellite connections can be breached. Even if a particular system is normally not connected to any network, it will still require software updates and need to perform data transfers using a flash drive or a non-permanent modem connection, both of which can be compromised by hackers using social engineering techniques, such as installing malware on a thumb drive and leaving it for an unsuspecting employee to find.

The Stuxnet virus, which ravaged Iran's Natanz nuclear facility and was believed to have been developed and unleashed by the governments of the US and Israel, entered the system through an infected thumb drive planted by a malicious insider: an Iranian double agent. And, in March, a federal indictment accused a team of hackers with ties to the Iranian government of using a cable modem to breach the SCADA system at the Bowman Avenue Dam in New York State.

To successfully defend against SCADA attacks, organizations need a complete solution that does not adhere to the outdated belief that just physically isolating systems and buying technology will make a facility safe. Since 90 percent of system breaches, including the Stuxnet attack on Iran and the Ukraine power system breach, are the result of hackers stealing legitimate login credentials, a two-fold approach that combines technological defenses with rigorous internal cyber security training and procedures is necessary. **A few suggestions to consider:**

- Identify all connections to the SCADA system, including LANs, WANs, satellite links, and modems. Disconnect any devices that do not need to be connected. Likewise, identify and disconnect any unused or unnecessary services, such as automated meter reading and remote billing systems, email services, and remote maintenance. Isolation is not information security, but limiting the number of source points hackers have access to is a good starting point.
- Implement intrusion detection systems and establish 24-hour-a-day incident monitoring and response. Incident response procedures must be in place to ensure that security personnel are available to respond to breaches at any time of the day or night.
- Perform system backups and have a robust disaster recovery plan. The organization must have a disaster recovery plan that can handle any type of emergency, including a cyber terrorist

attack, and get systems back online as soon as possible.
- Establish strict, specific cybersecurity rules and protocol for employees. An organization's employees can be the weak link in an otherwise secure environment, which is why hackers commonly use social engineering techniques as a first entry point into a system.

Because it is necessary to monitor SCADA networks and respond to incidents 24/7, many organizations choose to outsource part or all of their SCADA network security to a managed security services provider, or MSSP. In addition to providing a level of expertise that may not be available in-house, MSSPs have the specialized hardware and software needed to monitor the entire SCADA network, from the RTU/PLC layer down to the HMI, as well as 24-hour staffing to immediately investigate unusual activity and respond to incidents.

The *Wall Street Journal* reported in March 2015 that if only nine of the country's approximate 55,000 electrical substations went down – whether from mechanical issues or malicious attack – the nation would experience a coast-to-coast blackout. Providers of utilities and other critical infrastructure services must act now to protect not only themselves and their customers but also the entire country from a terrorist attack. It's a war that must be fought daily, but one that can be won.

***Mike Baker** is founder and Principal at Mosaic451, a bespoke cybersecurity service provider and consultancy with specific expertise in building, operating and defending some of the most highly-secure networks in North America.*

Pro-ISIS Hacking Group Threatens to Target the West With A Destructive 'Electronic Virus' Soon

Source: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-threatens-to-target-the-west-with-a-destructive-electronic-virus-soon/

Nov 04 – On October 31, 2016, pro-ISIS hacking group Hack Kabir announced on its Twitter account that it will soon launch a destructive electronic virus on the "infidel West." The group, also known as AnonTerror, stated that Kabir Hacker had "eliminated" members of the Syrian Electronic army and sent their information to the "wolves," meaning ISIS fighters. The group further threatened to launch a major attack on Russia's government website.

The full text of this report is available to MEMRI Jihad and Terrorism Threat Monitor subscribers.

Want to spy on the boss? Try this phone-mast-in-an-HP printer

Source: http://www.theregister.co.uk/2016/11/02/printer_spy_box/

An engineer has shown how you can sneak a tiny cellphone base station into an innocuous office printer. The idea is the brainchild of New Zealand's Julian Oliver, who was inspired by the Stingray cellphone snooping technology now in widespread use by the cops and FBI. He was looking to see how such tech could be hidden and what better to do this in than the humble office printer.

The system uses an HP Laserjet 1320, which is both in widespread use around the world and also has a good amount of free space inside the casing. Oliver then added a RaspberryPi 3 and BladeRF x40 software-defined radio, along with a couple of antennas and some cabling to link into the printer's power supply. The whole kit forms a tiny cellphone mast that masquerades as a legit tower.

"The Raspberry Pi 3 was chosen after failed attempts to acheive stable YateBTS performance on the Intel Edison (tiny - would've saved space!), Beaglebone Black and even an I-MX6 Marsboard," he said. "Unlike the antiquated OpenBTS, YateBTS really seems to need those extra cores, otherwise ignoring accelerators like NEON on the Cortex A8/9 platforms."

The printer still does its main job of spewing out documents, but now – using code Oliver developed and published – it also acts as a fake cellphone tower that detects and communicates with nearby phones and sends them SMS messages.

The computer also harvests the IMEI number for the phones and whatever else information it collects from the devices when they automatically connect to it. He rigged it up so that this information is printed out, and the phone will also receive a random call that plays them Stevie Wonder's *I Just Called To Say I Love You*.

While the printer in its current design doesn't have malicious intent, it would be easy to set it up to pump out SMS malware or possibly perform man-in-the-middle attacks against unsuspecting workers. It would also make a very useful surveillance device.

Cybersecurity to bolster safe transfer of hazardous liquids at ports

Source:http://www.homelandsecuritynewswire.com/dr20161115-cybersecurity-to-bolster-safe-transfer-of-hazardous-liquids-at-ports

Nov 15 – The U.S. Coast Guard (USCG) oversees approximately 800 waterfront facilities that, among other activities, transfer hazardous liquids between marine vessels and land-based pipelines, tanks or vehicles. These "maritime

bulk liquid transfers" increasingly rely on computers to operate valves and pumps, monitor sensors, and perform many other vital safety and security functions. This makes the whole system more vulnerable to cybersecurity issues ranging from malware to human error, and is the reason behind a new voluntary cybersecurity guide for the industry.

Maritime bulk liquid transfer processes are part of a complex and sophisticated supply chain of the oil and natural gas industry that brings together various types of organizations and systems. The USCG and industry representatives joined with the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), to develop a profile to help those organizations assess their cybersecurity risk.

NIST says that the document is the first in a series of planned profiles that will help maritime industry organizations make the most of the voluntary *Framework for Improving Critical Infrastructure Cybersecurity*, published by NIST in February 2014. The profile pulls into one document recommended cybersecurity safeguards to provide a starting point for organizations to review and adapt their risk management processes, and it describes a desired minimum state of cybersecurity.

"Working with the U.S. Coast Guard to engage the oil and natural gas industry in creating this profile is a prime example of the collaboration that takes place at the NCCoE," said Don Tobin, NIST senior security engineer. "Organizations working in this critical mission area can leverage the profile to develop a plan to reach their desired state of cybersecurity."

The profile is aimed at those involved in overseeing, developing, implementing and managing the cybersecurity components of maritime bulk liquid transfer. This includes operations executives, risk managers, cybersecurity professionals and vessel operators. It recognizes a need for security controls on operational technologies such as storage, transfer, pressure and vapor monitoring, emergency response and spill mitigation systems. The profile provides guidance on appropriate security controls for information technology to reliably support these increasingly connected processes, as well as traditional ones such as human resources, training and business communication.

"These facilities face inherent cybersecurity vulnerabilities and the U.S. Coast Guard hopes this profile will assist organizations with mitigating them, and provide a long-term process for developing an internal cyber risk management program," said Lt. Josephine Long, a marine safety expert in the Critical Infrastructure Branch within the USCG's Office of Port & Facility Compliance.

The profile can help individual companies clarify how cybersecurity fits into their mission priorities and how best to allocate resources to secure their information and operational systems. Benefits also include improved understanding of the environment to foster consistent analysis of cybersecurity risks, and alignment of industry and USCG cybersecurity priorities.

According to Long, the USCG plans to work with the NCCoE to build additional profiles that will cover mobile offshore drilling operations, passenger vessel and terminal operations.

The NCCoE works with industry, academia and other government agencies to address real-world cybersecurity problems with existing technology.

The *Maritime Bulk Liquid Transfer Cybersecurity Framework Profile* is available on the USCG Web site, and more information is available in a blog post on Maritime Commons.

The Future of Extremism: Artificial Intelligence and Synthetic Biology Will Transform Terrorism

Source: http://futurism.com/the-future-of-extremism-artificial-intelligence-and-synthetic-biology-will-transform-terrorism/

There weren't many people who had heard of bioterrorism before 9/11. But shortly after the September 11th terrorist attacks, a wave of anthrax mailings diverted the attention of the public towards a new weapon in the arsenal of terrorists—bioterrorism. A US federal prosecutor found that an army biological researcher was responsible for mailing the

anthrax-laced letters, which killed 5 and sickened 15 people in 2001. The cases generated huge media attention, and the fear of a new kind of terrorist warfare was arising.
However, as with every media hype, the one about bioterrorism disappeared quickly.
But looking toward the future, I believe that we may not be paying as much attention to it as we should. Although it may be scary, we have to prepare ourselves for the worst. It is the only way we can be prepared to mitigate the damages of any harmful abuses if (and when) they arise.
Ultimately, this means investing in research related to the policy and governance surrounding a host of new technologies. Here is where some of the most pressing concern lies.

Augmenting Intelligence

In the future, brain implants will be able to empower humans with superpowers with the help of chips that allow us to hear a conversation from across a room, give us the ability to see in the dark, let us control moods, restore our memories, or "download" skills like in *The Matrix* movie trilogy. However, implantable neuro-devices might also be used as weapons in the hands of the wrong people.
When we have implanted microchips in our brains to enhance cognitive capabilities, it could serve as a platform for hackers to cause damage from a distance. They could turn on functionalities, turn off devices, or bombard the brain with random harmful messages. They could even control what you are thinking and, by extension, how you act.
Fortunately, there are several initiatives that seek to understand exactly how such technologies might work, which could give us the knowledge needed to keep a step ahead.

The Medicine of Tomorrow

As the medical wearable and sensor market starts to truly boom, it is logical to think ahead to what might follow this "wearable revolution." I think that the next step will be insideables, digestables, and digital tattoos.
"Insideables" means devices implanted into the body, generally just under the skin. In fact, there are people who already have such implants, which they can use to open up a laptop, a smartphone, or even the garage door. "Digestables" are pills or tiny gadgets that can be swallowed, which could do things like track digestion and the absorption of drugs. "Digital tattoos" are tattoos with "smart" capabilities. They might easily measure *all* of our health parameters and vital signs.
All of these teeny-tiny devices might be misused—some could be used to infuse lethal drugs into a organism or strip a person of their privacy. That is the reason why it is of the utmost importance to pay attention to the security aspect of these devices. They can be vulnerable to attacks, and our life will (quite literally) depend on the safety precautions of the company developing the sensors. That may not sound too comforting—putting your health in the hands of a company—but microchip implants are heavily regulated in the US, and so we are already looking ahead to issues surrounding this advancement.

The Tiny Robot Revolution

In the future, nanoscale robots could live in our bloodstream or in our eyes and prevent any diseases by alerting the patient (or doctor) when a condition is about to develop. They could interact with our organs and measure *every* health parameter, intervening when needed.
Nanobots are so tiny that it is almost impossible to discover when someone, for example, puts one into your glass and you swallow it. Some people are afraid that, by using such tiny devices, total surveillance would become feasible. There also might be the possibility there to utilize nanobots to deliver toxic or even lethal drugs to the organs.
By researching ways to identify when these nanobots are being utilized now, we could potentially prevent their misuse in the future.

Robotic Strides

Robots are quickly becoming ubiquitous in a number of industries. Surgical robots constitute one of the most important strains. For example, the da Vinci Surgical System enables a surgeon to operate with enhanced vision, precision, and control. However, these types of robots have certain security and privacy indications which are not explored in detail yet. But there are already signs that they should be. Last year, MIT reported that researchers at the University of Washington successfully demonstrated that a cyberattack can be carried out against medical telerobots. Imagine what might happen if a hacker disrupts an operation by disturbing the

communication connection between the robot surgeon and the human giving commands to the robotic scalpel. Proper encryption and authentication cannot foil every kind of attack, but companies need to invest in this now to make sure operations are safe.

Putting Scientific Tools in the Hands of the People

Community labs, such as The Citizen Science Lab in Pittsburgh, are getting more and more popular. The aim of these laboratories is to spark more interest in life sciences in citizens—from small children to pensioners. In these labs, people can (for the most part) work on whatever they want, from producing a drug to using genome editing. However, such DIY biotech projects raise a lot of safety concerns.

As the price of lab equipment goes down, the elements of scientific experimentation become affordable to a wide variety of people….of course, that includes criminals and terrorists, who might use such labs to create drugs, biomaterials for weapons use, or harmful synthetic organisms.

The US Food and Drug Administration held a workshop in 2016 in order to better understand 3D printing and bioprinting and how these technologies might be used and abused. Similar conversations are currently taking place about CRISPR gene editing; however, these need to be accelerated and expanded to include the entire community of experts, researchers, and innovators.

A New Kind of Intelligence

Artifical intelligence is expanding at an amazing rate, and of course, the biggest fear isn't that AI will take our jobs…it's that they will take our lives.

The concern is that AI systems will become so sophisticated that they will work better than the human brain, and after a while, they will take control. In fact, Stephen Hawking even said that the development of full artificial intelligence could spell the end of the human race. Elon Musk had similar feelings, and in response, launched OpenAI, a non-profit research company that aims to carefully promote and develop AI that follow human ethics. The organization ultimately plans to make its patents and research open to the public.

By far the scariest scenario involves hacking the AI systems that we will have. Imagine an autonomous car that is no longer under your control. At all. Or imagine a military drone that is no longer controlled by the military.

That is surely a world that we must avoid, and so we must take action to prevent these things now.

Images that fool computer vision raise security concerns

By Bill Steele (Cornell Chronicle)

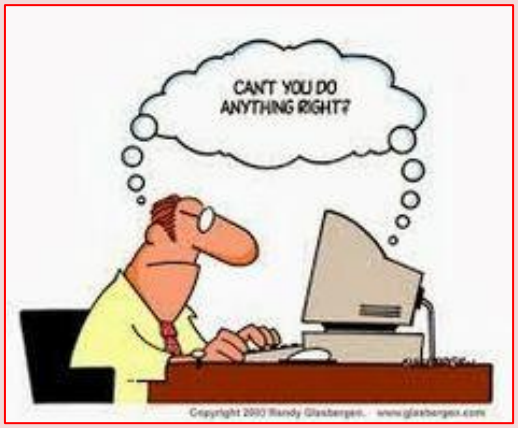
Source: http://www.homelandsecuritynewswire.com/dr20161117-images-that-fool-computer-vision-raise-security-concerns

Nov 17 – **Computers are learning to recognize objects with near-human ability. But Cornell researchers have found that computers, like humans, can be fooled by optical illusions, which raises security concerns and opens new avenues for research in computer vision.**

Cornell graduate student Jason Yosinski and colleagues at the University of Wyoming Evolving Artificial Intelligence Laboratory have created **images that look to humans like white noise or random geometric patterns but which computers identify with great confidence as common objects.** They will report their work at the IEEE Computer Vision and Pattern Recognition conference in Boston 7-12 June.

"We think our results are important for two reasons," said Yosinski. "**First**, they highlight the extent to which computer vision systems based on modern supervised machine learning may be fooled, which has security implications in many areas. **Second,** the methods used in the paper provide an important debugging tool to discover exactly which artifacts the networks are learning."

Computers can be trained to recognize images by showing them photos of objects along with the name of the object. From



many different views of the same object the computer assembles a sort of fuzzy model that fits them all and will match a new image of the same object. In recent years, computer scientists have reached a high level of success in image recognition using systems called Deep Neural Networks (DNN) that simulate the synapses in a human brain by increasing the value of a location in memory each time it is activated. "Deep" networks use several layers of simulated neurons to work at several levels of abstraction: One level recognizes that a picture is of a four-legged animal, another that it's a cat, and another narrows it to "Siamese."

But computers don't process images the way humans do, Yosinski said. "We realized that the neural nets did not encode knowledge necessary to produce an image of a fire truck, only the knowledge necessary to tell fire trucks apart from other classes," he explained. Blobs of color and patterns of lines might be enough. For example, the computer might say "school bus" given just yellow and black stripes, or "computer keyboard" for a repeating array of roughly square shapes.

Working in the Cornell Creative Machines lab with Hod Lipson, associate professor of mechanical and aerospace engineering, the researchers "evolved" images with the features a DNN would consider significant. They tested with two widely used DNN systems that have been trained on massive image databases. Starting with a random image, they slowly mutated the images, showing each new version to a DNN. If a new image was identified as a particular class with more certainty than the original, the researchers would discard the old version and continue to mutate the new one. Eventually this produced images that were recognized by the DNN with over 99 percent confidence but were not recognizable to human vision.

"The research shows that it is possible to 'fool' a deep learning system so it learns something that is not true but that you want it to learn," said Fred Schneider, the Samuel B. Eckert Professor of Computer Science and a nationally recognized expert on computer security. "This potentially has the basis for malfeasants to cause automated systems to give carefully crafted wrong answers to certain questions. Many systems on the Web are using deep learning to analyze and draw inferences from large sets of data. DNN might be used by a Web advertiser to decide what ad to show you on Facebook or by an intelligence agency to decide if a particular activity is suspicious."

Malicious Web pages might include fake images to fool image search engines or bypass "safe search" filters, Yosinski noted. Or an apparently abstract image might be accepted by a facial recognition system as an authorized visitor.

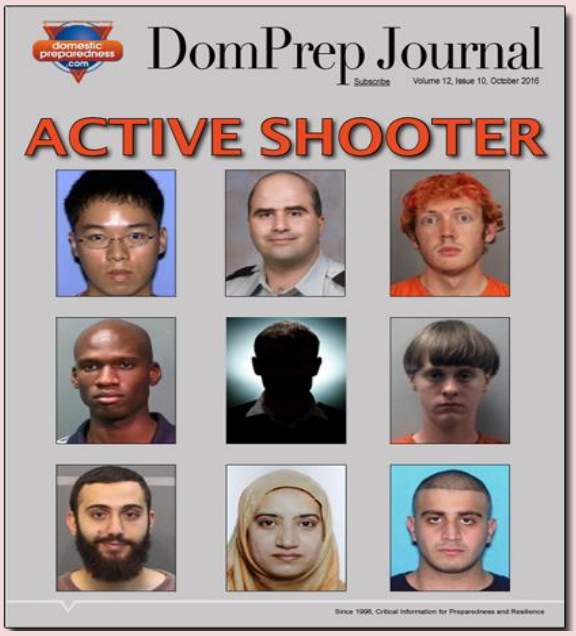
In a further step, the researchers tried "retraining" the DNN by showing it fooling images and labeling them as such. This produced some improvement, but the researchers said that even these new, retrained networks often could be fooled.

"The field of image recognition has been revolutionized in the last few years," Yosinski said. "[Machine learning researchers] now have a lot of stuff that works, but what we don't have, what we still need, is a better understanding of what's really going on inside these neural networks."

Yosinski collaborated with Jeff Clune, assistant professor of computer science at the University of Wyoming, and Wyoming graduate student Anh Nguyen. The research was supported by a NASA Space Technology Research fellowship.

Domesctic Preparedness Journal

Source: http://us8.campaign-archive1.com/



Drills, exercises, trainings, and education can be used in different ways to promote community preparedness and resilience when faced with threats such as active shooters.

Stephen Maloney, Michelle Rosinski, and Anthony Vivino emphasize the importance of first determining realistic threat levels to develop an effective resilience strategy. Once risks and threats are determined, various stakeholders can take steps to prepare and protect their facilities. Kay Goss shares an update on school preparedness efforts for active shooters, whereas Aric Mutchnick addresses liability issues for businesses to consider. Suspicious activity reports as discussed by Jerome Kahan can help thwart some attacks, but citizens must be prepared to respond when an attack does occur. For example, citizens can learn how to stop the bleeding before medical services arrive through programs like the one described by Richard Hunt. Edward Jopeck explains how gunshot technology in buildings can save lives. Peter LaPorte and Thomas Lockwood look at how to close existing vulnerability gaps using various drills and exercises. For any critical incident involving trauma, discussion to promote an understanding of both the citizens' and responders' perspectives can help communities heal faster. Paul Ames shares how this is being done in Cambridge, Massachusetts, to help police officers better serve their communities. Groups such as the International Association of Emergency Managers (IAEM) further such discussions with its Think Tanks, which are facilitated by Richard Serino. IAEM just released an audio recording of its latest discussion on active shooters.

Anyone could potentially face an attacker at some point in his or her life. Minimizing risks and threats before an attack, knowing what to do

during an attack, and promoting resilience after an attack are responsibilities that are shared among all community members.

Calls in Italy for quake-proofing the country's buildings, infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20161027-calls-in-italy-for-quakeproofing-the-country-s-buildings-infrastructure

Oct 27 – More and more Italians are urging the government to invest more funds to make buildings in the country earthquake resistant. Earlier today (Thursday), Italy was dealing with the cost of two quakes which reduced villages in the Apennines to rubble and left thousands homeless.

Some 3,000 were sheltered in community centers, schools, and sports arenas after two tremors struck within two hours of each other on Wednesday.

The *Financial Times* reports that the second quake was measured at 5.9 in magnitude, but the number of casualties was much smaller than the 300 killed two months ago when a 6.0 magnitude earthquake struck central Italy.

The two Wednesday earthquake killed only one person, and nearly 100 were treated for injuries.

"Italy is wounded, but will not be bowed," Matteo Renzi, the prime minister, said. He promised that the homeless would not have to live in tents through the winter months. "I'm optimistic that we can rebuild," he said.

Experts as well as ordinary Italians said the government must allocate more funds on quake-proofing buildings – rather than spend money on headline-grabbing infrastructure projects such as building a suspension bridge across the Strait of Messina to connect the mainland to Sicily.

Renzi revived the suspended bridge proposal last month, saying it would create tens of thousands of jobs. Critics say that the bridge would cost billions and that much of the money would find its way to the pockets of mafia organizations.

"The only big project that this country needs is to make public buildings safe (from earthquakes)," said Paolo Ferrero, of the leftist PRC party. "Renzi should stop blathering on about the Messina Strait bridge and stump up the funds needed to prevent buildings from collapsing in the future."

Ferrero called for 20 billion euros to be allocated to quake-proof vulnerable buildings across the country. Other Italians grumble about the huge amounts of money spent on rescuing migrants in the Mediterranean – money, they say, which should be used to make the country's seismic-prone regions more quake-safe.

The *FT* notes that geologists have been saying that Italy is such seismically active country that the only option is to strengthen buildings to the extent possible and learn to live with the threat.
"The seismic risk has been underestimated, when we should have learnt to live with it. The only thing that can be done is to build safer homes," said Paolo Messina, director of the Institute of Geology at the National Research Center. "When you buy a car, you make sure that it has air bags and good brakes. But when people build or restore houses, they often prefer to save money rather than ensure that they are safe (against earthquakes)," he told *La Repubblica* newspaper.
Scientists say that the area of Italy most at risk from quakes is the Apennine chain of mountains and surrounding valleys, where thousands of towns and villages are located, many with centuries-old houses, churches, convents, towers, castles, and monasteries.
Experts say that quake-proofing all these structures would be daunting and expensive, but that there is no other choice. "We run the risk of having to spend even more money if we don't do that. Building houses that can withstand quakes is the only weapon in our armory," said Messina.
The 6.0 earthquake which struck central Italy on 24 August caused an estimated €4 billion in damage.
Since Wednesday, there have been more than 340 aftershocks, according to the National Institute of Geophysics. **Some of the aftershocks were felt in Rome, but experts examining the Colosseum, Roman Forum, and other historic sites found no damages.**

EDITOR'S COMMENT: Bla, bla, bla… if care was given before the recent earthquakes overall cost would be much-much lesser; now they have to re-build "bombed" villages and fortify those still standing. Always post-active; never pro-active! The nature of humans in all aspects of life…!

Harnessing science to help in emergency response

Source: http://www.homelandsecuritynewswire.com/dr20161031-harnessing-science-to-help-in-emergency-response

Oct 31 – **Four years ago, communities across the East Coast faced Superstorm Sandy, a weather system that claimed more than seventy lives in the United States and caused $65 billion in damages. Earlier this month, Hurricane Matthew devastated Haiti, killing more than a thousand people before turning north to the United States, where it caused another forty-three deaths.**
The NSF says that in an effort to minimize the loss of life in future events, a new partnership between the National Science Foundation (NSF) and the National Oceanic and Atmospheric Administration (NOAA) aims to provide the necessary tools to ensure people respond appropriately to dangerous weather systems. A key part of this work involves understanding how people behave when hazards approach, so emergency services can improve the content and distribution of storm warnings and other communications.
"This collaboration plays to the strengths of each agency. By reviewing a set of exciting new research studies of disaster response and selecting those that show great promise to be turned into tools, NSF and NOAA are working to translate the best new science into meaningful change for the public," said Bob O'Connor, a program manager with NSF's Social, Behavioral, and Economic Sciences Directorate.
Scientific and computing advances have improved forecasting in recent years, advances that have helped expand the science of prediction, preparedness and response.
"Going beyond the science of the forecast and understanding how weather warnings are perceived and how the perception may or may not lead to action is critically important to NOAA as it is our goal not just to predict the weather, but to keep people safe," said John Cortinas, director of the NOAA Office of Weather and Air Quality.
NSF funds basic research on disaster response and preparedness. NOAA, looking to develop useable applications from basic research, will supplement three NSF research projects in order to convert the findings from research on public response to disaster warnings into tools that it and other weather reporting entities can use.
This work is part of an ongoing partnership between NSF and NOAA that has helped bring new science to NOAA forecasters. The partnership also serves as a

model to shorten the path from the best basic science to usable tools.

The three awards, which are supporting five NSF-funded scientists, include:

Collaborative Research: Online Hazard Communication in the Terse Regime

Principal Investigators: Jeannette Sutton, University of Kentucky; Carter Butts, University of California-Irvine. Researchers will use what they have learned about how weather-related risks are communicated through social media to create a tool that can be used by National Weather Service (NWS) forecasters to improve the understanding and reach of their storm-related messages.

Improving Public Response to Weather Warnings

Principal Investigator: Susan Joslyn, the University of Washington.

Researchers will build on previous work that examines how forecast uncertainty can sometimes muddy the waters for people making real-world decisions about risk. This project will result in a tool for NWS forecasters to use when working with local emergency management to make sure uncertainties are conveyed in a way that helps people take appropriate action.

Next Generation, Resilient Warning Systems for Tornadoes and Flash Floods

Principal Investigators: Brenda Philips, University of Massachusetts Amherst; Joseph Trainor, University of Delaware. Researchers will build on previous work that incorporates atmospheric data and human response data to understand public actions in extreme weather events. Scientists will analyze information about NOAA's products and services and make recommendations about steps NOAA can take to collect enough high-quality, relevant data to evaluate and improve their forecast warning systems over time.

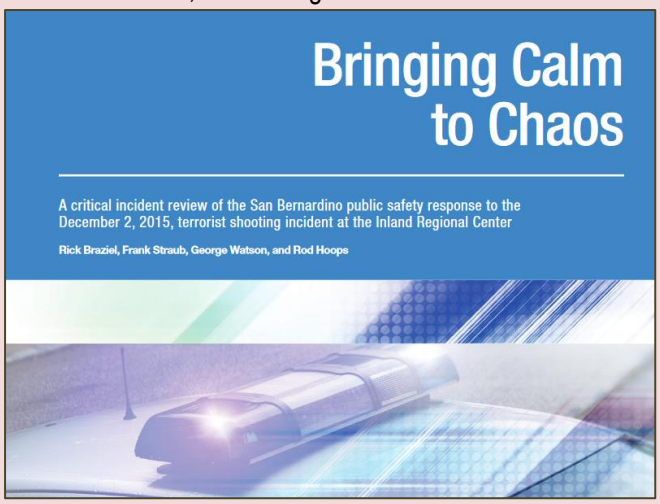
A review of the San Bernadino public safety response to 2015 terrorist shooting incident

By Roger Gomm

Source: https://www.crisis-response.com/comment/blogpost.php?post=294

Sept 23 – **A critical incident review titled *Bringing calm to chaos*, looks at the San Bernardino public safety response to the 2015 terrorist shooting incident at the Inland Regional Centre,** *reports Roger Gomm for* CRJ.

On December 2, 2015, at 10:59hrs, the Inland Regional Centre (IRC) in San Bernardino, California, came under attack. The incident began as what is now known to be two shooters, dressed in all black, entered the IRC, a building in which San Bernardino County Environmental Health Department employees were meeting, and began shooting.



In a matter of minutes, the couple fired more than 100 .223 rounds, before they fled in a rented SUV. The attack led to a midday shootout between the police and Rizwan (male criminal) and his wife Tashfeen Malik (female criminal), as well as a search for a third subject some officers believed had fled the suspects' vehicle (it was later determined that there was not a third suspect). Law enforcement officers killed both assailants on a normally peaceful residential street.

The incident left 22 civilians wounded, 14 civilians dead, and two officers injured. Two days later, after an investigation into the assailants' background and motivation, it was realised that this was a premeditated act of terrorism.

This incident was a fast moving and challenging incident for responding agencies operating in the full glare of the media. The purpose of this Office of Community Oriented Policing Services (COPS Office) Critical Incident Review was to: "Critically, objectively, and

thoroughly examine the public safety response – including preparation and aftermath – to the December 2, 2015, terrorist shooting in San Bernardino."

This review provides a detailed overview of the incident response; lessons learnt to improve responding agencies' policies, procedures, tactics, systems, culture, and relationships; and guidance to other agencies and first responders as they prepare for responses to terrorist, active shooter or other hostile events, or mass casualty incidents.

Some of the key themes include the following:

1. **Build relationships: leader-to-leader, organisation-to-organisation and police-to-community** prior to a critical incident: At both the operational and strategic levels, the responders who were interviewed attributed much of the success of the response to these attacks to the relationships they had built regionally through training and working with others.
2. **Review, study, and apply lessons learnt from critical incident reviews:** Lessons learnt from the Police Foundation review of the Christopher Dorner incident in 2013 contributed to the response to the December terrorist shooting at the IRC.
3. **Regional public safety partners should plan and exercise unified command for complex incidents on a regular basis**. The need for an 'understood' multi-agency incident command structure to manage a marauding terrorist attack or other hostile events would seem obvious but, in reality, the key is regular joint training and implementation during routine events and emergencies.
4. **Conducting regional multi-agency training improves response:** The report highlights the need to ensure that training is inclusive, involving public safety agencies, medical community, legislators, other governmental organisations, faith leaders, mental health providers and others. Training should extend past the initial response into transition to victim extraction and all the way through family notifications.
5. **Prepare and use equipment and technology to keep officers and community members safe and informed.**
6. **Attend to community, victim, and officer wellness**: Active shooter or other hostile events are devastating to a community, to the victims and to the public safety personnel responding to them. It is critical that departments plan and work with mental health, faith, and other partners to accommodate victims and witnesses and provide the necessary welfare resources.

It is worth reflecting on the US State and local law enforcement organisations' structure as there are many, different in size and capability, which emphasises the need for co-operation highlighted above. In 2015/16, San Bernardino Police Department had 248 officers and 173 civilian staff. The terrorist shooting at the IRC and the final shootout between the terrorists and law enforcement occurred within their jurisdiction. Their officers were first on scene and the department, in conjunction with the San Bernardino County Sheriff's Department (which serves 14 of the county's 24 cities and has 3,571 employees) and the Federal Bureau of Investigation (FBI), maintained primary incident command. Such operational understanding does not happen by chance and they should be congratulated.

I would recommend the report to all agencies developing plans for the response to and recover from a marauding terrorist attack or similar incident.

▶▶ **The full report is available in PDF format** here

Roger Gomm *QPM, is Advisor, Trainer, Consultant, Associate Lecturer, Cabinet Office Emergency Planning College, UK and a Member of CRJ's Editorial Advisory Panel*

Be Prepared: Canada engages youth in disaster resilience

Source: http://www.homelandsecuritynewswire.com/dr20161103-be-prepared-canada-engages-youth-in-disaster-resilience

Nov 03 – Large-scale natural disasters have been on the rise worldwide, and while the exact cause is unclear, there is something most scientists, policy-makers, and legislators can all agree with — the increasing global need to invest in disaster preparedness, prevention, and recovery. Canadian experts say they are constantly evaluating and improving Canada's

emergency preparedness and the most effective ways to keep people safe. But some experts are taking a different approach to disaster resiliency: they are engaging youth.

DRDC-RDDC says that in Alberta, a major effort is underway through the Alberta Resilient Communities (ARC) project funded by Alberta Innovates Health Solutions. This project builds on the experiences of children, youth, and their communities in order to inform and strengthen child and youth mental health and enhance disaster resilience in Southern Alberta. It represents an impressive collaborative partnership between academics of the University of Calgary (Dr. Julie Drolet), Mount Royal University (Dr. Caroline McDonald-Harker), and Royal Roads University (Dr. Robin Cox), along with community-based partners from Calgary, High River, and the Foothills region.

"We know that children and youth are often cited as a vulnerable population to disasters because of their dependency on adults and their developmental stage, but we also know that young people are motivated and want to contribute to the conversation around disaster resiliency. They have the capacity, strength, and intelligence to do so," said Dr. Robin Cox, director of ResilienceByDesign Research Lab, professor and program head of the Disaster & Emergency Management (DEM) program at Royal Roads University.

Disaster resilience, according to the UN Office for Disaster Risk Reduction, is the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. The question is: what role can youth play in a world under pressure from environmental degradation, population growth, unsustainable development in hazard-prone areas, and widening social and economic disparities?

"I think youth are more excited about the topic, which brings an added level of passion and a willingness to change things. Being a young person, you see things and think 'That's not the most efficient way of doing that' and look for ways to improve it," said Zachary Cox (no relation to Dr. Cox), 26, one of the learning lab participants.

"Youth bring a citizen voice that is unique based on their age and perspective. They have capabilities that are underutilized. They're often catalysts for change, they're more prone to want to invest in positive social change, because that's their future"

The Canadian Safety and Security Program (CSSP), a federal program led by Defense Research and Development Canada's Centre for Security Science (DRDC CSS), in partnership with Public Safety Canada, supported the project by funding various deliverables, such as work done in the ResilienceByDesign (RbD) research lab. Public Safety Canada also provided support during the scoping phase of the project and during the review of the deliverables.The researchers at the RbD research lab have been engaging with disaster-affected youth from Southern Alberta to explore and contribute to disaster risk reduction, climate action, and community resilience.

The ARC project's focus here in Canada aligns with the goals emphasized by the Sendai Framework for Disaster Risk Reduction, which was adopted at the third United Nations (UN) World Conference in Sendai, Japan, in March 2015. Members of the RbD participated and contributed in Sendai, and continue to work with international partners and collaborators who are also invested in the ways youth can help in disaster resilience and climate change adaptation.

In a series of "learning labs," youth have been developing skills in community research, design thinking and visual storytelling. In the process, they have been generating data, broadening understanding, and developing new ideas to address social-environmental problems. Funding from the CSSP also supported the development of the Resilience Innovation Skills Certificate, which is a youth-centered learning process that builds knowledge and mental capacity for social innovation and resilience.

As noted in the project's final report, research shows that younger people can demonstrate exceptional resilience in the face of disasters. They are creative, motivated, and interested in how they can become resilient themselves and contribute to building resilient families and communities.

"Youth bring a citizen voice that is unique based on their age and perspective. They have capabilities that are underutilized. They're often catalysts for change, they're more prone to want to invest in positive social change, because that's their future," adds Dr. Robin Cox.

As part of the CSSP-funded activities of the project, social media was used to help recruit young participants, who then answered a few questions about demographics and their

extent of disaster exposure, to ensure the study would include a wide variety of people. The eight learning labs are designed to engage youth in the design and testing of methods and practices that promote disaster resilience. From data collection and brainstorming to the creation of solutions and policy outreach, the youth are engaged in every aspect of the process.

The labs involved the participants in community action research, the world of design thinking, generating data, digital storytelling and analysis, and even working on creating prototype solutions to improve community disaster resilience.

After completing these labs, youth will meet with local community organizations, youth groups, researchers, industry, or other stakeholders to pitch ideas for community resilience projects. "They will be able to use their new skills to develop innovative approaches to complex social challenges," DRDC-RDDC says. "The ultimate goal is for the youth to implement these projects in their communities and participate in the evaluation and assessment of their impacts."

#1 The unexpected always happens!

2016 – Fukuoka, Japan (**NOTE**: Fixed one week after!)

Paramedics Provide Safety Net for Regional SWAT

Source: http://www.emergencymgmt.com/safety/Paramedics-provide-safety-net-for-regional-SWAT.html

Nov 02 – Art Culver, manager of Altru Health System's ambulance services, reflected last Friday on some of the various titles used for emergency medical services personnel.

Some of the nuances that differentiate EMS roles can be lost on the public, which in turn can lead to mix-ups. But while EMT is not synonymous with paramedic, there was one name that stood above the others as a true misnomer.

"Just don't call us ambulance drivers," Culver said with a smile.

Given the setting, that'd be an unlikely slip—he was making the distinction while standing alongside a fully equipped Grand Forks Regional SWAT Team truck.

Part of Culver's management role involves overseeing the health system's tactical medics, a crew with two Altru paramedics who work directly alongside SWAT to provide law enforcement with medical support services.

The program is the result of a memorandum of understanding forged between Altru and the Grand Forks Police Department.

Culver's oversight is based in personal experience. He became one of the very first members of the team at its inception in 2003 and remained in the program until 2014.

Culver, who made a career in the U.S. Air Force before returning to civilian life, said medics are trained with all of the weapons used by SWAT but carry none of their own when called into action. What they do get is a bulletproof vest loaded up with a variety of medical gear suited for use in combat situations.

Culver said part of the reason he "jumped on board" at the program's start was the prospect of excitement.

"I wanted maybe the adrenaline rush, of being part of the specialized team," he said.

Later, Culver said his favorite aspect of the job was being ready to lend a hand at a moment's notice.

"I was there to be able to help the team members focus on their jobs," he said. "In the case that they got hurt or someone else got hurt, I was immediately available."

Grand Forks Police Sgt. Travis Benson, SWAT team leader, said the medics are "100 percent part of our team."

"They train with us, they go on activations with us," Benson said. "Anytime that we're on anything, we typically have our medics involved as well."

The presence of the medical team doesn't change the way SWAT does its job, Benson said; in an ideal situation, a tactical medic wouldn't have to step in at all.

Still, Benson said, there's some relief knowing medical services are there if injuries do happen.

Emergency medical treatment is fortunately not a frequent part of SWAT dealings, he said, adding the subjects of SWAT action are usually looked over by medics when the scene is secure.

For the officers themselves, Culver said most injuries occur during training exercises.

Front-line treatment

After spending more than a decade on the team, Culver described the service as enjoyable and said the additional training and experience had made him a better paramedic.

"I learned a lot," he said of his time on the team. "I needed to stay highly skilled to be able to provide the front-line treatment."

Culver estimated about 20 different Altru employees have been on the team over the course of its existence.

Applicants to the program must first meet the more basic job criteria of having relevant certifications and work history and interviewing for the position. The more intense side of the job screening includes a physical agility portion in which candidates must hit their marks in tasks, such as running more than a mile in a certain amount of time, dragging a 200-pound dummy at least 50 yards, and completing timed fence and stair climbs.

Once they make it onto the team, new tactical medics go through SWAT basic training and medics courses. Last summer, Culver said one of the medics attended a specialized course known as Tactical Emergency Medical Support, or TEMS.

Mark Gibbons, a TEMS instructor with the National Tactical Officers Association—a group which represents and supports SWAT units across the country—said he'd been involved in tactical medicine since the late 1980s.

"A lot of the focus, just the scope of what a tactical medic does, continues to evolve with the changing times," Gibbons said.

Modern tactical medics "follow a lot of the military tenets" of medicine, he added, applying some of those standards to the civilian realm. In cases like mass shootings or other events with multiple casualties, Gibbons said tactical medics can be a valuable asset both in initial responses to dangerous scenes and in supporting cases where events are pulled into extended police operations.

Gibbons said a SWAT survey conducted by the association indicated more than half of 254 responding law enforcement agencies with tactical squads included paramedics as part of the team, as of 2013.

TEMS training, he added, is a good way to link medical practices with police action in such a way as to reconcile was can sometimes be "two competing missions."

"There needs to be a good match between the law enforcement tactical thing and the medicine," Gibbons said. "Otherwise, you're pulling the same rope in opposite directions.

The synergy between the two allows for the tactical mission to be successful and to save more lives."

6 Ways to Prep Your Home for Natural Disasters

Source: http://www.emergencymgmt.com/emergency-blogs/disaster-zone/6-ways-to-prep-your-home-for-natural-disasters.html

Nov 07 – This website has some good tips. It is not all-inclusive of the things you can do, but covers the basics. See 6 Ways to Prep Your Home for Natural Disasters.

Prepare Your Home for Some Rockin' and Rollin'
Prevent Flooding in Your Home
Create a Digital Home in the Cloud
Get Your Finances in Order Before Disaster Strikes
Put Together a Natural Disaster Kit
Don't Forget About Your Pets

While all the tips are valid, I suggest adding a minimum of two. First is buying flood insurance if you live in a flood zone. And if you are "just outside of a flood zone," I'd also buy it. Your mortgage company might not require it, but with the types of historic rains we've been having, we are seeing flooding where it has "traditionally" not been seen before. Next, besides fastening the TV, the water heater and the chimney, make sure your older home is fastened to the foundation. Homes built before 1980-90 just might not have had this accomplished.
All the above measures will keep your property protected and the few personal preparedness tips are right on the money too. Remember, if it is a regional-sized disaster like a hurricane or earthquake, having a two-week disaster kit is a better option.

#2 The unexpected always happens!

New Zealand's earthquake (7.8R – 13 Nov 2016)

Powerful earthquake causes substantial destruction in New Zealand

Source: http://www.homelandsecuritynewswire.com/dr20161114-powerful-earthquake-causes-substantial-destruction-in-new-zealand

Nov 14 – A 7.8 magnitude earthquake in New Zealand has killed at least two people and destroyed infrastructure and property. The prime minister said the damage was likely to amount to nearly $1.5 billion. Overnight, aftershocks measuring up to 6.3 magnitude were registered in the area, which in 2011 saw a similar magnitude quake kill 185 people.

New Zealand Prime Minister John Key on Monday said that damage caused by a 7.8 magnitude tremor that struck the country on Sunday could cost New Zealand $1.43 billion.

"It's hard to believe that the bill is going to be less than a couple of billion," Key told Radio New Zealand.

The U.S. Geological Survey placed the quake's epicenter in the South Island's North Canterbury region, saying it occurred at a depth of 14.3 miles.

The BBC reports that in the hours after seismic event, a 6.3 magnitude aftershock caused severe shaking in Christchurch, where a similar magnitude earthquake killed 185 people in 2011. Sunday's quake killed at least two.

The New Zealand authorities said there has been substantial damage to infrastructure and property in some areas.

"I think had there been serious injury or suspected further loss of life then we would have heard about it by now," said Civil Defense Minister Gerry Brownlee.

"It looks as though it's the infrastructure that's the biggest problem, although I don't want to take away from the suffering … and terrible fright so many people have had," he told Radio New Zealand.

Prime Minister Key and Brown flew over the areas affected by the quake to assess the damage. Outside of Kaikoura, a popular tourist destination in the worst-hit region, aerial footage showed train tracks ripped up and tossed some ten meters away.

Key said it may take days to assemble a full picture of the damage. "As we have daylight we can use the military assets that we have to make sure we get a stock-take of the overall damage, but I suspect that will take quite some time to fully understand," the premier said.

The government said it would appoint a senior official to oversee reconstruction in the aftermath of the quake.

Using drones, insect biobots to map disaster areas

Source: http://www.homelandsecuritynewswire.com/dr20161118-using-drones-insect-biobots-to-map-disaster-areas

Nov 18 – **Researchers at North Carolina State University have developed a combination of software and hardware that will allow them to use unmanned aerial vehicles (UAVs) and insect cyborgs, or biobots, to map large, unfamiliar areas – such as collapsed buildings after a disaster.**

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

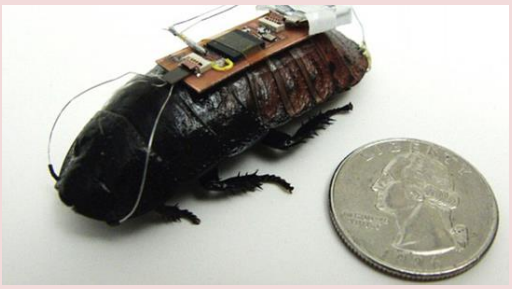
"Using remote-control technology, we would restrict the movement of the biobots to a defined area," Lobaton says. "That area would be defined by proximity to a beacon on a UAV. For example, the biobots may be prevented from going more than twenty meters from the UAV."

NCSU says that 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.

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 then stitches the new map to the previous one. 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.

"This has utility for areas – like collapsed buildings – 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."

Co-lead author Alper Bozkurt, an associate professor of electrical and computer engineering at NC State, has previously developed functional cockroach biobots.



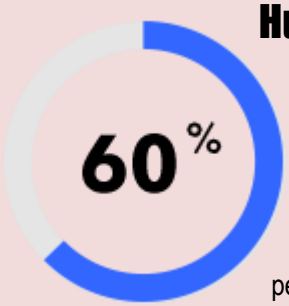
However, to test their new mapping technology, the research team relied on inch-and-a-half-long robots that simulate cockroach behavior.

In their experiment, researchers released these robots into a maze-like space, with the effect of the UAV beacon emulated using an overhead camera and a physical boundary attached to a moving cart. The cart was moved as the robots mapped the area (see video from the experiment here).

"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.

"The next step is to replicate these experiments using biobots, which we're excited about."

— Read more in Alireza Dirafzoon et al., "A framework for mapping with biobotic insect networks: From local to global maps," Robotics and Autonomous Systems (11 November 2016) and "Geometric Learning and Topological Inference with Biobotic Networks," IEEE Transactions on Signal and Information Processing over Networks (28 October 2016).



Human, economic costs of disasters underestimated by up to 60 percent

Source: http://www.homelandsecuritynewswire.com/dr20161122-human-economic-costs-of-disasters-underestimated-by-up-to-60-percent

Nov 22 – The impact of extreme natural disasters is equivalent to a global $520 billion loss in annual consumption, and forces some twenty-six million people into poverty each year, a new report from the World Bank and the

Global Facility for Disaster Reduction and Recovery (GFDRR) reveals.

"Severe climate shocks threaten to roll back decades of progress against poverty,"said World Bank Group President Jim Yong Kim. "Storms, floods, and droughts have dire human and economic consequences, with poor people often paying the heaviest price. Building resilience to disasters not only makes economic sense, it is a moral imperative."

The World Bank says that the report, *Unbreakable: Building the Resilience of the Poor in the Face of Natural Disasters*, warns that the combined human and economic impacts of extreme weather on poverty are far more devastating than previously understood.

In all of the 117 countries studied, the effect on well-being, measured in terms of lost consumption, is found to be larger than asset losses. Because disaster losses disproportionately affect poor people, who have a limited ability to cope with them, the report estimates that impact on well-being in these countries is equivalent to consumption losses of about $520 billion a year. This outstrips all other estimates by as much as 60 percent.

With the climate summit, COP22, underway, the report's findings underscore the urgency for climate-smart policies that better protect the most vulnerable. Poor people are typically more exposed to natural hazards, losing more as a share of their wealth and are often unable to draw on support from family, friends, financial systems, or governments.

Unbreakable uses a new method of measuring disaster damages, factoring in the unequal burden of natural disasters on the poor. Myanmar's 2008 Cyclone Nargis, for example, forced up to half of the country's poor farmers to sell off assets including land, to relieve the debt burden following the cyclone. Economic and social repercussions of Nargis will be felt for generations.

The report assesses, for the first time, the benefits of resilience-building interventions in the countries studied. These include early warning systems, improved access to personal banking, insurance policies, and social protection systems (like cash transfers and public works programs) that could help people better respond to and recover from shocks. It finds that these measures combined would help countries and communities save $100 billion a year and reduce the overall impact of disasters on well-being by 20 percent.

"Countries are enduring a growing number of unexpected shocks as a result of climate change,"said Stephane Hallegatte, a GFDRR lead economist, who led preparation of the report. "Poor people need social and financial protection from disasters that cannot be avoided. With risk policies in place that we know to be effective, we have the opportunity to prevent millions of people from falling into poverty."

Efforts to build poor people's resilience are already gaining ground, the report shows. For example, Kenya's social protection system provided additional resources to vulnerable farmers well before the 2015 drought, helping them prepare for and mitigate its impacts. And in Pakistan, after record-breaking floods in 2010, the government created a rapid-response cash grant program that supported recovery efforts of an estimated eight million people, lifting many from near-certain poverty.

— Read more in Stephane Hallegatte et al., *Unbreakable: Building the Resilience of the Poor in the Face of Natural Disasters. Climate Change and Development* (Washington, D.C.: World Bank, 2017)

Japan's latest tsunami reaction shows lessons learned from previous disasters

By James Goff

Source: http://www.homelandsecuritynewswire.com/dr20161122-japan-s-latest-tsunami-reaction-shows-lessons-learned-from-previous-disasters

Nov 22 – Parts of Japan were on tsunami alert today following a magnitude 6.9 earthquake off the east coast of the country.

This was the first real test for Japan since the 2011 earthquake which led to a deadly tsunami. The destruction led to a meltdown at the Fukushima nuclear power plant.

Japan's latest tsunami Paul Somerville, from Risk Frontiers at Macquarie University, said this latest earthquake was caused by a normal fault associated with faults in and around the Japan trench subduction zone.

The seafloor moved and a small tsunami was generated, largely because this was a much smaller earthquake than 2011, about 40 times smaller, and it released about 250 times less energy.

Having said that, the type of tsunami it produced was pretty much the same, but with wave heights certainly not expected to exceed 3.0 meters and actually appearing to not exceed about 1.5 m in the end.

Be prepared

This was the kind of tsunami that Japan is used to and is prepared for, but with the earthquake occurring close to the Fukushima nuclear power plant and with the world watching to see how they responded, this was to a certain extent a trial by media.

The lessons learned from 2011 saw higher seawalls, more effective public education and evacuation protocols, a beefed-up response from the nuclear industry and so on, but would it pass the test?

In a sense, this was the perfect tsunami to test everybody – the expected wave heights were on the cusp of being potentially catastrophic if a seawall failed or people did not heed the warnings.

The good news is that Japan came through this with flying colors. It wasn't long after the earthquake hit that the tsunami warnings were later downgraded.

Undoubtedly there will have been one or two glitches, but the tsunami was managed well by a country that has experienced more of these events that any of us would ever like to contemplate. **Japan accounts for about 20 percent of the world's earthquakes of magnitude 6 or greater, and many of these generate tsunamis.**

Waiting for the next one

We were all right to be nervous, there has been a lot happening in and around the Pacific Ring of Fire lately. But it's comforting to know Japan can at least cope with these smaller incidents. As can probably most of the other countries sitting on the edge of the Ring of Fire. After all, Chile had a big one in 2010 and Samoa in 2009.

But a question mark must remain over countries such as Australia. Tsunamis are not really something we worry about too much, but they do affect us from time to time.

If we judge our response by what happened following the tsunami warning for the 2010 Chilean event, then quite frankly we fail dismally. Hundreds of people rushed down to areas like Bondi Beach to see any waves.

It is not the fault of the warning system, but rather our ability (the public) to treat these warnings with respect.

We can undoubtedly expect more quakes around Japan and all parts of the Pacific Ring of Fire. The enduring question is always, where will it happen and how big will it be?

Another quake hits New Zealand

As I write we have just had another reasonably large earthquake off the SE corner of the North Island of New Zealand.

Yes, this is probably associated with all of the activity that has happened around Kaikoura since last week's earthquake.

Is this building up to something? Possibly. On the other hand, it is winding down a bit for now? Possibly too.

What we can be sure of is that there will most definitely be more large devastating earthquakes and tsunamis. Many of these will be associated with the Pacific Ring of Fire, but not all of them.

How we manage, prepare, and adapt for such events will show whether we have learned from the previous disasters experienced by other countries or whether we see them as some type of reality TV show that could never happen here.

James Goff *is Honorary Professor of Tsunami Research, PANGEA Research Centre, UNSW Australia, UNSW Australia.*

Worrisome milestone: Atmospheric CO_2 levels reach 400 parts per million in 2015

Source: http://www.homelandsecuritynewswire.com/dr20161025-worrisome-milestone-atmospheric-co2-levels-reach-400-parts-per-million-in-2015

Oct 25 – Globally averaged concentration of carbon dioxide in the atmosphere reached the symbolic and significant milestone of 400 parts per million for the first time in 2015 and surged again to new records in 2016 on the back of the very powerful El Niño event, according to the World Meteorological Organization's (WMO) annual Greenhouse Gas Bulletin.

CO_2 levels had previously reached the 400 ppm barrier for certain months of the year and in certain locations but never before on a global average basis for the entire year.

The longest-established greenhouse gas monitoring station at Mauna Loa, Hawaii, predicts that CO_2 concentrations will stay above 400 ppm for the whole of 2016 and not dip below that level for many generations.

WMO says that the growth spurt in CO_2 was fueled by the El Niño event, which started in 2015 and had a strong impact well into 2016. This triggered droughts in tropical regions and reduced the capacity of "sinks" like forests, vegetation, and the oceans to absorb CO_2. These sinks currently absorb about half of CO_2 emissions but there is a risk that they may become saturated, which would increase the fraction of emitted carbon dioxide which stays in the atmosphere, according to the Greenhouse Gas Bulletin.

Between 1990 and 2015 there was a 37 percent increase in radiative forcing — the warming effect on our climate — because of long-lived greenhouse gases such as carbon dioxide, methane and nitrous oxide (N_2O) from industrial, agricultural and domestic activities.

"The year 2015 ushered in a new era of optimism and climate action with the Paris climate change agreement. But it will also make history as marking a new era of climate change reality with record high greenhouse gas concentrations," said WMO Secretary-General Petteri Taalas. "The El Niño event has disappeared. Climate change has not."

"The recent agreement in Kigali to amend the so-called Montreal Protocol and phase out hydrofluorocarbons, which act as strong greenhouse gases, is good news. WMO salutes the commitment of the international community to meaningful climate action," said Taalas.

"But the real elephant in the room is carbon dioxide, which remains in the atmosphere for thousands of years and in the oceans for even longer. Without tackling CO_2 emissions, we cannot tackle climate change and keep temperature increases to below 2°C above the pre-industrial era. It is therefore of the utmost importance that the Paris Agreement does indeed enter into force well ahead of schedule on 4 November and that we fast-track its implementation." he said.

WMO says it is working with partners toward an Integrated Global Greenhouse Gas Information System to provide information that can help nations to track the progress toward implementation of their national emission pledges, improve national emission reporting and inform additional mitigation actions. This system builds on the long-term experience of WMO in greenhouse gas observations and atmospheric modelling.

WMO is also striving to improve weather and climate services for the renewable energy sector and to support the Green Economy and sustainable development. To optimize the use of solar, wind and hydropower production, new types of weather services are needed.

Highlights of Greenhouse Gas Bulletin

The WMO Greenhouse Gas Bulletin reports on atmospheric concentrations of greenhouse gases. Emissions represent what goes into the atmosphere. Concentrations represent what remains in the atmosphere after the complex system of interactions between the atmosphere, biosphere, cryosphere, and the oceans. About a quarter of the total emissions is taken up by the oceans and another quarter by the biosphere, reducing in this way the amount of CO_2 in the atmosphere.

The Greenhouse Gas Bulletin provides a scientific base for decision-making. WMO released it ahead of the UN climate change

negotiations in Marrakech, Morocco, to be held 7–18 November 2016.

- ***Carbon dioxide (CO_2)*** accounted for about 65 percent of radiative forcing by long-lived greenhouse gases. The pre-industrial level of about 278 ppm represented a balance between the atmosphere, the oceans and the biosphere. Human activities such as the burning of fossil fuels has altered the natural balance and in 2015, globally averaged levels were 144 percent of pre-industrial levels. In 2015, global annual average concentration of CO_2 concentrations reached 400.0 ppm. The increase of CO_2 from 2014 to 2015 was larger than the previous year and the average over the previous ten years. In addition to reducing the capacity of vegetation to absorb CO_2 the powerful El Niño also led to an increase in CO_2 emissions from forest fires. According to the Global Fire Emission Database, CO_2 emissions in Equatorial Asia – where there were serious forest fires in Indonesia in August-September 2015 - were more than twice as high as the 1997-2015 average.
- ***Methane (CH_4)*** is the second most important long-lived greenhouse gas and contributes to about 17 percent of radiative forcing. Approximately 40 percent of methane is emitted into the atmosphere by natural sources (for example, wetlands and termites), and about 60 percent comes from human activities like cattle breeding, rice agriculture, fossil fuel exploitation, landfills and biomass burning. Atmospheric methane reached a new high of about 1845 parts per billion (ppb) in 2015 and is now 256 percent of the pre-industrial level.
- ***Nitrous oxide (N_2O)*** is emitted into the atmosphere from both natural (about 60 percent) and anthropogenic sources (approximately 40 percent), including oceans, soil, biomass burning, fertilizer use, and various industrial processes. Its atmospheric concentration in 2015 was about 328 parts per billion. This is 121 percent of pre-industrial levels. It also plays an important role in the destruction of the stratospheric ozone layer which protects us from the harmful ultraviolet rays of the sun. It accounts for about 6 percent of radiative forcing by long-lived greenhouse gases.
- ***Other long-lived greenhouse gases.*** Sulphur hexafluoride is a potent long-lived greenhouse gas. It is produced by the chemical industry, mainly as an electrical insulator in power distribution equipment. Atmospheric levels are about twice the level observed in the mid-1990s. Ozone-depleting chlorofluorocarbons (CFCs), together with minor halogenated gases, contribute about 12 percent to radiative forcing by long-lived greenhouse gases. While CFCs and most halons are decreasing, some hydrochlorofluorocarbons (HCFCs) and hydrofluorocarbons (HFCs), which are also potent greenhouse gases, are increasing at relatively rapid rates, although they are still low in abundance.

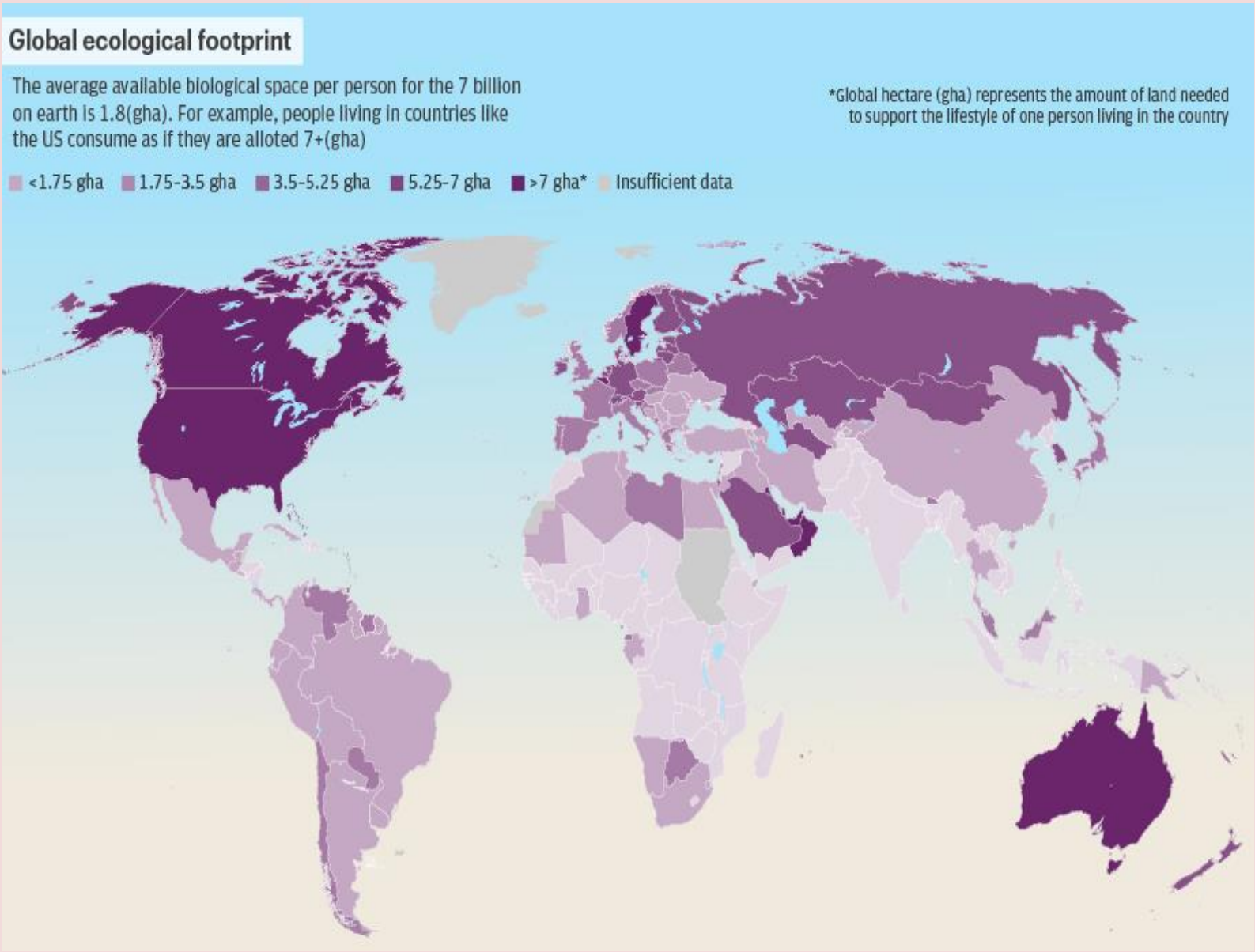
The WMO Global Atmosphere Watch Program coordinates systematic observations and analysis of greenhouse gases and other trace species. Fifty one countries contributed data for the Greenhouse Gas Bulletin. Measurement data are reported by participating countries and archived and distributed by the World Data Center for Greenhouse Gases (WDCGG) at the Japan Meteorological Agency.

WMO has produced three new animations to support the launch of the WMO Greenhouse Gas Bulletin 2015 and promote a new concept for monitoring greenhouse gas emissions, sources, and sinks. The animation on The Carbon Cycle provides basic background about rising atmospheric levels of greenhouse gases. Measuring National Emissions and Monitoring the Atmosphere to Reduce urban Greenhouse Gas Emissions describe how high-resolution monitoring of the atmosphere can now be used more accurately to measure GHG emissions in order to support decision-making.

End of the world as we know it is just ahead

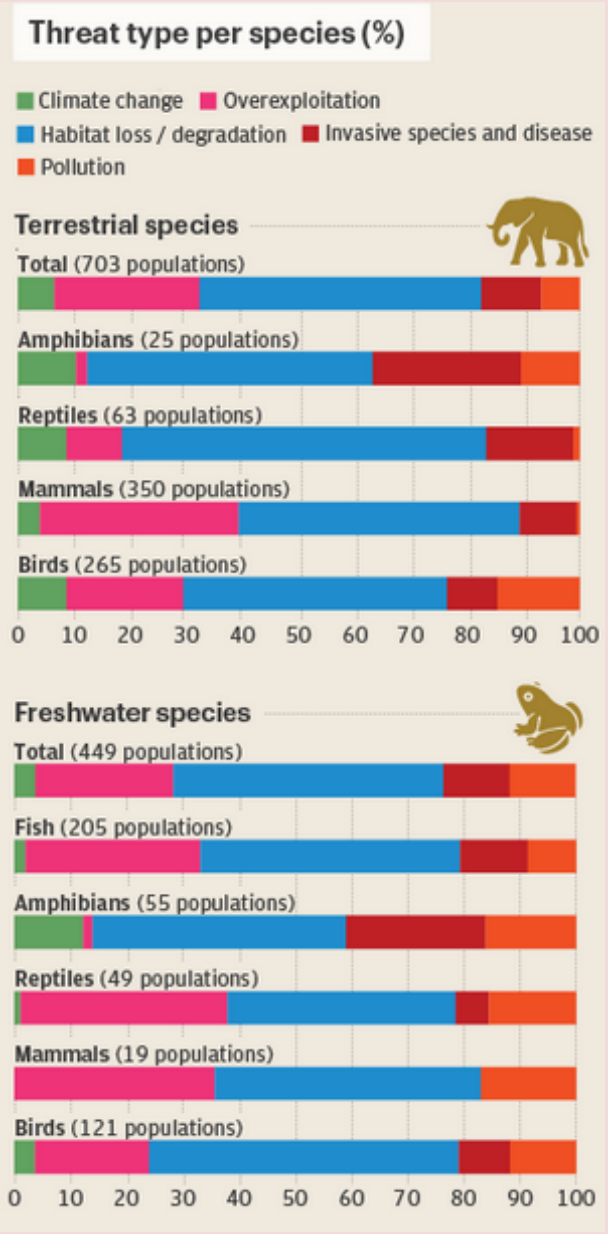
Source 1: http://www.thenational.ae/uae/environment/end-of-the-world-as-we-know-it-is-just-ahead#full
Source 2: http://www.thenational.ae/uae/environment/the-slow-death-of-planet-earth---graphic

Nov 10 – Mass extinction of species, how to boost economic growth without harming the planet and the effects of mass agriculture are all issues to be addressed at the **Cop 22 summit.**
The meeting in Morocco, which began this week, follows last year's Paris Agreement, where 196 countries committed to reducing global warming to less than 2°C.
One of the major discussion points is that the Earth is heading towards a sixth mass extinction – the worst spate of species dying off since the dinosaurs 65 million years ago.
According to the World Wildlife Fund's Living Planet Report, the extinction could result in a 67 per cent decline in wild vertebrate populations by 2020.
Scientists are beginning to understand how humans rely on the biodiversity of species, and the more wildlife that becomes extinct could threaten human development.



That development, according to the report, is beginning to take its toll and a need for a "great transition," towards an ecologically sustainable future, is at hand.
The report states that the world has moved from the Holocene era, which began about 12,000 years ago as the human populations expanded, to the Anthropocene era, when for the first time a single species – humans – has a greater effect on the Earth more than natural processes.
"During the Anthropocene [era], our climate has changed more rapidly, oceans are acidifying and entire biomes are disappearing – all at a rate measurable during a single human lifetime," the report said.

The results of global warming are beginning to affect modern society and alter the lives of millions.



The report said there is a correlation between natural disasters, social and economic pressures and food and water insecurity with an increasingly strained environment.

Conflicts over water security increased by four-fold increase in the last decade and, according to the Pacific Institute environment think tank, are expected to be one of the major causes of global conflict in the next 20 years.

The Living Planet Index, which monitors biodiversity abundance levels based on 3,700 species, showed a decline of 56 per cent since 1970. The loss of life is mostly attributed to habitat loss, over-exploitation and climate change, a subject addressed in Morocco.

Tanzeed Alam, climate and energy director at the Emirates Wildlife Society-World Wildlife Fund, hoped Cop 22 would address this and other issues.

"Through Cop 22, we hope to see the UAE ramp up its level of ambition and encourage others from the region to come to the table, as current global pledges are insufficient to limit warming to 1.5 degrees," he said.

"We also want to see a more coordinated approach to make ambitious targets and measures more effective action."

Another way to measure human pressures on the planet is by measuring the human ecological footprint.

It has been estimated that the current demand requires the capabilities of 1.6 our earths to sustain the strain placed on resources.

The footprint of higher income countries far outweighs that of lower-to-middle income countries, another topic to be addressed at Cop 22.

The Living Planet Report suggested that using GDP as a measure of well-being and the pursuit of economic growth on an already burdened planet without regard to ecological effects is no longer viable.

The consequence of global warming resulting from decades of pursuit of growth in western countries was harming the planet, especially for developing countries, which have fewer means to cope with these changes.

Tosi Mpanu-Mpanu, chairman of the Least Developed Countries group, an intergovernmental body of the 48 countries most at risk from climate change, said he hoped Cop 22 would work to enact "fair and ambitious action".

"We must build upon the foundations set in Paris to construct robust rules to support the agreement's implementation," he said.

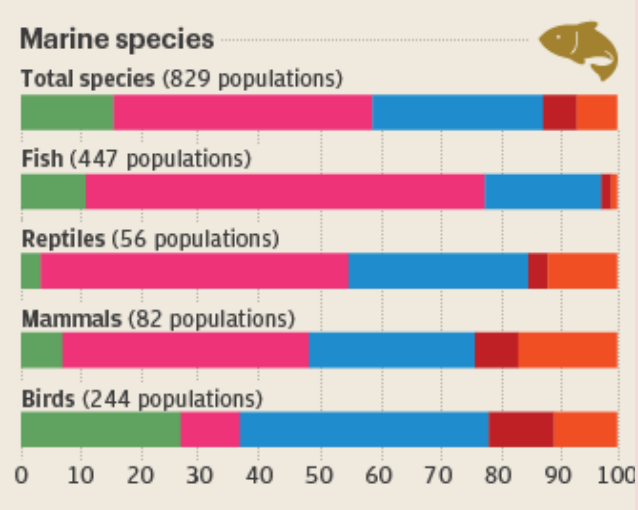
During Cop 21, Mr Mpanu-Mpanu and the G77, a United Nations coalition of developing nations, were fighting the issue of burden-sharing, where they said that the responsibility falls mostly on developed nations.

Their argument that developed nations are more responsible for the damage to the planet, as the US, China and the European Union countries account for more than half of global greenhouse gas emissions.

According to the Global Footprint Network, consumption patterns in high-income countries result in disproportional demands on Earth's renewable resources, often at the expense of elsewhere in the world.

Cop 22 will try to deal with this issue but also make sure developing nations do not commit the same mistakes western countries made during the industrial revolution when they were oblivious to the effects of climate change.

"Historically, we have a burden to help the poorest countries plan for that transition," said Jonathan Porritt, founder and director of Forum for the Future, a non-profit sustainable business organisation.
"That means we're going to [need] billions of dollars to make what for some of them is going to be a painful transition.



"The more we argue about this, the more we sound mean-minded, and I often get quite angry about that."
The changes to the environment are also leading to disasters that take lives, such as the super-typhoons that killed thousands in Philippines and the 2013 Pakistan floods that affected 20 million people.
Aside from natural disasters, the World Health Organisation predicted that between 2030 and 2050, climate change is expected to cause approximately 250,000 additional deaths per year, from malnutrition, malaria, diarrhoea and heat stress.
Mr Porritt was optimistic that resolutions could be found at Cop 22 to stave off these developments.
"Having witnessed many international treaties for 40 years, what has happened with Paris and the follow-up is astonishing. The speed with which countries have moved to ratify is unprecedented. It demonstrates the level of political leadership," he said.
He said Cop 22 was interesting because it would also look at agriculture as a source of emissions, as well as industry.
"Up now insufficient attention has been paid to land – agriculture, forestry, protection of critical ecosystems," he said.
"If you look at the total picture for climate change, these land-based issues are even more important than some of the energy-related issues," he said. "Yet we continue to farm such that billions of CO2 is being released. In Marrakech, there is a lot more focused on this issue."
Food production is one of the primary causes of climate change and biodiversity loss, as our consumption habits have shaped the unsustainable nature of agricultural practices around the world.
According to the Food and Agriculture Organisation of the UN, agriculture occupies about 34 per cent of the total land area on the planet and roughly half of the habitable surface. Of this space, approximately a third is used to produce animal feed and another 50 per cent is used for pasture for animals.
Almost 80 per cent of agriculture land is directly allocated to the production of animal protein, yet animal and dairy products only provide about 17 per cent of calories consumed by humans.
This process accounts for 25 to 30 per cent of greenhouse gas emissions, and, with the developing world growing richer and more populated, demand for animal protein is only growing.
As such, Cop 22 will address this issue. Consumption patterns of humans have been shaped by this demand, as mass production grows the price of meat goes down. Hence, governments are being urged to consider limiting consumption habits of their populations.
Other issues of habitat loss will be discussed, with the aim of creating law-abiding associations between countries that they must share responsibility for the decline of global biodiversity.
With Cop 22 having begun and with the Paris Agreement in full effect, its time to see just how willing countries are to protect the environment, not as a favour, but as a fundamental need for the continuation of human life.

Addressing the risk of an ecological breakdown

Source: http://www.homelandsecuritynewswire.com/dr20161114-addressing-the-risk-of-an-ecological-breakdown

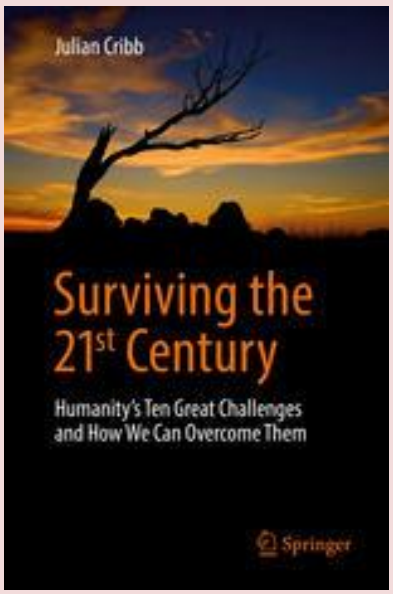
Nov 14 – In *Surviving the 21st Century*, Julian Cribb says that **"Our combined actions may be leading to a gross ecological breakdown that will strike humanity harder than anything in our experience."** The author and science writer notes that, "In the past week alone has come news that global populations of fish, birds, mammals, amphibians,

and reptiles declined by 58 percent between 1970 and 2012. From 20-30 percent of known species now appear at risk of extinction."

"This is an extermination of life on Earth without precedent. The human impact is on track to exceed the catastrophe that took out the dinosaurs.

"Many people don't realize it, but our own fate is completely bound up with these other creatures, plants, and organisms we heedlessly destroy. They provide the clean air and water, the food, the nutrient recycling, the de-toxing, the medications, the clothing and timber that we ourselves need for survival.

"Humans are now engaged in demolishing our own home, brick by brick. Every dollar we spend on food or material goods sends a tiny, almost-imperceptible signal down long industrial and market chains to accelerate the devastation.



"Together those signals are causing the very systems we ourselves need for survival to break down."

Springer Publishers notes that that a recent study by Princeton University found oxygen levels in the Earth's atmosphere have fallen by 0.1 percent in the past 100 years, probably due to land clearing, ocean acidification, and burning of fossil fuels. "Though it is still a small signal, it is another indicator of our ability to disrupt the Earth's life-support system," Cribb says.

The world is currently burning enough fossil fuels to raise its temperature by 4-5 degrees Celsius by 2100 — an event that will probably prove unsurvivable for the majority of large wild animals, and most humans too. "Yet we're still arguing about whether its real and what we should do," he adds.

"Today humanity is facing ten huge existential threats, all of our own making. The good news is that we have the brains and the technologies to solve them – and to prosper from their solution.

"However we currently lack the collective will, the ability to co-operate, and the institutions to save ourselves. That is a worry."

Drawing on the world's leading scientific thinkers, *Surviving the 21st Century* identifies systemic solutions for all of the ten major threats facing humanity, and actions which we must take both as a species and as individuals.

"This is absolutely a book about solutions – and opportunities. It is about hope – though a hope that is well-founded, on fact and science, not simply on belief, ignorance, or wishful thinking. It's about understanding and facing up to the things which imperil out future, so that we can overcome them," Cribb says.

In the book he argues that by moving food production back into cities, using advance technologies and recycling of water and nutrients, humanity can re-wild 24 million square kilometers of the Earth's surface. This would help to end the "sixth extinction" now taking place as well as locking up huge amounts of carbon causing climate change. It would create new jobs and new industries for both urban and rural populations.

Climate, not conflict, explains extreme "Middle East Dust Bowl"

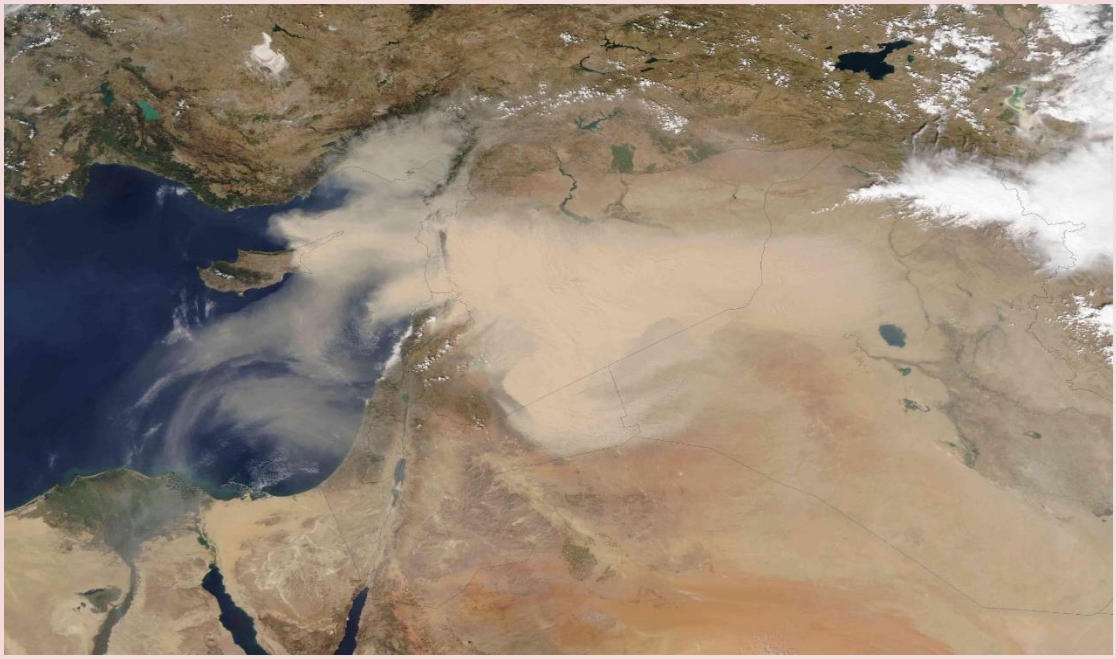
Source: http://www.homelandsecuritynewswire.com/dr20161117-climate-not-conflict-explains-extreme-middle-east-dust-bowl

Nov 17 – **Climate change, not ongoing regional conflict, was the cause of a severe dust storm that enveloped much of the Middle East and the Mediterranean last September,** according to new research published in *Environmental Research Letters*.

The storm, labeled by some media outlets as the **"Middle-Eastern Dust Bowl," affected Syria, Lebanon, Turkey, and Cyprus,** leading to scores of people being hospitalized, ports being closed, flights being cancelled, and large portions of the affected countries and eastern Mediterranean Sea being covered in an unprecedented haze.

Anthony Parolari, assistant professor of environmental engineering at Marquette University and a former

postdoctoral research associate in civil and environmental engineering at Duke University's Nicholas School of the Environment and Pratt School of Engineering, led the new study.



Gabriel G. Katul, the Theodore S. Coile Professor of Hydrology and Micrometeorology at Duke's Nicholas School of the Environment, co-authored the study along with researchers at Boston University, Princeton University and Israel's Institute of Soil, Water and Environmental Sciences.

Duke notes that at the time of the storm, several news stories blamed conflict-associated changes in regional land cover – including the widespread abandonment and reduced irrigation of agricultural lands and increased military vehicle traffic over unpaved surfaces – for the extreme dust and historic haze.

Parolari, Katul, and their team, however, find that rare meteorological conditions, including extreme heat and drought, coupled with cyclonic winds typical in the region during late summer, were more likely the cause.

"The Middle East is a notable hotspot for dust storms during summer, and these are usually associated with the Shamal – winds from the north – and seasonal cyclones," Parolari says. "We ran meteorological simulations that showed historically unprecedented aridity, or dryness, in the region during the summer of 2015 combined with these winds to play a key role in the severity of the storm."

The extremely hot and dry conditions occurring in the region increased the amount of dust that could be eroded by the storm, he explains. An unusual wind reversal at low levels immediately followed the storm, picking up this eroded dust and spreading it west into the Mediterranean.

Studies of surface air temperature, humidity, and wind speeds measured at the Har Kanaan weather station in northern Israel strengthened the team's assessment, Parolari says. The studies showed that the summer of 2015 was among the driest and hottest in twenty years, including the period from 2007 to 2010 when the region was gripped with a long-term drought. This extreme heat and aridity led to soil becoming less cohesive, making it more likely for cyclonic winds to dislodge large dust particles and transport them long distances in the atmosphere.

Studies of vegetative cover in the region over the last fifteen years also added weight to the team's finding that climate, not conflict, was to blame. These studies revealed that despite the abandonment of some farmlands due to escalating military conflict, the extent of vegetative cover in 2015 was nearly double the region's average from 2007 to 2010, and was also greater than the 2001-2007 pre-drought years in many areas. Areas experiencing recent vegetation decline were relatively scarce – meaning the abandonment of farmlands due to conflict was unlikely to be the reason for the massive dust plume.

"While climate, land use and conflict all remain key elements of a complex human-environment relationship that has been playing

out in the Middle East as far back as 4,000 years ago following the collapse of the Akkadian empire, the so-called 'Middle-Eastern Dust Bowl,' appears to be explained by climate, not conflict and abandonment of agricultural land," Parolari says.

— Read more in Anthony J. Parolari et al., "Climate, not conflict, explains extreme Middle East dust storm," Environmental Research Letters 11, no. 11 (8 November 2016).

2015 Indonesian fires exposed 69 million to "killer haze"

Source: http://www.homelandsecuritynewswire.com/dr20161117-2015-indonesian-fires-exposed-69-million-to-killer-haze

Nov 17 – **A new study, published today in *Scientific Reports*, gives the most accurate picture yet of the impact on human health of the wildfires which ripped through forest and peatland in Equatorial Asia during the autumn of 2015.**

The study used detailed observations of the haze from Singapore and Indonesia. Analyzing hourly air quality data from a model at a resolution of 10km – where all previous studies have looked at daily levels at a much lower resolution - the team was able to show that a quarter of the population of Malaysia, Singapore and Indonesia was exposed to unhealthy air quality conditions between September and October 2015.

NCL says that the study estimates that between 6,150 and 17,270 premature deaths occurred as a direct result of the polluted haze. The research team – involving academics from theUnited Kingdom, the United States, Singapore, and Malaysia – said the study confirmed the extent of this public health crisis.

Lead author Dr. Paola Crippa, from Newcastle University said: "**Our study showed that 69 million people living in Malaysia, Singapore, and Indonesia were exposed to unhealthy air quality conditions during the time of the fires – that's more than a quarter of the local population.**

"The wildfires of 2015 were the worst we've seen for almost two decades as a result of global climate change, land use changes, and deforestation. The extremely dry conditions in that region mean that these are likely to become more common events in the future, unless concerted action is taken to prevent fires.

"Our study estimated that between **6,150 and 17,270 premature deaths** occurred due to breathing in the polluted air over that short two month period. To put this into perspective, we estimate that around 1 in 6,000 people exposed to the polluted haze from these fires

died as a result. The uncertainty in these estimates is mostly due to the lack of medical studies on exposure from extreme air pollution in the area."

Ten times the recommended limit of $PM_{2.5}$

Performing numerical simulations on the Indiana University high performance computing resources, the team analysed the levels of particulate matter in the air – $PM_{2.5}$ – during the two months of the fires.

WHO air quality guidelines state that levels of $PM_{2.5}$ should not exceed 25 µg/m³ in a 24 hour period.

Dr. Christine Wiedinmyer, from the National Center for Atmospheric Research in Colorado, said: "Exposure to particulate pollution was substantially greater in autumn 2015 than in other recent years. This is due to the large particulate matter emissions from fires in this region in 2015."

During the two month period, levels of $PM_{2.5}$ – the most dangerous of these tiny toxic particles – were on average above 70 µg/m³ with peaks reaching 300 µg/m³ in densely populated areas such as Singapore.

Professor Dominick Spracklen, a co-author of the study based at the University of Leeds, explained:

"In most of the United Kingdom, levels of $PM_{2.5}$ are usually below 10 µg/m³ and we would consider a serious pollution episode to be where concentrations rose to above 30 µg/m³. During these fires, Singapore experienced levels of pollution ten times higher. It is hard for us in the United Kingdom to imagine air pollution as bad as that experienced across much of Indonesia and Singapore last autumn.

"**If large fires occurred every year, repeatedly exposing the local population to polluted air, the number of deaths would rise substantially - to as many as 75,000.** Our findings are consistent with a recent estimate of the number of deaths that occurred due to long-term exposure to air pollution from these fires."

The team say it is imperative that action is taken to prevent forest fires and killer haze events in the future. Deforestation and drainage of peatlands makes for very susceptible conditions for fire and new efforts are needed to re-wet peatlands and reduce further deforestation in this region.

— Read more in Paola Crippa et al., "Population exposure to hazardous air quality due to the 2015 fires in Equatorial Asia," Scientific Reports 6, article number 37074 (16 November 2016).

Water resources for developing countries

Source: http://www.homelandsecuritynewswire.com/dr20161118-water-resources-for-developing-countries

Nov 18 – **Water experts believe by 2050 almost half of the world's population will live in countries with a chronic water shortage. The shortfall is the result of population growth, which leads to a greater demand for food, increased pollution, and climate instability.** At the Ben-Gurion University of the Negev's (BGU)'s Zuckerberg Institute for Water Research, eighty scientists and 250 graduate students are working on ways to tackle the problem using cutting-edge science in partnership with academics around the world.

Israeli water experts believe by 2050 almost half of the world's population will live in countries with a chronic water shortage.

According to Prof. Noam Weisbrod, director of Ben-Gurion University of the Negev's (BGU)'s Zuckerberg Institute for Water Research, the shortfall is the result of population growth, which leads to a greater demand for food, increased pollution, and climate instability.

The American Associates, Ben Gurion University of the Negev (AABGU) says that Weisbrod and his team of eighty scientists and 250 graduate students are working on ways to tackle the problem using cutting-edge science in partnership with academics around the world.

"Not everything can be about novel research," Weisbrod says. It is also about educating a new generation of water experts and scientists.

Seven years ago, Weisbrod established a yearlong course called "Rural Water Development" to further educate students working on graduate degrees about such global problems. In the past few years, he has brought student groups to villages in rural areas of Ethiopia, Zambia, and Uganda.

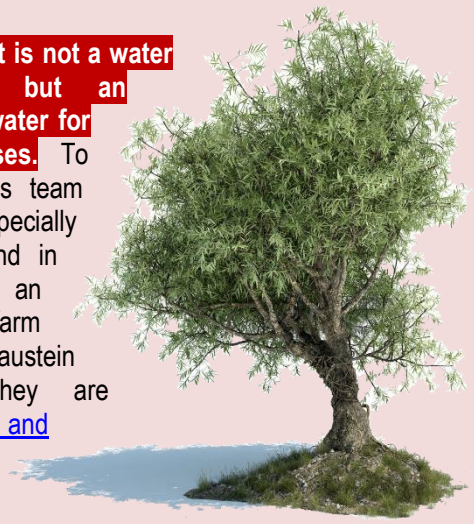
In each locale, the students work with locals and a cadre of non-governmental organizations to identify their water sources and test water quality. Projects range from drilling wells with local materials to building storage tanks that collect rainwater and installing bio-sand filters to reduce contamination.

"The students research the water challenges of wherever they will be traveling and determine the low-tech solutions they will implement when they get there," Weisbrod says.

In Ethiopia, for example, students drilled boreholes to provide drinking water and installed low-tech water pumps. In Uganda, they built a rain catchment system near school bathrooms, allowing children to wash their hands after going to the toilet.

Professor Emeritus Pedro Berliner, former director of BGU's Jacob Blaustein Institutes for Desert Research, is also addressing water issues. He has spent the last twenty-five years working on projects for third-world countries, and estimates that BGU spends as much as a few million dollars per year on these projects.

"The point here is that desertification — the process by which fertile land becomes desert, typically as a result of drought, deforestation, or inappropriate agricultural techniques — is a real problem in third-world countries," he explains.



In African drylands, it is not a water shortage problem but an inability to capture water for food and other uses. To combat this, Berliner's team established specially prepared plots of land in Wadi Mashash, an experimental farm operated by the Blaustein Institutes. There they are growing olive trees and crops between the rows, which helps trap flood water.

"This technique allows us to produce higher yields using the same amount of water or less water," Berliner says. The knowledge gained is shared with developing countries.

"By helping people in these areas, we are helping avoid massive migration [to overpopulated urban areas]."