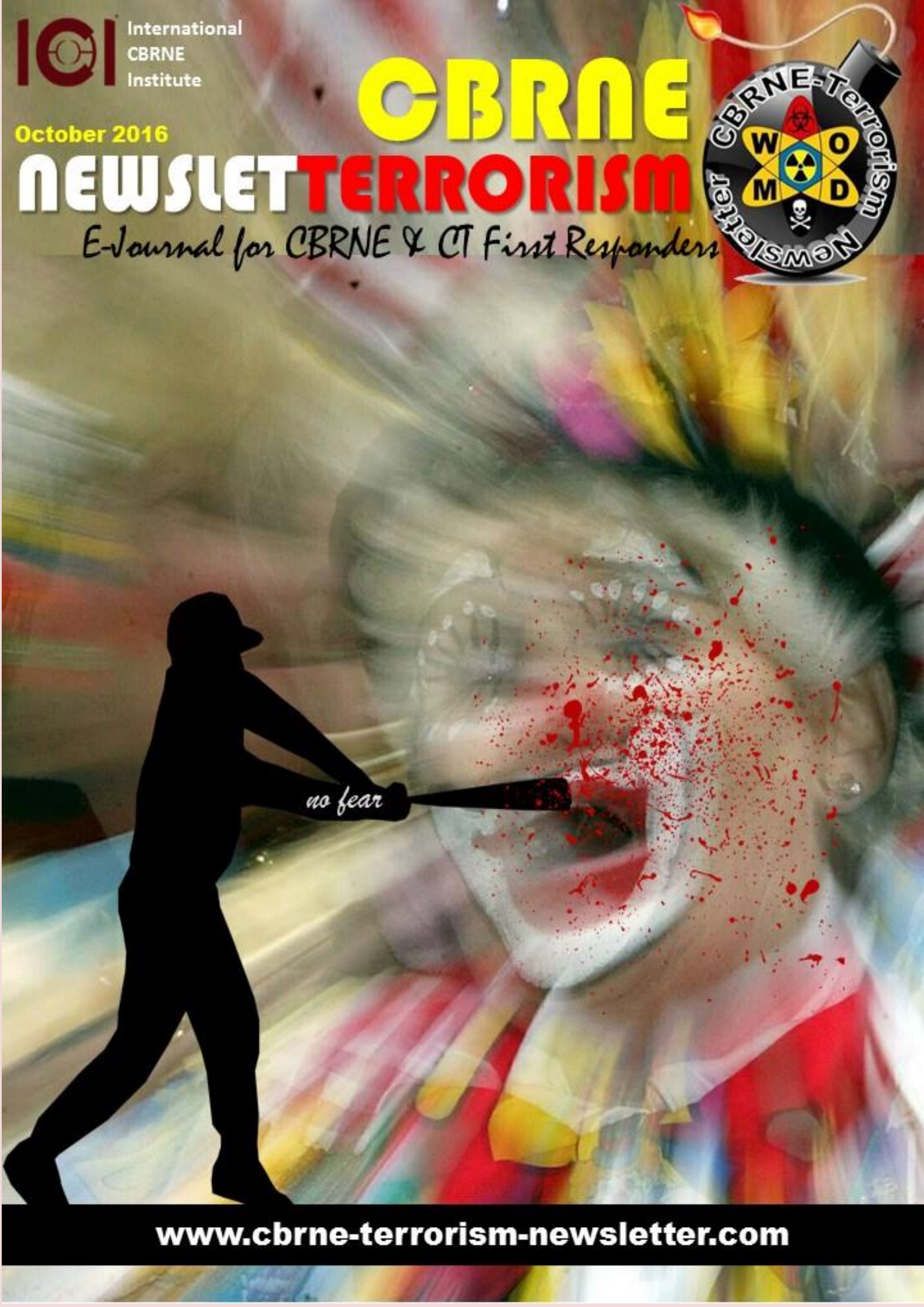
International CBRNE Institute

CBRNE NEWSLETTER TERRORISM

October 2016

E-Journal for CBRNE & CT First Responders



www.cbrne-terrorism-newsletter.com

Tsai to visit Orchid Island to discuss nuclear waste storage

Source: http://focustaiwan.tw/news/aipl/201608140014.aspx

Aug 14 – President Tsai Ing-wen is scheduled to visit Taiwan's offshore Orchid Island on Monday to discuss the issue of nuclear waste storage with the local people, the Presidential Office said Sunday.

The president will meet with a senior member of the indigenous Tao tribe and visit a kindergarten. She will also attend a forum during which she will address such issues as nuclear waste storage and garbage disposal on the island, the office said.

President Tsai Ing-wen, (second right), visits the nuclear waste storage field in 2011 before she took office

On Aug. 1, Tsai issued a formal apology on behalf of the government to Taiwan's indigenous people for the discrimination and neglect they have suffered over the past 400 years.

In her apology, the president said she will direct relevant agencies to present an investigative report on the decision-making process of nuclear waste storage on the island.

Before finding a permanent solution for the nuclear waste, Tsai said her government will provide the Tao tribe with appropriate compensation.

Local residents had received over NT$2.1 billion (US$66.9 million) in payments as of the end of May 2016 from state-run utility Taiwan Power Co. and the Atomic Energy Council since a low-level nuclear waste storage facility was built on Orchard Island in 1982.

During her visit Monday, Tsai will again apologize to the indigenous people, sources said.

In the near future, the government will also send people to indigenous villages around Taiwan to explain the formation of the Indigenous Historical Justice and Transitional Justice Commission under the Presidential Office.

Before Sept. 30, the government will also review relevant regulations to ensure that the Pingpu ethnic group identity will receive the rights and status it deserves, sources said.

In addition, the Executive Yuan has been instructed to convene the Indigenous Peoples Basic Law Promotion Committee within the shortest time to coordinate indigenous affairs.

Orchid Islanders' health unaffected by nuke waste

Source: http://www.eco-business.com/news/orchid-islanders-health-unaffected-by-nuke-waste/

March 2012 – The health of Orchid Island residents has not been compromised by the presence of a nuclear waste storage facility, the Atomic Energy Council said March 3.

The AEC issued a clarifying statement following a news conference held by aboriginal Tao at the Legislative Yuan March 1 calling for the removal of the stored nuclear waste from their island, also known as Lanyu.

The results of tests over the years by its Radiation Monitoring Center, as well as by Taiwan Power, have indicated that the dose equivalent radiation that Lanyu plants and animals are exposed to is well below 0.1 megasieverts per year, a standard set by the International Commission on Radiological Protection in its 2003 report, the AEC said.

The council also noted that according to data from the Department of Health's Bureau of Health Promotion, the increase in the incidence of cancer among Lanyu residents since 1980, two years before the establishment of the nuclear waste storage facility on the island, has not been notably higher than for Taiwan's population as a whole.

In 1980, the cancer incidence rate for Taiwan was 86 per 100,000 people, rising to 275 in 2008, while that for Lanyu's population was 35 per 100,000 in 1980, and 149 in 2008.

The AEC said inspection and repackaging work at the Orchid Island site was completed in November last year. Conditions are now normal and in compliance with safety standards, it added.

As for when and where the radioactive waste will be moved, the AEC pointed out that the matter must undergo comprehensive evaluation by the Ministry of Economic Affairs and Taipower, and

that the council cannot state a position in advance. It will ensure that any decisions are in line with safety regulations, the council said.

The AEC said it will urge Taipower to actively work out a plan for a final storage site for low-radiation waste, adding that it has written to the MOEA to request that it announce the candidate sites and coordinate with relevant local governments on related follow-up matters.

Before the storage site is relocated, the AEC said, it will continue rigorous management and control measures and closely monitor radiation levels to ensure the safety of Lanyu residents and the quality of the island's environment.

Unmanned Nuclear Defence and Attack

By David Oliver

Source: http://www.cbrneportal.com/unmanned-nuclear-defence-and-attack/

Sep 23 – Unmanned vehicles and nuclear power plants have had a contentious relationship, both positive and negative. The positive side was highlighted by the response to the Fukushima nuclear power plant in Japan that was severely damaged by a devastating earthquake in 2011.

Unmanned vehicles were first deployed at Fukushima just weeks after an earthquake and tsunami devastated the northeast coast of Japan. The US company iRobot, now Endeavour, deployed four unmanned ground vehicles (UGV) to the site, including the lightweight, versatile PackBot 510 and the heavy-duty Warrior 710. These UGVs were built for the battlefield, but modified to navigate and endure the hazardous conditions at the facility. The PackBot was equipped for the mission with a full HazMat kit which enabled it to measure temperature and detect gamma radiation, explosive gases and toxic chemicals, and feed all of that data to the power plant controllers in real-time.

QinetiQ North America also donated three TALON and two Dragon Runner UGVs. The US Department of Energy's Idaho National Laboratory modified the TALONs to be fitted with radiation-hardened cameras, GPS, night vision and Chemical, Biological, Radiological, Nuclear and Explosive (CBRNe) detection kits.

Endeavour has fielded its family of UGVs with defense forces worldwide, hundreds of law enforcement agencies and nearly two dozen nuclear power plants in North America. Its UGVs have performed countless dangerous missions across CBRNe and HazMat reconnaissance and surveillance.

Other nations have developed a range of UGVs for CBRN detection including France with the ECA Robotics Cameleon, the Nexter Robotics Nerva LG and the Thales u-Trooper. Poland's range of PIAP unmanned vehicles have chemical and radiological sensors the UK MIRA Mace 2 Guardsman has been tested with sensors for CBRN contamination.

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

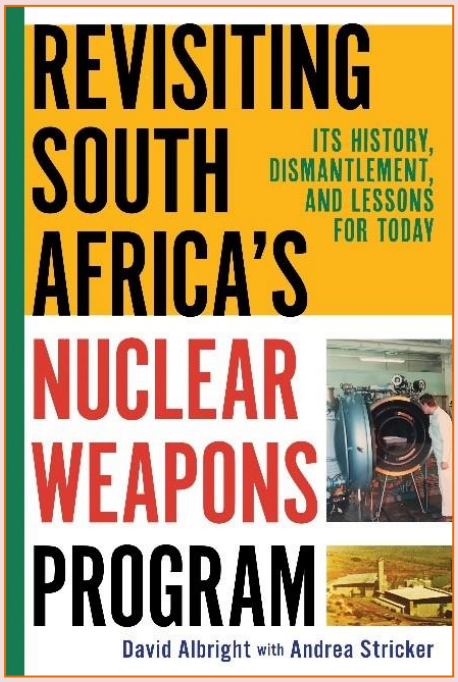
__David Oliver__ is a defence photo-journalist for more than 30 years, and member of the Independent Defence Media Association (IDMA) and the European Security and Defence Press Association (ESDPA). David is the author of 18 defence-related books, and is former IHS Jane's consultant editor and a regular correspondent for defence publications in the UK, USA, France, Poland, Brazil and Thailand.

The apartheid bomb: First comprehensive history of South Africa's nuke program

Source: http://www.homelandsecuritynewswire.com/dr20160930-the-apartheid-bomb-first-comprehensive-history-of-south-africas-nuke-program

Sep 30 – The Institute for Science and International Security has today (Friday) released **a new book,** *Revisiting South Africa's Nuclear Weapons Program: Its History, Dismantlement, and Lessons for Today*, by David Albright with Andrea Stricker. It is the first comprehensive, technically oriented history of South Africa's nuclear weapons program and its dismantlement. The Institute notes that lessons of this dynamic and complicated nuclear weapons program remain valid today. "Although none of the nine states that currently possess nuclear weapons appears on the verge of following South Africa's example, the South African case contains many valuable lessons in non-proliferation, disarmament, export controls, and verification," the Institute says.

Bomb casings at South Africa's abandoned Circle nuclear bomb production facility near Pretoria. These most likely would have accommodated a gun-type nuclear package for air delivery



Twenty five years ago South Africa acceded to the Nuclear Non-Proliferation Treaty (NPT) after dismantling its nuclear weapons. Yet, the full story of that nuclear weapons program was not revealed publicly at that time, even after then-President F. W. de Klerk revealed South Africa's nuclear weapons program in 1993. Parts were hidden from the International Atomic Energy Agency (IAEA) as well.

Now, after many years of work by the media and independent experts at the Institute for Science and International Security and elsewhere, and with the additional revelations and cooperation of a number of former members of South Africa's nuclear programs, a much fuller picture of South Africa's nuclear weapons program has emerged.

In particular, the new information and findings in *Revisiting South Africa's Nuclear Weapons Program* include:

- Three generations of nuclear weapon production facilities are described for the first time publicly. The book includes many photos of these sites that were not available before.
- The book contains the first detailed chronicle of South Africa's complicated struggle to

make highly enriched uranium for nuclear weapons.

- It is a popular misconception that a change in the South African leadership, for example, a form of regime change, was the key factor in making dismantlement possible. In fact, the historical record shows that South Africa's perceived security threats diminished first and then an internationally focused leader was able to make the decision to disarm.
- From an engineering standpoint, South African nuclear weapons were highly sophisticated and designed to be mated to advanced delivery systems, including a television guided glide bomb. At the end of the program, it had created the industrial wherewithal to mate a nuclear warhead to a ballistic missile. The South African nuclear weapon program explored, but was by no means rushing, to build boosted and thermonuclear weapons.
- Despite its recognized military and nuclear industries, South Africa depended on foreign procurements up until the end of the nuclear weapons program.
- The leadership of the South African Air Force sought to dramatically ramp up the nuclear arsenal and delivery capabilities for the 1990s, ahead of F. W. De Klerk coming into office and ending the nuclear weapons program.
- A closer look, based on declassified South African government documents, at South Africa's nuclear strategic thinking, shows a government at conflict with itself over the question of whether South Africa would use nuclear weapons in a crisis or maintain them strictly as a deterrent.
- South Africa initially did not plan to disclose its nuclear weapons program to the international community and the IAEA. An evolution of thinking by South Africa's new leaders and the IAEA, and intense pressure from the African National Congress, NGOs, and other governments, led to the acknowledgement that greater transparency was key to assuring South Africa's neighbors that it had denuclearized. This process has valuable historical lessons for today's proliferation cases.
- Despite establishing a policy of greater transparency in 1993, South Africa held back key details of its nuclear weapon delivery systems from the IAEA inspectors. It also was highly circumspect in describing its foreign procurements for its nuclear programs. This lack of disclosure in two key areas did not stop the IAEA from verifying South Africa's nuclear disarmament. However, history deserves a fuller treatment, and this book seeks to contribute to that goal.

RSA-3 3 stage LEO rocket

The Institute for Science and International Security notes that work on South Africa's nuclear program goes back to the Institute's founding in 1992. One of its first projects was working with African National Congress (ANC) officials, who were interested in learning more about nuclear non-proliferation in anticipation of assuming key positions in a democratic South African government. This cooperation led to contacts with several former members of South Africa's nuclear weapons program and a range of collaborative endeavors with them. It included two tours of the old nuclear weapons production sites. On the trip in August 2002, Albright was allowed to photograph the old nuclear weapon production sites before they were modified beyond recognition of their original purpose. Many of these images appear in the book for the first time.

Revisiting South Africa's Nuclear Weapons Program has relied on many interviews conducted by the authors in the 1990s and early 2000s with past members of the nuclear weapons programs and IAEA inspectors directly involved in verifying South Africa's nuclear dismantlement. The authors relied as well on a range of documents from that period, some of which they regret to state can still not be revealed publicly.

The book is organized as a chronology of the nuclear weapons program's growth, maturation, and demise. However, it can be read out of order. For those interested in the details of the bomb

program, the authors recommend looking at chapters, 2, 5, and 7. For those interested in the program's dismantlement, see chapters 8-12. If nuclear weapons strategy is of interest, start with chapters 4 and 6. For those who are more technically inclined to the nuclear fuel cycle, and in particular highly enriched uranium production, see chapters 1, 3, and 12. Finally, for those interested in today's lessons, read chapter 13.

Timeline of South African nuclear weapons programme	
Year	**Activity**
1950s & 1960s	Scientific work on the feasibility of peaceful nuclear explosives and support to nuclear power production efforts
1969	Atomic Energy Board forms group to evaluate technical and economic aspects of nuclear explosives
1970	Atomic Energy Commission (AEC) releases report identifying uses for nuclear explosives
1971	R&D approval granted for "peaceful use of nuclear explosives"
1973	AEC prioritises work on a **gun-type design**
1974	Work on a nuclear device and the **Vastrap** test site are authorised
1977	AEC completes bomb assembly for "cold" test
1978	First **HEU** produced; Armscor assumes control of weapons programme
1979	**Vela Incident**; First bomb with HEU core produced by AEC
1982	First deliverable bomb built; work on weapons safety
1985	Three-phase nuclear strategy reviewed
1987	First production bomb built
1988	Armscor prepares Vastrap for a nuclear test
1989	Nuclear weapons dismantled
1991	Accedes to **NPT**

Although not every question could be answered, this history reveals a great deal of new information about the program. The authors say they hope that this book will be regarded as a useful contribution to policy debates and serve as a compendium of information on South Africa's nuclear weapons program and its dismantlement.

The Institute has produced multiple electronic and print versions of this book to allow it be viewed on several platforms. We want to especially thank 52 Novels for making this possible and Stewart Williams for designing the cover.

The Institute has also funded the dissemination of the book so that electronic pdf and e-publication versions could be provided at no cost. The pdf is available on the Institute's Web site; at the Naval Postgraduate School's Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC); and also on the Homeland Security Digital Library. An e-book version is available at no cost at Smashwords and Nook – and also on Kindle, but note that the policies of Kindle do not allow for the book to be offered at no cost on its platform, at least initially. The book is also available in a paperback version (with black and white photos only) for purchase on Amazon.

— Read more in David Albright and Andrea Stricker, Revisiting South Africa's Nuclear Weapons Program: Its History, Dismantlement, and Lessons for Today (Institute for Science and International Security, 2016).

Surprise finding could improve future handling of nuclear waste

Source: http://www.homelandsecuritynewswire.com/dr20160930-surprise-finding-could-improve-future-handling-of-nuclear-waste

Sep 30 – A researcher at the University of Manchester has made a surprise finding after observing variations of a chemical bond with a radioactive metal called thorium — and this newly revealed relationship could one day contribute to improving nuclear fuel management.

U Manchester says that Elizabeth Wildman, a Ph.D. student in the research group led by Professor Steve Liddle, has reported compounds in which unusual forms of phosphorus — known as the Devil's element — are stabilized by thorium, a radioactive chemical element named after the Norse god of thunder which can be used as a nuclear fuel in the nuclear power industry.

"This has been an exciting experience and I am delighted my work has been recognized in this way," said Elizabeth Wildman. "It seems the Norse god of thunder has tamed the Devil's element."

This latest study from Professor Liddle's research group looked at how "soft" elements such as phosphorus can interact with thorium in unusual bonding environments.

The research looked at species with single and double thorium-phosphorus bonds, and even managed to trap moieties as fundamental as PH and a naked P atom between two thorium ions.

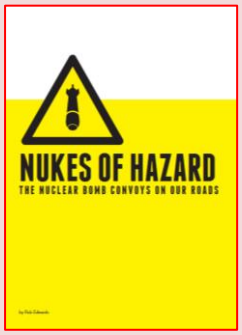
"Nuclear power could provide energy security for the United Kingdom and produce far less carbon dioxide than fossil fuels, but the waste it produces is potentially very dangerous if not handled properly" said Professor Steve Liddle, co-director of the Center for Radiochemistry Research at the University of Manchester. "In order to find ways of reducing the volume of nuclear waste and recycle unspent fuel, research has focused on developing our understanding of how radioactive actinide elements interact with elements from around the periodic table that they could come into contact with in the fuel cycle."

The work was carried out as part of a collaborative research project between the universities of Manchester and Regensburg, and was funded and supported by the Royal Society, European Research Council, Engineering and Physical Sciences Research Council, and European Cooperation in Science and Technology.

— Read more in Elizabeth P. Wildman et al., "Thorium–phosphorus triamidoamine complexes containing Th–P single- and multiple-bond interactions," Nature Communications 7, Article number 12884 (29 September 2016) (DOI: 10.1038/ncomms12884).

Nukes of Hazard: 180 Mishaps Befall UK Nuclear Convoys

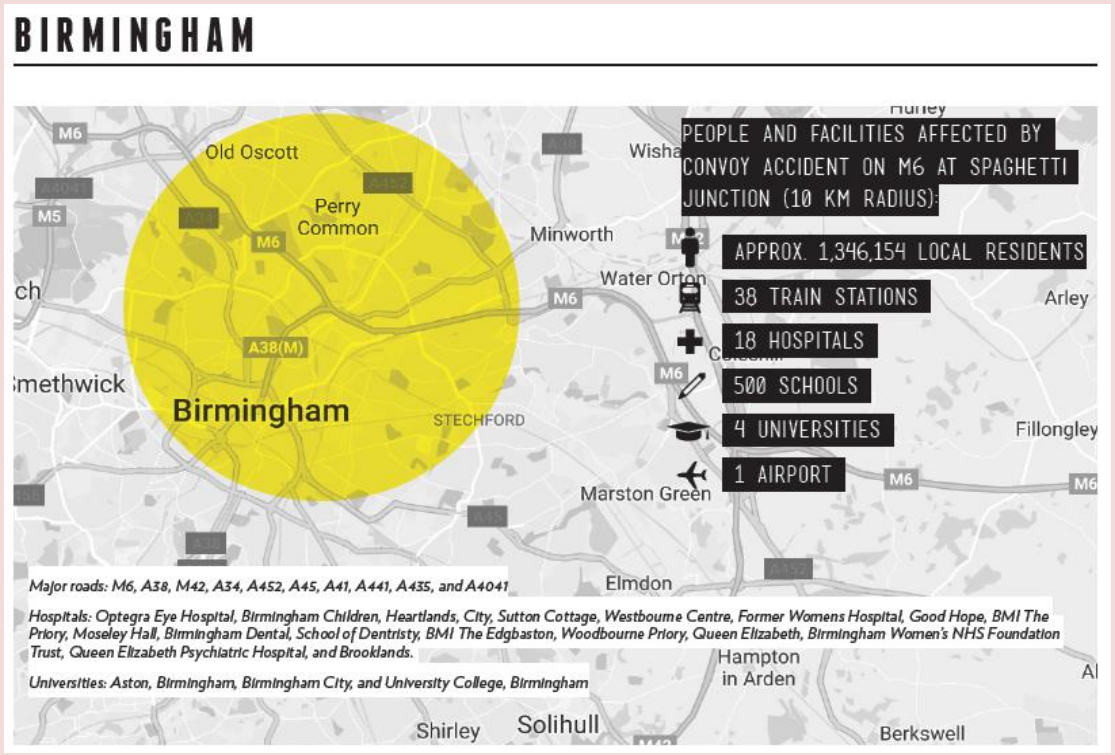
Source: https://sputniknews.com/europe/20160921/1045555227/uk-nuclear-convoys-hazard.html



Anti-nuclear campaigners say that the regular transportation of nuclear weapons across the UK is putting lives at risk.Military convoys carrying nuclear materials have suffered collisions, breakdowns and brake failures. There have been at least "180 mishaps in 16 years" involving military convoys carrying nuclear bombs around the UK. That's the startling news according to a "Nukes of Hazard" report by the International Campaign to Abolish Nuclear Weapons (ICAN), published on Wednesday (September 21). The report, based on Ministry of Defense logs released due to Freedom of Information requests, reveals that materials for nuclear weapons are driven through or flown over 122 separate local councils in the UK. They include densely-populated areas in major cities such as Birmingham, Bristol, Cardiff, Edinburgh, Glasgow, Leeds,

Liverpool, Sheffield, Manchester and Newcastle. According to ICAN, the convoys carry nuclear warheads in dark green trucks accompanied by up to 20 vehicles, including police and fire trucks, around 6 times per year, making a 900 mile trip on each occasion. The last trip reportedly happened earlier this month. Matt Hawkins a project officer from the ICAN, who worked

with the report's author, investigative journalist Rob Edwards, said: "We can only rely on what the Ministry of Defense wants us to k now. There is of course a lot of material that they do not wish to share. The kind of accidents that have happened range from crashes with other vehicles, break downs, the trucks actually overturning in the road, the trucks overheating, brakes failing, fuel leaks, smoke emitting from the bomb carrier fuel box, and, perhaps most unusually, dogs being loose on the motorway," Mr. Hawkins told Sputnik. The Ministry of Defense (MoD) issued a statement in



response to the report: "The transport of defense nuclear material is carried out to the highest standard in accordance with stringent safety regulations, and all operational and engineering incidents are reported, however minor. "In over 50 years of transporting defense nuclear material in the UK,

there has never been an incident that has posed any radiation hazard to the public or to the environment," the MoD said.

▶ **Read the report at:**
http://nukesofhazard.gn.apc.org/wp-content/uploads/2016/09/NoH_Report_Final.pdf

Syrian Army Discovers Turkish Manual Instructing Terrorists in Use of Nukes

Source: https://sputniknews.com/middleeast/20160923/1045637762/turkish-terrorist-manual-syria.html

Sep 24 – In the course of a recent operation to liberate a terrorist-held enclave in northern Latakia, Syrian Army troops discovered a 'manual for terrorists'. Printed in Turkey, the book teaches jihadis "the proper

conduct of war on foreign soil," up to and including the use of nuclear weapons. The manual, printed in Arabic and called 'Zad al-Mujahed' (roughly, 'Fruits for the work of God's Warriors') was published in Istanbul, with its publishers making no attempt to even try to hide the book's origins. It features the logo of the Istanbul-based Guraba publishing company, contact information, and even an ISBN, inside its front cover.

Speaking to Sputnik Arabic, the Syrian Army soldier who discovered the book said that it was filled with hatred and calls to war against people who don't share jihadists' faith, as well as instructions on what must be done with "enemies and their property."

"The book describes how to properly burn cities captured by jihadi fighters, how to cut down all the trees, destroy all life, how to execute prisoners in the correct manner," the soldier explained. The book is banned in Syria for its radical content, and repeated calls to violence and terror. For this reason, Sputnik Arabic decided not to quote it directly. Still, it published photos, republished here, showing the cover and details on the book's publisher. It remains unclear how many copies of this book were found.

Syrian authorities are extremely sensitive about published materials which could be seen to inspire sectarian conflict. Before it was engulfed in war in 2011, Syria was known as a secular, multicultural and multiethnic nation with a large number of religious minorities. Since then, many

of these minorities have been threatened with enslavement or extermination by homegrown and foreign-sponsored radical Islamist terrorists, including Daesh (ISIS), al-Nusra and a collection of affiliated groups.

Moscow prepared for possible nuclear attack - EMERCOM

Source: http://www.pravdareport.com/russia/politics/30-09-2016/135749-moscow_nuclear_war-0/

Sep 30 – Representatives for the Russian Emergency Situations Ministry (EMERCOM) said that all bomb shelters and underground shelters in Moscow meant for the evacuation of people in case of a nuclear attack or other emergencies, "were prepared and will be able to accommodate the entire population of

the capital."

"As a result of the introduction of new approaches to civil defense, an inventory of underground facilities of the city was conducted. The Moscow underground facilities will be able to protect 100% of the population of the city," deputy head of EMERCOM of Russia in Moscow, Andrei Mishchenko said.

He also added that the department takes urgent measures to enhance civil defense. The department updates the legal framework and modernizes control and alarm systems.

"We work to improve the public training system in the field of civil defense," he said.

Noteworthy, the Ministry for Communications, the Finance Ministry, the Ministry for Industry, the Russian State Reserve and the Bank of Russia earlier took part in a sudden inspection of the Russian army. **The above-mentioned departments worked in a "war-time" mode to test their systems for a possible war.**

The Washington Free Beacon wrote citing US intelligence that Russia suddenly started building super bunkers. According to the publication, "dozens" of such bunkers are being built across the country.

Experts point out that their creation is associated with the introduction of a prospective integrated automated command and control system of the fifth generation into Russian missile forces.

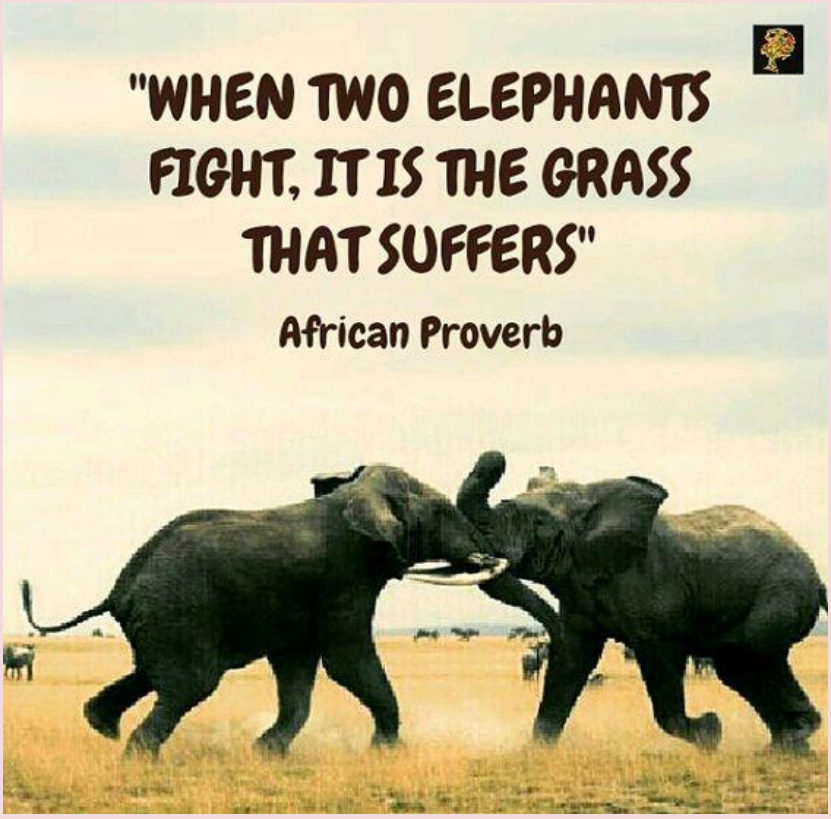
To crown it all, according to services responsible for the organization of civil defense and emergency response, a special program was launched in Moscow in 2015 , within the scope of which bomb shelters and fallout shelters were built or renewed in every district of the Russian capital.

Two years ago, Russia conducted drills to repulse a nuclear attack on Moscow and strike a massive retaliatory blow. Reportedly, President Putin used the "nuclear suitcase" during the drills.

In 2015, both Russian and American generals said for the first time that a nuclear war between the United States and Russia was close like never before.

"Despite the fact that the majority of Russians, including Muscovites, do not know where bomb shelters are located in their neighborhoods, there is a list of addresses of bomb shelters. The

shelters are now maintained accordingly to give people an opportunity to go through several days of a man-made emergency or a nuclear attack," EMERCOM officials said.



Is Nuclear War Becoming Thinkable?

Both the U.S. and Russia are prepared to go there under certain circumstances

Source: https://www.theamericanconservative.com/articles/is-nuclear-war-becoming-thinkable/

Oct 06 – People who make their living thinking about defense policy and national security like everything to fit into a nice framework, preferably one that can be visualized on a PowerPoint slide. If you are unfortunate enough to be standing next to two officials speaking Pentagonese during a reception, you will note that their language is full of acronyms relating to projects and obscure government agencies—and that they refer regularly to strategic concepts and systems, including the venerable "triad" of nuclear deterrence.

The "triad" concept holds that when a country fields land-, air-, and submarine-based nuclear capabilities, it greatly increases its chances of being able to retaliate after an attack. In the case of the U.S. and the Soviet Union during the Cold War, for example, if either side would have launched a first strike and knocked out the other side's land- or air-based systems, submarines would still have provided a devastating second-strike capability. Nuclear war was such an awful prospect that it long was described as intrinsically the ultimate universal deterrent, rendering an actual armed conflict between NATO and the Warsaw Pact that might escalate unthinkable.

The end of the Cold War in 1991 seemed to reduce the chance of nuclear war still further, even though the weapons had proliferated. But no one anticipated the level of hostility toward Russia that is now evident, and talk in the Pentagon is again focused on what it would take to win a war against an apparently resurgent Moscow. And for his part, earlier this week, Russian President Vladimir Putin withdrew from a nuclear security pact, citing "hostile actions" by the U.S.

To be sure, much of the Pentagon's animosity regarding Moscow is budget-driven, with generals and admirals needing an enemy more formidable than "international terrorism" to justify an enhanced role for their respective branches of the service. Recent general-staff claims that the

U.S. Army is "outranged and outgunned" by the Russian military are credible only if one counts tanks and does not consider the opposing air forces. Alarms raised by former general and current self-promoting politician Wesley Clark that Russia has built an "invulnerable" tank have been met with derision. Many of the claims regarding advanced Russian weaponry come from the Ukrainian government, which clearly has an agenda to support as it seeks sophisticated U.S. offensive arms and military aid.

The reality is that Russia, apart from its nuclear arsenal, is a bit of a mouse that roared. Its struggling economy generates a GNP that is on par with that of Italy, and it spends one-seventh as much as the U.S. on the military. It has one aircraft carrier versus 10 in the American arsenal, one-sixth as many helicopters, one-third the number of fighter aircraft, and less than half as many active-duty military personnel. It has no effective military allies, while the U.S. has nearly all of Eastern and Western Europe in NATO.

Official U.S. policy is that NATO provides conventional deterrence at such a level that Russia would not be inclined to start a conflict with any alliance member lest it be defeated in short order. But Russia would have certain advantages if it were to attack without warning, relying on internal lines and deploying locally superior forces. And the reliability of a coordinated NATO response can be questioned, as the *raison d'etre* for NATO itself is wearing thin even as the alliance has expanded to include countries like Montenegro. One U.S. Army officer observed to journalist Mark Perry, "How many British soldiers do you think want to die for Estonia?"

The problems involved in actually mounting a credible conventional defense in Europe are why there is a second level of deterrence: the nuclear umbrella maintained by the United States, Britain, and France. U.S. officialdom used to suggest that Washington and NATO would not be the first to use nuclear weapons in a conflict, but that was never an actual policy. Last month there were reports that President Obama had considered committing to "no first use" but was overruled by his cabinet, with Secretary of Defense Ash Carter describing such a pledge as "a sign of weakness." Two liberal congressmen have since introduced a bill that would prohibit U.S. first use of nuclear weapons, but it appears to have little support and is likely to die in committee.

Carter, who describes nuclear weapons as the "bedrock" and "guarantor" of U.S. security, recently spoke at several Minuteman missile bases in the United States. He stated that the U.S. and its European allies are now "refreshing" U.S. strategy by integrating conventional and nuclear weapons in order to "deter Russia from thinking it can benefit from nuclear use in a conflict with NATO." Carter explained that Moscow has little regard "for long-established accords of using nuclear weapons," raising "serious questions" about "whether they respect the profound caution that Cold War-era leaders showed in respect to brandishing their nuclear weapons."

Ash Carter also elaborated that "if deterrence fails, you provide the president with options to achieve U.S. and allied objectives … all to reduce the risk of nuclear weapons being used in the first place." He emphasized "our will and ability to act." Note that Carter did not suggest that the U.S. would not be the first to use nuclear weapons, and was clearly indicating that such weapons are in the mix of how to respond to what he obviously sees as an increasing Russian threat.

Carter is admittedly an anti-Russian hawk. He is also a physicist by training and is somewhat of an expert on policies relating to the use of nuclear weapons. Some of the changes he has made to our nuclear-deterrent policies were recently observable on CBS's *60 Minutes*, which ran a series on the state of the American nuclear arsenal. On board a nuclear-armed Ohio class submarine, officers spoke openly of the heightened state of alert—back up to a Cold War level—since "Russia invaded Crimea." A relatively new tactical option was also discussed, referred to as "escalate to de-escalate," which envisions defeating a conventional attack by means of a nuclear demonstration strike. The nuke would serve as a warning of more to come if the attack continued.

The concept of using a nuke as a warning is not exactly new. "Going nuclear" was considered a viable option during America's two Iraq wars, if Saddam Hussein possessed weapons of mass destruction and was prepared to use them, and it has also been a part of the battle plan should the United States go to war with Iran. But what has changed the calculus is the sophistication of the weapons themselves. New tactical nuclear weapons, like the latest versions of the U.S. B-61, are small and portable. They can be launched from a bomber or as part of a cruise missile or even from a ground installation or vehicle. Further, their operators can "dial up a yield"—i.e., select the size of the explosion on the bomb itself. That means a demonstration nuclear strike can be effectively "nuclear" while also designed to have a relatively small footprint to reduce both civilian and military casualties. This selectivity

makes such a bomb, in the minds of some generals and politicians, potentially an effective warning rather than an automatic escalation of the fighting—and as a result it is a weapon that is much "more usable."
The Russians, of course, have similar weapons, and by some accounts their nuclear arsenal is more modern than that employed by the U.S. Moscow's war doctrine was recently spelled out by Putin. He said that Moscow "would reserve the right to use nuclear weapons if the existence of Russia is threatened." This has been interpreted as Putin acknowledging that his conventional forces cannot go head-to-head with those of the U.S. in the long run—and warning that Russia might be forced to go nuclear first, relatively early on in the conflict, to defend itself.
So one should conclude that both sides confronting each other over Eastern Europe are now prepared to go nuclear under certain circumstances. No one is asking the Poles and Slovaks, whose land might well be the site for such a demonstration, what they think, but their governments are officially on board with NATO strategies designed to deter Russia. Germany has, however, expressed considerable nervousness over the saber-rattling as memories of the Red Army are still somewhat fresh. And there are frightening indications that some senior military officers might be eager to get things started in the belief that a war with Russia could actually be winnable. Certifiable loose cannons on deck include Wesley Clark, who reportedly tried to engineer a confrontation with Russian peacekeepers in Kosovo in 1999. Crazier still, Gen. Philip Breedlove (who retired earlier this year) worked hard during his time as supreme commander of NATO forces in Europe to get NATO and the U.S. involved in a proxy war over Ukraine. In leaked emails, an interlocutor suggested he and the U.N. secretary general might "fashion a NATO strategy to leverage, cajole, convince or coerce the U.S. to react" to the Russian "threat"; Breedlove found this "very promising." Breedlove, who has regularly lied about the extent of the Russian presence in Ukraine, has hysterically described Moscow as a "long-term existential threat to the United States and to our European allies." The general was also reportedly in contact with State Department Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland, who helped engineer the coup that overthrew the Ukrainian government in 2014.
Meanwhile, Hillary Clinton is calling Putin a new Hitler while the *New York Times* editorializes against "Vladimir Putin's Outlaw State." And the real danger is that the Russian people are watching this display with concern and might soon believe themselves to be backed into a corner by an implacable enemy. Putin has several times warned that there is an increasing perception in Russia that the country is being surrounded and endangered by the continuous expansion of NATO as well as by threats relating to his country's involvement in Syria. Opinion polls suggest that the average Russian now expects war with the West.
The insistence on the part of the many in the West that Putin must be resisted by using *force majeure* if necessary is based on gross exaggeration of the actual threat coming from Moscow. That nuclear weapons are now apparently employable in the plans for deterrence on the part of NATO, as well as in the Russian plans for self-defense, should be a terrifying prospect for anyone who cares about what might come next.

***Philip Giraldi**, a former CIA officer, is executive director of the Council for the National Interest.*

Terrorism fallout shelters: Is it time to resurrect nuclear civil defense?

By Timothy J. Jorgensen
Source: http://www.homelandsecuritynewswire.com/dr20161006-terrorism-fallout-shelters-is-it-time-to-resurrect-nuclear-civil-defense

Oct 06 – Fifty-five years ago, on 6 October 1961, President John F. Kennedy advised Americans to build an underground protective room, commonly known as a "fallout shelter," in their homes.
At that time – the middle of the Cold War – the United States feared that a nuclear attack by the Soviet Union was imminent. Kennedy said, "in the event of an attack, the lives of those families which are not hit in a nuclear blast and fire can still be saved if they can be warned to take shelter and if that shelter is available."

He proposed spending $207.6 million for a civil defense plan "to identify and mark space in existing structures – public and private – that could be used for fallout shelters."
The American people heeded his advice and began an enormous grassroots effort to construct fallout shelters in every private residence and public building. **Today, those shelters in the basements of 1960s-era homes are largely used for storage.** The only reminder of the public shelters is the occasional yellow fallout shelter sign that still remains affixed to the outside wall of some buildings. Now, no one builds fallout shelters.
But, why not? The nuclear weapons are still around.
As a radiation protection expert and a professor of radiation medicine, I am sometimes asked this question. The answer is an interesting story that should give us all pause, especially as we now face new nuclear weapon threats.

The Cold War

The main reason we no longer build fallout shelters is that as nuclear bombs have grown in size and number, the prospects of surviving a nuclear war – even in a shelter – have decreased. A study by the RAND Corporation in 1966 determined that as many as 62 percent of all Americans would die in a nuclear exchange with the Soviet Union, and painted a pretty grim picture of the lives of the survivors.
As a result, fallout shelters became seen as an ineffective way to protect the lives of the vast majority of the population. Gradually, civil defense efforts moved away from nuclear bombs and concentrated on everyday threats that could be more easily defended against, such as tornadoes, earthquakes and hurricanes.
How, then, could Americans protect themselves from the threat of nuclear holocaust if a nuclear war between the United States and the Soviet Union was not survivable?
Mutually assured destruction, commonly known as "MAD," became the cornerstone of our nuclear defense strategy. Since no sane leader would initiate a suicidal war, an arms race began in order to produce so many nuclear weapons on both sides that only a deranged person would think it wise to launch a nuclear attack. The basic defense strategy, using the MAD approach, was to make nuclear war such an unthinkable option that nuclear weapons would never be used offensively by either side.
But the nuclear arms race became a huge financial burden, and each country soon had excess capacity to annihilate the other many times over. Talks were initiated between the United States and the Soviet Union (now Russia) to limit the production of new nuclear weapons and even reduce the existing stockpiles. Beginning with the Strategic Arms Reduction Treaty (START) of 1991, and culminating with the New START agreement that entered into effect in 2011, stockpiles of nuclear weapons have been reduced from a peak of about 35,000 strategic nuclear warheads held by each country in the mid-1980s to about 7,000 each today. With regard to deployed strategic nuclear weapons, the goal is to limit each side to just 1,550 by 5 February 2018.
Whether this reduction in nuclear warheads has made us any safer is debatable. Both sides still retain enough to maintain a defense strategy of mutually assured destruction. Certainly, the societal costs of feeding the massive nuclear war machine have been reduced to the benefit of all.
But, a war between superpowers is not the only nuclear weapon threat Americans currently face.

Nuclear terrorism

Today, smaller nations and terrorist groups, such as al-Qaeda, are seeking nuclear weapons. Some nations, like North Korea, already have them. Others may be a decade away.
It is not unreasonable to believe that the use of a single nuclear weapon by a rogue nation or a terrorist group now poses a more likely scenario for a nuclear confrontation than a nuclear war between Russia and the United States. Nevertheless, some downplay the threat of a nuclear attack to the U.S. mainland by these new nuclear adversaries. They argue that adversaries not only need nuclear weapons, but must also be able to deliver them to their targets.
Since missile technology is not a strength of small nations and terrorists, the lack of launch capacity is often cited as a major obstacle to such would-be nuclear attackers. But recently, North Korea's successful missile launch tests seriously challenge this assumption about limited missile capabilities. Regardless, missiles aren't essential to deliver a nuclear weapon. A bomb in a cargo ship in New York harbor is just as much a threat as one launched by missile from overseas. And, as bombs are

miniaturized, the prospects of detecting and stopping nuclear weapons coming across our borders and through our ports is greatly reduced.
We are entering an era in which multiple small countries or terrorist organizations may acquire a few "small" nuclear weapons in hidden locations around the world. Such small weapons could be used to inflict a considerable amount of damage, but nothing on the scale what we envisioned during the Cold War. These small bombs are probably survivable with fallout shelters that would be useless during a full nuclear war. In fact, these relatively small nuclear weapons – if you consider Hiroshima-sized bombs to be small – are precisely the size that were envisioned when fallout shelters were first proposed for civil defense.

Old solution, new problem

Is it time to resurrect nuclear civil defense in response to the increasing threat from terrorists?

Although experts think it unlikely that terrorists are currently technologically sophisticated enough to make their own nuclear weapons from scratch, even if they had access to enriched uranium (the required fuel), there is no question that they could steal one from some small (or large) nuclear nation, particularly during the chaotic aftermath of a coup. Turkey had nuclear weapons at the time of its recent coup attempt, for example. Alternatively, terrorists could obtain them by discretely purchasing them from renegade nuclear nations, or clandestinely by bribing military officials.
One nuclear bomb, in one ship, in one harbor is all it takes to get into the nuclear terrorism business.
It is clear that mutually assured destruction is a defense strategy that only works between stable nations with sane leaders. Mutually assured destruction is not a strategy that works against nations with unstable rulers, such as in North Korea, or enemies with no known address to which you can deliver a retaliatory strike, such as terrorists.
For these adversaries, we need an alternative strategy to protect ourselves. Right now we don't have one, other than screening cargo for nuclear weapons and weapons-grade uranium. And, as I describe in my book, *Strange Glow: The Story of Radiation*, mock tests of this screening program have revealed significant weaknesses.
I believe we need to better address this new and growing threat of nuclear terrorism right now, and devote as many resources as necessary toward dealing with it. If we don't find a more effective strategy to thwart nuclear terrorism soon, we may be forced to go back to fallout shelters as our only protective option, whether we like it or not.

Timothy J. Jorgensen *is Director of the Health Physics and Radiation Protection Graduate Program and Associate Professor of Radiation Medicine, Georgetown University.*

EDITOR'S COMMENT: It would be very interesting to have in the same table Prof Jorgensen and Prof Stephen Schwalbe ("*Where are the Terrorist WMD Attacks?"* – can be read at "Chem News" chapter) and hear what their conclusions would be about the overall new emerging threats' issue. And perhaps have Philip Giraldi (from previous article) as moderator.

The continuing danger of Semipalatinsk

By Magdalena Stawkowski
Source: http://thebulletin.org/continuing-danger-semipalatinsk9969

Oct 06 – **During the Cold War, the Semipalatinsk Nuclear Test Site in Kazakhstan was the Soviet Union's primary nuclear weapons testing ground. Between 1949 and 1989, more than 450 nuclear bombs were exploded above and below ground on its once secret, 7,000-square-mile territory.** In the post-Soviet period, Kazakhstan has attracted much international praise for its "extraordinary leadership" and "courage" in closing Semipalatinsk, for giving up its nuclear weapons stockpile, and for helping to create a nuclear weapon free zone in Central Asia. Kazakhstan has also been celebrated for having an extraordinary record in advancing nuclear security and thus was judged to be perfectly suited to host an international fuel bank for low-enriched uranium. The Obama administration has described Kazakhstan's president, Nursultan Nazarbayev, as "really one of the model leaders in the world" on non-proliferation and nuclear safety issues.

These commendations are perhaps overly enthusiastic. They exaggerate Kazakhstan's commitment to nuclear safety; actually, Kazakhstan's leadership has done little to address pressing humanitarian issues

at Semipalatinsk, failing to provide adequate funding for environmental clean up and adequate security for the site itself. How can the world talk about nuclear safety in Kazakhstan when it is the only place on Earth where thousands of people still live in and around an atomic test site? How can there be safety, when residual radioactivity and environmental damage are a normal part of life for people who live there? Nuclear security should mean more than the physical protection of nuclear materials. Nuclear security must also mean the physical protection of individual citizens from radioactivity.

Today, most of the abandoned Semipalatinsk territory is accessible to anyone who wishes to enter. Except for a 37-mile area "exclusion zone" at the Degelen Mountain complex, guarded by drones and other surveillance equipment, few signs indicate radiation danger. For the thousands living nearby, it is

no secret that the former nuclear testing area is poorly secured. I have been conducting anthropological fieldwork in the region since 2009, living in Koyan, a remote village on the nuclear test site's border. I know first hand the ease with which people make use of the territory. ("Koyan" and "Tursynbek," the name of an ethnographic interlocutor mentioned later in this article, are pseudonyms, used to protect village residents and the interlocutor following the convention of confidentiality spelled out in the American Anthropological Association Code of Ethics on professional responsibility).

Koyaners, like most everyone else living in and around Semipalatinsk, use the test site in a number of ways: They drive across the dusty steppe during warmer months to visit relatives in nearby villages. In July and August, men, women, and children come back from the site, buckets brimming with wild strawberries they have picked from its shallow valleys. Many graze their herds of sheep, goats, horses, and cows on the Semipalatinsk pastures, sometimes near craters formed by underground explosions. Many of these places are known to contain radioactive "hot spots," but since the area around Koyan is mostly unmarked, no one in the village is certain where the hot spots are. Koyaners are not privy to this information, because no one in the government shares it with them.

On a hot, sunny day in July 2015, Tursynbek, a burly stockbreeder and miner in his mid-50s, decided we should go out and measure radiation on our own. As we got in the car, he complained that when he has had a chance to ask scientists, who occasionally do research in the area, if there is radiation, they dismiss his concerns by saying, "There is nothing here; no radiation." I made sure to bring my Geiger counter on this trip, and a short car ride later I was looking down from the rim of a nuclear crater, trying to hear the Geiger counter readings Tursynbek was shouting. His camouflage jacket was barely visible on the steep pitch, among the tall grasses; a rather sizeable water hole was beyond, inside the crater. He scanned the ground for radioactivity, his white paper sanitary mask pulled down under his chin, rather than over his mouth. The sanitary mask was meant to protect against small particles of plutonium or other radioisotopes that are dangerous when inhaled but can be stopped by a sheet of paper. But Tursynbek was not afraid. Tursybek knows this area well; he was born in Koyan and has decades of experience raising livestock, sheep, goats, cows, and horses, which includes grazing them on the test site.

Still, he had never been here on this kind of mission. As he climbed out, he eagerly used the Geiger counter to check the wreckage of the atomic landscape: trenches, mangled barbed wire enclosures, scattered cement blocks with clusters of electrical cables jutting from them. The frantic clicking of the Geiger counter disturbed the otherwise calm summer afternoon. Not far from us, Kazakhstan's Institute of Radiation Safety and Ecology (IRSE) *wazik* (van) carrying "geologists," as the scientists are known to Koyaners, passed by. "They have never shared any of this information with us," Tursynbek said motioning to the van and pointing at the .700 milliRem per hour reading displayed by the counter.

Normal background is between .008-.015 milliRem/hr. According to the US Nuclear Regulatory Commission (NRC), Americans receive an average radiation dose of about 620 milliRem per year. Half of this dose comes from naturally occurring radiation found in soil, rocks (uranium), and air (radon). The other half comes from man-made sources, like radiation therapy, x-rays, and nuclear power plants. At the crater, five weeks is enough time to receive the average yearly dose of radiation described by the NRC. In one year that dose is equal to 6,136 milliRem.

Looking around the abandoned test site, it is almost never obvious what went on here, except at a few key experimental locations, which have decaying cement structures and other visible points of interest. The once high levels of security have long since disappeared. Yet for 40 years various technical sites at Semipalatinsk were used to experiment with different types of nuclear explosions. At "Ground Zero" for example, 116 aboveground tests were conducted, as part of a full-scale experiment designed to record damage done to animals (sheep, goats, cows, and pigs), plants and soil, building construction, military equipment, and people living in settlements found near the site. At other technical areas, more than 300 underground nuclear explosions were used to test their peaceful applications. Several of these high-yield tests produced nuclear craters and contaminated much of the area nearby.

Near the nuclear crater Tursynbek and I visited, only a small and badly faded radiation warning sign clung to a mangled barbed wire enclosure that once provided some level of protection. The plight of people who suffered from radiation exposure during the Soviet-era is well known in the country and abroad, even if the level of radioactive pollution and its impact on human health are hotly disputed, in local and international peer-reviewed scientific journals.

In an August 2015 editorial for the *Bulletin of Atomic Scientists*, Kazakhstan's ambassador to the United States, Kairat Umarov, highlighted the fate of 1.5 million Kazakh citizens whose lives continue to be affected by nuclear testing. He wrote with the optimism of a man hoping to promote a nuclear-weapons-free world. But Umarov ignored an obvious fact: The Nazarbayev government, lacking financial resources, has done very little to address the security problems at Semipalatinsk and has not spent a penny to clean up the area. Praise of the nation's leadership for making Kazakhstan a non-nuclear state has come at a price: It has overshadowed and limited conversations about lack of oversight of Semipalatinsk and the toxic mess that the Soviet nuclear testing program left behind and continues to endanger thousands of citizens living in the area. Given this unresolved and underreported situation at Semipalatinsk, the

international community should offer financial help and expertise for the cleanup of Semipalatinsk, or at the very least help with cordoning off the most contaminated areas of the site.

__Magdalena Stawkowski__ is a medical anthropologist researching Cold War nuclear legacies in Kazakhstan. She is currently a teaching scholar at North Carolina State University and a fellow at the Center for Slavic, Eurasian and East European Studies (CSEEES) at the University of North Carolina-Chapel Hill. Previously, Stawkowski was a Stanton Nuclear Security Fellow and a MacArthur Nuclear Security Fellow at the Center for International Security and Cooperation (CISAC) at Stanford University. She received her doctorate in anthropology from the University of Colorado Boulder.

Nuclear Weapons and Terrorism: A Dangerous Mix

By Jean-Bernard Latortue

Source: http://www.iar-gwu.org/content/nuclear-weapons-and-terrorism-dangerous-mix

Sep 30 – When video footage of a Belgian nuclear official was discovered in the apartment of a terrorist behind the Paris attacks of November 13, 2015, it heightened the concerns of national security experts in the United States and abroad about nuclear weapons falling into the hands of terrorist groups. As strange as it may sound, though, catastrophe is opportunity. The United States and the other nuclear powers must seize this opportunity to work together to broaden their nuclear security policy to mitigate the growing threat of a nuclear-armed terrorist group. Stronger physical protection of nuclear facilities, tigher border controls around nuclear power states, and increased transparency among civilian and military nuclear programs will undeniably lower the risk of this threat.

Since an improvised nuclear bomb can be made from highly enriched uranium or plutonium, a terrorist group would not need to take over a nuclear-armed state to posses such a weapon. A thriving black market exists for just the materials a terrorist would need to create a bomb on his or her own. **As of December 2015, the Internal Atomic Energy Agency Incident and Trafficking Database system has recorded a total of 2889 incidents involving thefts, losses, and attempts to illegally sell or traffic fissile materials across international borders.** Therefore, a terrorist attack involving an improvised nuclear device is not inconceivable nor impossible, although it may be improbable.

Currently, the International Atomic Energy Agency (IAEA) does not inspect every nuclear facility globally, thus some countries may not be in accordance with the agency's safeguards and nuclear security measures. Even more striking is that states sometimes fail to account for the totality of the nuclear material at their various facilities. **For instance, in Pakistan, missing weapons-usable materials are rarely reported by the facility and subsequently turn up on the black market.** Another shortcoming of the status quo is that some states with nuclear programs do not have the proper resources to require all employees undergo an extensive security clearance process before being hired. Without a thorough background check, employees at nuclear facilities could act as double agents, working for the facility while simutaneously passing information to terrorist groups.

Much of U.S.' nuclear security and non-proliferation endeavors over the past half-century have been rightly focused on arms control treaties and agreements such as the Nuclear Proliferation Treaty, which deters states from acquiring nuclear capabilities. **However, nuclear security today requires a more proactive approach that must work towards or achieve:**

- **Safer nuclear facilities**. Collaborating with countries like Pakistan, where terrorists are more likely to train. Physically strengthening the security of research reactors and other affiliated facilities would reduce the likelihood of non-state actors reaching those facilities;
- **Tighter border controls**. Reduce the smuggling of nuclear materials and make it extremely difficult for non-state actors to get the necessary components needed to build nuclear devices. This would entail border police and other law enforcement bodies playing a greater role in the prevention of trafficking of radioactive materials; And
- **Better understanding of the threat**. Greater transparency among states would develop a common understanding of the threat and help establish broad political agreements on more effective ways to secure nuclear sites.

The aforementioned efforts require abundant resources and strong domestic political support. While these policy steps may not completely eliminate the threat of nuclear weapons from falling into the hands of radical groups, they would certainly demonstrate a commitment from the international community to confront threats from terrorist groups and signal a step in the right direction.
The United States has shown extraordinary and effective leadership in the past in its non-proliferation policy aiming to avoid the acquisition of nuclear weapons among state actors. The United States surely can rise to the occasion again to ensure global peace and security.

***Jean-Bernard** is a second-year graduate student in the International Affairs master's program at the Elliott School of International Affairs. He received a B.A. in History and Political Science from St. Thomas University in Miami, Florida in 2013. Before enrolling in the MA program, he interned on Capitol Hill and worked for a lobby group in Washington, DC.*

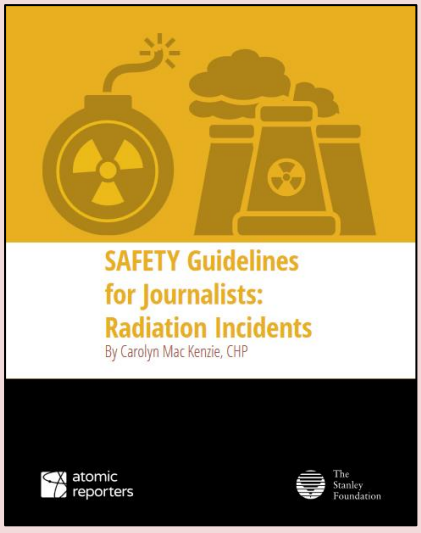
New Delhi Int'l Airport Cargo Area Cordoned Off Over Suspected Radioactive Leak

Source:https://sputniknews.com/asia/201610091046149265-india-new-delhi-radioactive-leak/

Sep 10 – According to media reports the cargo area of T3 terminal of the New Delhi's Indira Gandhi International Airport has been cordoned off on Sunday over a suspected radioactive leak. The entire area has been evacuated with fire fighters and a team from the National Disaster Management Authority being on their way, NDTV broadcaster reported. The leaking package has been reportedly isolated and will be tested.

START research contributes to radiation safety guide

Source: http://www.start.umd.edu/news/start-research-contributes-radiation-safety-guide



Oct 06 – START research contributed to a new resource for journalists and the general public: "Safety Guidelines for Journalists: Radiation Incidents." Published by Atomic Reporters and The Stanley Foundation, the guide and infographic were developed as part of the Rotterdam Nuclear Security Workshop, which START's Steve Sin participated in earlier this year.
The guide is designed to highlight the critical role that journalists play in communicating and responding to nuclear and radiological security issues.
"It was a fascinating topic to discuss," Sin said. "We are always looking at how disasters and incidents could play out, but this time, we approached it with a very specific audience in mind. An audience that can really help affect the outcome in these situations."
The larger research team is continuing its outreach on the topic and will be presenting the journalist recommendations that came out of the Rotterdam workshop, along with the safety guide and infographic, at the International Atomic Energy Agency's International Conference on Nuclear Security in December.

Yes, Japan Could Build Nuclear Weapons (But at What Cost?)

By Nidhi Prasad

Source: http://nationalinterest.org/blog/the-buzz/yes-japan-could-build-nuclear-weapons-what-cost-18019

Oct 12 – George Shultz's axiom that "proliferation begets proliferation" appears to be contested in East Asia.

North Korea conducted its fifth nuclear test on September 9, leaving its non-nuclear Asian neighbors vexed. Japanese Prime Minister Shinzo Abe termed it "totally unacceptable" and has called for strict sanctions. But the international fear of North Korea's nuclear tests triggering a chain of nuclear tests in East Asia or the rise of a nuclear tsunami seems to have been dispelled with the United States' Asian allies favoring "strategic assurance."

Japan and South Korea are American treaty allies. Both have given up the nuclear option in exchange for protection under the US nuclear umbrella. Despite possessing the technical capacity to go nuclear, Japan hasn't displayed intent yet. South Korea's nuclear ambitions have been repeatedly thwarted by the CIA.

North Korea's nuclear provocations and belligerent policies immediately put a spotlight on neighbors like Japan and South Korea. In 1991 Kenneth Waltz famously predicted that Japan would develop an independent nuclear deterrent as a result of an emerging multipolar international system. The North Korean case resurrected this argument — that the proliferation of weapons of mass destruction legitimises Japan's bargaining power for nuclear protection.

If Japan did decide to go nuclear, there are five critical calculations it must keep in mind.

First, Japan would have to overrule its institutional commitment to the 'three non-nuclear principles' declared in 1967 by then prime minister Eisaku Sato as a response to Chinese nuclear tests. This entails that Japan will not produce, possess or position nuclear weapons on its soil. A reinterpretation of Article 9 of the constitution would also be required, which currently does not allow for the maintenance of war potential and offensive weapons.

Japan's constitution allows for a 'minimum level of force' necessary for self-defense. In the past, leaders from the Liberal Democratic Party of Japan have argued in favor of producing tactical nuclear weapons for self-defense purposes. But Japan is part of the Nuclear Non-Proliferation Treaty (NPT). To develop an independent deterrent capability, Japan would have to instigate Article 10 of the NPT to withdraw in light of "extraordinary events." This path would severely damage Japan's diplomatic capital, which hinges on a rigorous pursuit of disarmament diplomacy.

Second, a Japanese shift in nuclear policy would mean backtracking from its vigorous disarmament and non-proliferation strategies. As the only country to be the victim of an atomic bombing, Japan has developed a sense of nuclear aversion that stems from a moral and political rationale. Apart from Hiroshima and Nagasaki, Japan was also a victim of radiation during the 1954 Bikini Atoll incident when the United States tested a hydrogen bomb in the Marshall Islands. Both the institutionalization of peace education and the coalescence of discourses regarding pacifism and nuclear aversion pose a strong block on Japanese leaders arguing for the development of nuclear weapons.

Third, Japan's development of nuclear potential would significantly impact its security alliance with the United States. In 1968 Eisaku Sato defined Japanese nuclear policy based on four pillars, which included a reliance on US extended deterrence. Japan breaking out would mean undermining the foundations of the alliance which have become hardwired into the strategic landscape of the region. Japan's own security policy would also have to be seriously modified.

Fourth, Japan would have to factor in the political ramifications of such a decision, particularly with respect to its relationships with China and South Korea. The outbreak of conflict between the world's second and third largest economic powers would be catastrophic. China's creeping operations in the South and East China Sea could also expand if Japan developed its strategic capabilities. Additionally South Korea may demand its own deterrent capability, which would drastically transform the strategic landscape of East Asia.

Last, the domestic consensus on Japan's nuclear policy would lose stability. During 1968–70 and 1995 Japan conducted domestic debates on the issue, but studies revealed the expensive trade-offs involved with such a pursuit (including the lack of strategic depth). Recently Japan has invested in strengthening the credibility of the US alliance and sought to bolster its alliance contributions through the revision of the US-Japan Defense Cooperation Guidelines in April 2015 rather than simply 'relying' on the US nuclear umbrella. Japan and the United States also began holding regular bilateral nuclear deterrence dialogues in 2010 to enhance allied deterrence.

The political cost of going nuclear has become more complex in the 21st century. Japan has looked towards strengthening its insurance policies such as dependence on multilateral regimes and emphasis on US extension of its deterrent when dealing with nuclear threats. Japan's nuclear insurance against North Korea lies in the strategic assurance of the US nuclear umbrella and the multilateral regimes currently in place.

__Nidhi Prasad__ recently completed a Masters of Philosophy in Japanese Studies at the Centre for East Asian Studies, Jawaharlal Nehru University, New Delhi.

Here's what the earth would be like after a nuclear war

Source: http://tribune.com.pk/story/1198216/heres-earth-like-nuclear-war/

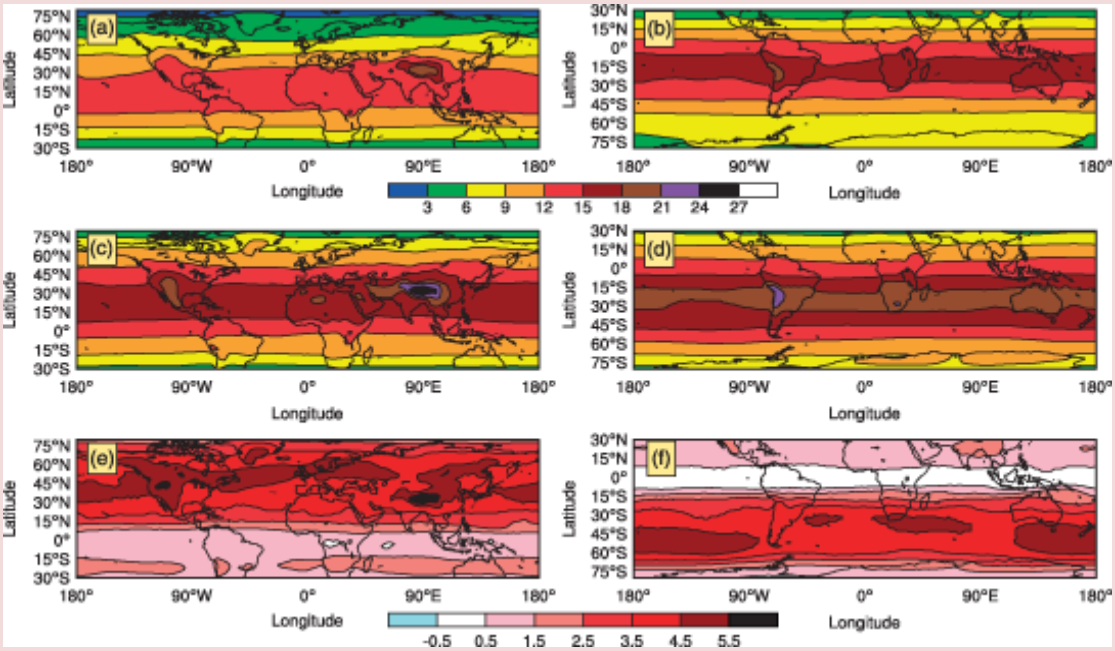
Oct 13 – The Earth could face dire consequences should there be a nuclear war. Knowledge of nuclear consequences will hopefully lead to the realisation that a nuclear war rhetoric is not something to throw around as a threat.

Russian news broadcaster Dmitry Kiselyov has warned of nuclear implications that may result as a consequence of "any impudent behaviour" by Washington towards Moscow.

His remarks came after US Secretary of State John Kerry said that Russia and Syria must be subjected to a war crimes investigation for recent attacks on Syrian civilians.

Kiselyov's remarks can be considered fairly inflammatory between the two nuclear-armed super powers. **A study outlining the effects of a nuclear war show the severe impact on planet earth.**

The study estimated the consequences to the planet after a limited, regional nuclear war, which assessed the impact of 100 nuclear warheads dropping over India and Pakistan — a conflict considerably smaller than a Russo-American one.



UV index in June (left) and December (right) is shown for the control (a, b), the experiment (c, d), and the experiment minus the control (e, f). Values are ensemble averages for year 3.

The results of the nuclear outbreak in the study are extremely unpleasant, to say the least. Along with the hundreds of thousands of deaths, five megatons of black carbon are thrust into the atmosphere. Black carbon absorbs heat from the sun before it reaches the earth, while some of it comes back down as rain.

This has an adverse effect because it causes atmospheric cooling. The effect on the temperature is profound. Earth's falling temperature would cause, among other things, less rain — nine per cent less than usual five years after the strikes — which would have an effect on crops, combined with increased frost.

Over time, Earth's ozone layer will be depleted by around 20 to 25 per cent in five years. More sunburns and skin cancer will occur because of this, and fewer crops will grow. This can lead to food shortages, even famine in some regions.

Therefore, it is fairly reasonable to conclude that, in light of the study, nuclear war is pretty bad and should be refrained from at all costs.

Bacteria can help make underground nuclear waste repositories safer

Source: http://phys.org/news/2016-10-bacteria-underground-nuclear-repositories-safer.html

Oct 17 – Scientists may have found an unexpected ally in the long-term disposal of nuclear waste: bacteria. In a recent study, a research team led by École polytechnique fédérale de Lausanne (EPFL) discovered a microbial community made up of seven species of bacteria that live naturally hundreds of meters underground in the very rock layers that have been chosen to host Swiss nuclear waste. Far from posing a threat, they found that, by tweaking the design of nuclear waste repositories, the bacteria could be used to increase their safety by consuming hydrogen that accumulates as the steel canisters bearing the waste corrode. If left unchecked, the gas pressure build up that could affect the integrity of the host rock. They published their findings in the journal *Nature Communications*.

EPFL notes that **it takes about two hundred thousand years for the**

radioactivity of spent nuclear fuel to revert to the levels of naturally occurring uranium. As a result, most research into the long-term safety of nuclear waste disposal focuses on processes that tick to a slow geological clock: the mechanics of the rock layers that make up the storage site or the robustness of the protective barriers in place that are engineered to contain the radiation. However, all these studies neglect one key factor: biology.

Life underground

Bacteria can be found everywhere, even hundreds of meters underground. And according to Rizlan Bernier-Latmani, the senior author of the study, they will pounce on any available energy source. "In water samples from 300 meters underground at the Mont Terri Rock Laboratory, we unearthed a community bacteria forming a closed food chain. Many of them had never been observed before. Under pristine conditions, the species at the bottom of this bacterial food chain get their energy from hydrogen and sulfate from the host rock, powering the remaining species," she explains.

Adding nuclear waste to the mix changes the conditions altogether. Vitrified, sealed in steel canisters, surrounded by a thick layer of self-sealing bentonite, and buried hundreds of meters underground in geologically stable layers of Opalinus Clay, the radioactive waste is sealed off from the surrounding environment. But the inevitable corrosion of the steel canisters leads to the production of hydrogen gas.

Dropping the pressure

Five years ago, Bernier-Latmani and her researchers took their hypothesis to the field. "For two years, we subjected underground bacteria to increased hydrogen levels, right in the heart of the Opalinus Clay rock at the Mont Terri site," explains Bernier-Latmani. During that time, they monitored the composition of the bacterial population and how they changed individually, both in terms of their potential to support biochemical pathways, and in terms of the proteins they actually produce.

Once the bacteria had consumed all the available oxygen and iron, the researchers observed a shift in their population numbers and in their metabolism. Both were driven by the increased availability of hydrogen gas. "Two of the bacterial species that are able to use hydrogen to drive their metabolisms flourished, while the other species piggybacked on their growth," explains Bernier-Latmani. It was good news, as the proliferation of the bacterial community helped keep the buildup of hydrogen gas at bay.

A biological barrier

So how can these findings be used to make nuclear waste repositories safer? Bernier-Latmani proposes adding a fourth, biological, engineered barrier. "What we could do is to add a layer of porous material between the bentonite and the host rock. This porous layer would provide an ideal niche for bacteria that could feed off of sulfate from the host rock and hydrogen from the corroding canisters," she says.

But one issue still troubles the researcher: genomic studies of the bacterial community suggest that the microorganisms could possess the capacity to transform the hydrogen gas into methane, which would be a less favorable outcome. "We have been trying to provoke methanogenesis at Mont Terri. After half a year, we are still waiting to observe it."

— Read more in Alexandre Bagnoud et al., "Reconstructing a hydrogen-driven microbial metabolic network in Opalinus Clay rock," Nature Communications 7, article number: 12770.

Developing tests for radiation absorbed in nuclear emergency

Source: http://www.homelandsecuritynewswire.com/dr20161018-developing-tests-for-radiation-absorbed-in-nuclear-emergency

Oct 18 – In a large-scale nuclear or radiological emergency, such as a nuclear detonation, hundreds of thousands of people may need medical care for injuries or illness caused by high doses of radiation. To help save as many people as possible and better prepare the nation for the health impacts of such catastrophic emergencies, the U.S. Department of Health and Human Services' (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) will sponsor late-stage

development of two tests, known as biodosimetry tests, which can determine how much radiation a person's body has absorbed.

HHS says that **in a large-scale emergency involving radiation, doctors would need information about how much radiation each survivor has absorbed to determine the type of treatment the person should receive to combat any radiation injuries to internal organs and blood cells.**

Although devices are available to detect radiation externally, such as on skin, there are no biodosimetry tests approved to measure the amount of radiation absorbed into the body.

ASPR's Biomedical Advanced Research and Development Authority (BARDA) will use authority granted under the Project BioShield Act of 2004 to support the tests' late-stage development and potentially purchase tests from one or more of the companies for the Strategic National Stockpile. BARDA will provide more than $22.4 million over two years to DxTerity Diagnostics based near Los Angeles and more than $21.3 million over four years, three months to MRIGlobal of Kansas City, Missouri.

HHS notes that under Project BioShield, the U.S. government can support the late-stage development and procurement of new medical countermeasures — drugs, vaccines, diagnostics, and medical supplies — to mitigate the health impacts associated with chemical, biological, radiological and nuclear threats. With these two biodosimetry tests, BARDA has sponsored development or purchased twenty products using Project BioShield.

The agreements with the two companies support the clinical studies required for the companies to apply for U.S. Food and Drug Administration (FDA) approval of the biodosimetry tests. The work also allows the companies to seek Emergency Use Authorization from FDA if a nuclear or radiological incident occurs prior to full approval of the tests.

Both biodosimetry tests are being designed for use in clinical health care labs and analyze blood samples to measure how genes respond to different amounts of radiation and are expected to generate results in about eight hours and can be used up to seven days after exposure. Both are high throughput tests with the potential to process 400,000 or more tests a week.

Nuclear Accidents and Disasters- Vinca Nuclear Institute, 1958

Source: http://politicsreport.com/article/nuclear-accidents-and-disasters-vinca-nuclear-institute-1958

The 1958 accident at the Vinca Nuclear Institute in what was then Yugoslavia led to **the death of a scientist at the facility as well as emergency surgeries on several others.** The facility was conducting a type of experiment called a "subcritical counting" experiment when power levels began increasing in a heavy water reactor.

The detection equipment at the facility malfunctioned, and scientists didn't realize the power levels were getting dangerously high. No one noticed anything was going wrong until one of the researchers conducting the experiment suddenly smelled ozone, a tell-tale warning sign of a "criticality excursion". Radiation was leaking.

Six of the researchers at the Vinca Nuclear Institute received a dangerously high dose of radiation. **All of them were sent to France for bone marrow transplants, but none of the surgeries were successful**. One of the scientists died from the radiation, and the other five survived despite the failure of the surgery. **One of the six scientists was a woman who went on to have a child later in her life without any trouble.**

This accident was later investigated by international nuclear regulatory officials, and was one of the first nuclear accidents to result in such an investigation. Of course, with the sheer frequency of dangerous or even deadly nuclear accidents going on by 1958, you'd have to conclude that an agency of that sort was probably long overdue. Sadly, in all too many cases, regulatory agencies have served the role of industry lapdog more often than industry watchdog.

Hitachi Starts Providing "Walk-Through Type Explosives Trace Detection System" to Detect the Presence of Explosives in 3 Seconds

Source: http://news.sys-con.com/node/3922684

Sep 29 – Hitachi, Ltd. (TSE:6501) today announced that it will begin providing "walk-through type explosives trace detection system" for critical infrastructure facilities such as power plants and data centers from this October. The system detects explosives in 3 seconds by efficiently collecting the fine particles attached on ID cards and analyzing them with built-in devices. It can screen a maximum of 1,200 individuals per hour without disrupting people flow. As a first step, Hitachi aims to provide this system to critical infrastructure facilities such as power plants and data centers. Hitachi will contribute to improve the safety and security in the future by expanding the applications of this system to public facilities, such as airports, train stations event venues, etc.

In recent years, the need of explosive screening has increased to reinforce management of people flow and to tighten security measures for important infrastructures, public facilities, and event venues. Metal detector, X-ray equipment, and wipe-type explosives detector have been implemented to prevent people from bringing in explosives. However, conventional explosives detection methods are time-consuming because they require human-operations. To reduce the inspection time, Hitachi developed an explosive detection prototype in 2012* in the "Integral promotion of social system reform and research and development project" of MEXT (The Ministry of Education, Culture, Sports, Science and Technology). The development of the current system has been accomplished after system refinement by considering practical use cases through field tests at airports and train stations.

The system enables more sensitive detection by adopting a newly-developed sampling component. A high-speed air flow collects fine explosive particles from an ID card when it is inserted into the authentication unit. In the prior prototype, fine particles were collected by holding the ID card over the reading unit. This product integrates a new sampling component where inserting the card into the authentication unit allows for shorter and more accurate inspections because the air flow hits uniformly the card at a fixed angle. The detection of explosive components from a very small sample is achieved by efficiently collected fine particles and concentrating them in a short period of time.

Prototype boarding gate with built-in explosives detection equipment

In addition, Hitachi downsized the gate width from 35 cm to 29 cm by refining its internal design such as by creating a more compact mass spectrometer for explosive detection and modularizing each unit. The system can run nonstop whole day because it features long-life and high environmental-resistant parts.

Hitachi will exhibit the system at the Special Equipment Exhibition & Conference for Anti-Terrorism 2016 held at Tokyo Big Sight from 19th October (Wed) through 21st (Fri). It will also showcase the system at the Hitachi Social Innovation Forum 2016 TOKYO held at Tokyo International Forum from 27th October (Thu) through 28th (Fri).

Hitachi aims to ensure safety and security in public spaces by providing extensive security

systems that would integrate surveillance cameras, face authentication systems, etc. Hitachi will also help customers and society to solve the issues by providing security systems as part of the basic feature sets of the IoT platform Lumada.

Features of the prototype boarding gate with built-in explosives detection equipment are as described below.

(1) High-speed collection of minute particles adhering to IC cards or portable devices while reading the device

Technology utilizing high speed air current to collect minute particles attached to IC cards or portable devices used as boarding passes, while reading the card or device, was developed. The efficient extraction and collection of the minute particles within a short period of time was achieved by optimizing the timing to generate the air flow, positioning of the pass, and air current speed.

(2) High-speed concentration of the collected particles and high-sensitivity mass spectrometry analysis

In order to achieve high-sensitivity mass spectrometry, it was necessary to release the unnecessary gas to outside the equipment and increase the concentration of the particles since the particles are collected within a large volume of air, cyclone method centrifugal technology was employed to efficiently and quickly separate and collect only the particles from the gas, enabling the particles to be introduced into the mass spectrometer to be collected and concentrated in a short time, thus achieving high sensitivity mass spectrometry.

(3) Internalized compact high-sensitivity mass spectrometer

A linear ion trap type* high sensitivity mass spectrometer which can continuously detect explosive compounds in real-time was employed, and by innovating the assembly of the power and control systems, the size of the equipment was reduced even further to achieve internalization within a boarding gate.

Two bomb attacks take place in Dresden, Germany

Source: http://edition.cnn.com/2016/09/27/europe/bombs-attacks-germany/

Sep 27 – **Security has been stepped up in the German city of Dresden, following two bomb attacks on a mosque and a conference center Monday evening.**

No one was injured in the attacks, which included two homemade devices, according to police.

The bombings come ahead of next weekend's German Unity Day celebrations, which German Chancellor Angela Merkel is expected to attend. The celebrations mark the 26th anniversary of the reunification of East and West Germany.

The explosions -- first at the mosque and then at the International Congress Center -- happened within minutes of each other, leading police to believe they're related.

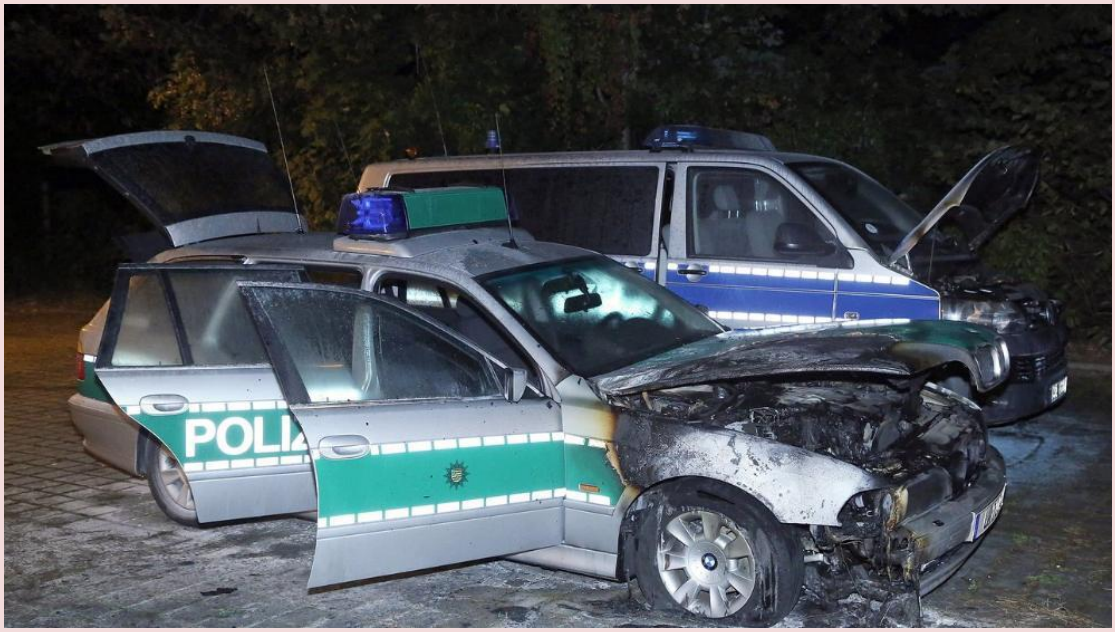
Part of Dresden's Unity Day celebrations were set to be held at the center.

All Muslim institutions in the city are now under increased surveillance, Saxony Interior Minister Markus Ulbig told reporters Tuesday.

It is unclear who is behind the attacks.

"Although no one claimed responsibility for the incident, we must have to consider a xenophobic motive for the attack," Horst Kretzschmar, Dresden's police chief, said in a statement, adding that police were on high alert.

Overnight, Kretzschmar had deployed police personnel to protect Islamic institutions in Dresden as well as the Turkish General Council.



New bomb attacks against three police cars (Dresden – Oct 02, 2016)

Pro-ISIS Supporter Posts New Tutorials On Building Pressure Cooker Bombs

By Anthony Kimery (Editor-in-Chief)

Source: http://www.hstoday.us/single-article/pro-isis-supporter-posts-new-tutorials-on-building-pressure-cooker-bombs/a0dadea68176a1e09a7f9653e3e9a691.html

Sep 29 – In the wake of the bombings in New York and New Jersey, the pro-Islamic State (ISIS) hacking entity Cyber Kahilafah posted new and potentially more deadly tutorials on building pressure cookers bombs using modified cell phones and Bluetooth devices to detonate the bombs remotely, according to the Middle East Media Research Institute (MEMRI), which monitors jihadi social media sites.

US counterterrorism officials told *Homeland Security Today* on background that they're taking this potential new threat "very seriously," as one said. "This shows the growing sophistication of jihadi groups to develop new methods of creating new attack capabilities."

The officials acknowledged that this represents a "serious new threat."

The main suspect in the New York bombings, Ahmad Khan Rahami, was arrested September

19 following a shootout with police in Linden, NJ. Rahami reputedly was identified through a fingerprint and other clues from the cell phone and pressure cooker device found at the 27th Street location in Manhattan.

"The recent pressure cooker bomb tutorial … posted on the Cyber Kahilafah Telegram channel with links to the group's Dark Web website" using modified cell phones and Bluetooth devices to remotely denote the bombs is a new methodology for detonating this type of improvised explosive device (IED), MEMRI said, noting, "The content [of the tutorial] included an image of the booby-trapped pressure cooker found in Manhattan," and that, "One of the videos featured surveillance footage that captured the explosion in Chelsea, NY."

"Since AQAP's *Inspire* Magazine released its infamous article, How To Make A Bomb In Your Mom's Kitchen – Al Qaeda, and now ISIS and other jihadi groups, have been fixated on lone wolf attackers making their own homemade bombs and using them inside the West," MEMRI Executive Director Steve Stalinsky told *Homeland Security Today*. "Examples of this can be found daily on their social media accounts such as the German-based Telegram app which continues to grow in popularity among this group. Just today a jihadi hacker's telegram channel announced that soon it will explain how to install WI-FI in cars to use it for explosions."

According to MEMRI, "On September 26, the pro-ISIS hacking group Cyber Kahilafah announced on its Telegram channel that it will soon publish instructions on how to modify a vehicle for remote operation using Wi-Fi. The group states that such remotely-operated vehicles could be used to spread poisons, gather intelligence, or detonated remotely. The announcement read as follows:"

"In the near future we intend to launch a project that will include instructions on how to modify vehicles for remote operation using a Wi-Fi network and use them for various missions such as gathering intelligence or booby-trapping and detonating them remotely. Additionally, the vehicles could be used to spread poisons while maintaining a safe distance between the target and the mujahid brother. The wireless hardware in the vehicle could also be fitted with equipment to disrupt enemy communications. While in this case we would lose contact with the vehicle, but we will still attain our goal – disrupting enemy communications. The project is still in its infancy, but we will present it once it is finalized."

Although ISIS has not claimed any connection to the New York attacks, the original pressure cooker bomb tutorial was published in a 2010 issue of *Inspire*, the English-language online magazine published by Al Qaeda in the Arabian Peninsula (AQAP).

The article provided detailed instructions on how to make a pressure cooker bomb, and

encouraging "lone wolf" attacks against the United States and its allies.

That same month, the Department of Homeland Security (DHS) issued an "information bulletin" to warn authorities of the dangers of pressure cookers bombs.

By 2004, US counterterrorism officials were so concerned about the potential threat these sorts of

IED attacks DHS issued the bulletin, *Potential Terrorist Use of Pressure Cookers*. The three-page bulletin warned Al Qaeda training camps were teaching jihadists how to build pressure cookers into IEDs "using simple electronic components including, but not limited to, digital watches, garage door openers, cell phones or pagers."

DHS stated it issued the "bulletin to alert frontline border inspectors and agents, state and local officers and other first responders that there is continued interest by terrorist organizations to use innocuous items to package IEDs. A technique commonly taught in Afghan terrorist training camps is the use/conversion of pressure cookers into IEDs."

One of the deadliest pressure cooker bomb attacks was a series of train bombings in Mumbai, India in July 2006 by Lashkar-e-Taiba, an Al Qaeda-affiliated jihadi group. The blast killed more than 200 people and injured 700.

DHS noted that, "In September 2003, India's security forces in Jammu foiled a major terrorist attack during the Navratra celebrations by seizing 40 kg of an explosive, RDX, which was put in two large pressure cookers, and that, "In March 2003, four Algerians, three of whom admitted training in Afghan terror camps, were convicted of plotting to bomb a French Christmas market using pressure cookers packed with explosives."

In February 2002, two pressure cooker bombs were deployed in an attack on Lukla Airport near Mount Everest.

At Christmas 2000, French police thwarted an Al Qaeda attack in Strasbourg using a pressure cooker, after which their popularity soared, especially in jihadi attacks in Afghanistan, Pakistan and India.

In February 2001, Maoist Rebels also used two pressure cooker bombs in an attack on a convoy containing judicial officials in which four escort policemen were killed.

More recently, in July 2011, Army Private Naser Jason Abdo stationed at Fort Hood, Texas, was arrested for planning to bomb a restaurant popular with soldiers. Authorities found pressure cookers and bomb-making materials in his hotel room, along with evidence that he'd used the Al Qaeda tutorial.

Boston Marathon bomber, Dzhokhar Tsarnaev, testified at his 2015 trial that he and his brother learned to make the two pressure cooker bombs they exploded at the marathon from the bomb-making blueprint published by Inspire.

"Typically, these bombs are made by placing TNT or other explosives in a pressure cooker and attaching a blasting cap at the top of the pressure cooker," DHS reported, noting that, "The size of the blast depends on the size of the pressure cooker and the amount of explosive placed inside. Pressure cooker bombs are made with readily available materials and can be as simple or as complex as the builder decides. These types of devices can be initiated using simple electronic components including, but not limited to, digital watches, garage door openers, cell phones or pagers. As a common cooking utensil, the pressure cooker is often overlooked when searching vehicles, residences or merchandise crossing the US borders."

How Police Trace Cellphones in IEDs Like the Ones in NYC

Source: https://www.wired.com/2016/09/police-trace-cellphones-ieds-like-ones-nyc/

Sep 19 – **A cellphone makes a convenient detonator for an improvised explosive device. But it's also one of the most conveniently trackable devices under the eye of American law enforcement.**

Less than 48 hours after a bomb exploded in a dumpster on a streetcorner in the Chelsea neighborhood of New York—and another device a few blocks away failed to explode—police have tracked the attack to New Jersey resident Ahmad Khan Rahami. At least one crucial link that investigators seem to have made came from the cellphone planted in one of the bombs. The incident is a reminder of just how difficult it is to anonymously use a cellphone in America—whether to sell drugs, make an untraceable call to a journalist, or explode a deadly weapon in downtown Manhattan.

"Buying a burner phone correctly isn't easy," says Nicholas Weaver, a security- and privacy-focused computer science researcher at Berkeley University, referring to the pre-paid phones often used by criminals and terrorists. "Using a burner phone correctly isn't easy." For the operator of a remote explosive device, he adds, that means "a cellphone-type detonator is a good robust mechanism….As long as

you don't mind a high probability of getting caught."

According to multiple reports, at least one unexploded bomb—constructed from a pressure cooker and placed in a Chelsea trash can—contained a cellphone that law enforcement was able to recover. And that device, in addition to fingerprints and likely other clues, enabled police to find connections to Rahami's family and then to Rahami himself.

The connection to Rahami's family suggests that a phone call meant to trigger the detonator cellphone may have been made from a phone that also—rather foolishly—called or received calls from Rahami's contacts. A simple, urgent request from the New York Police Department or the FBI to the phone's carrier, with or even without a court order if the telco is sympathetic, would be enough to provide the metadata necessary to identify a suspect.

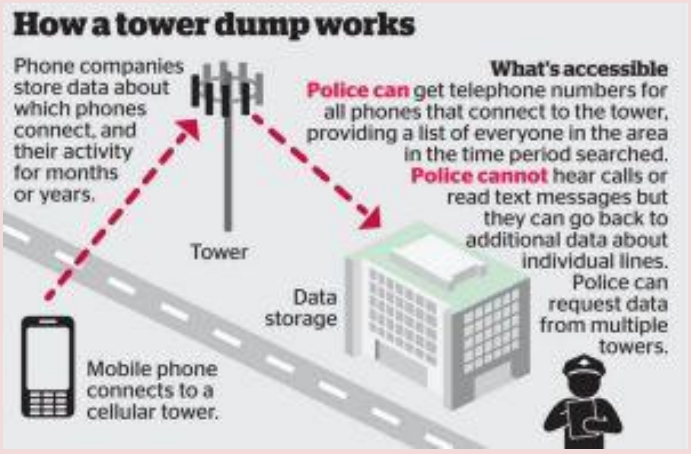
But even if the bomb had exploded *and* Rahami had been careful to use new burner phones on both ends of the detonation call, cops with access to carrier records would likely still have plenty of tools to track down the source of the trigger call, American Civil Liberties Union technologist Chris Soghoian wrote on Twitter.

A phone carrier technique called a tower dump, for instance, offers law enforcement all the records on which phones connected to a particular cell tower during a particular period of time. A tower dump from a certain cell tower in Chelsea on Saturday night would have shown all the phones connecting to the tower, including one that received a phone call and then suddenly disappeared, no longer periodically reporting its location back to the tower. The carrier's records could then lead cops to the phone that called that number and any other numbers connected to it, potentially unraveling an entire terrorist cell or pointing to other detonation calls made from that phone. (New York mayor Bill DeBlasio said in a press conference Monday that no evidence suggests Rahami had any accomplices, and the NYPD declined to comment on its ongoing investigation.)

If the creator of an IED is careful, he or she will buy new burner phones without incriminating call records for both the detonator and the phone intended to call it. But even then, Berkeley's Weaver says, burner phones can be tracked. He points to the example of a case in California last year when police asked AT&T for help tracing a burner phone used in a kidnapping based only on its number. AT&T revealed that the phone was a prepaid TracFone handset, and that it had been activated at a certain Target store. Target then gave the police in-store surveillance footage that helped identify and arrest the alleged kidnapper.

"A burner phone can be a dead end, but that takes more than walking into Target and buying a phone," says Weaver, who has written a guide on how to use burner phones and other anonymity tools to leak information to the press.

Even if a retailer doesn't capture surveillance video of the burner phone's buyer, it might capture his or her credit card number. Or if he or she isn't careful about where the phone is turned on, it can serve as a location beacon, calling out to nearby cell towers and quickly giving police a record of the bomber's location within at least a few hundred feet. Google and its operating system Android, according to one criminal affidavit earlier this year, can also provide police



with location data detailed enough to pinpoint a bank robber inside a bank. "If you're actually trying to do this, you have to do *everything* right to avoid this kind of mistake," says Matt Blaze, a security-focused science professor at the University of Pennsylvania. "One trivial slip-up like appearing on camera or using a credit card or turning it on in your house or using it to make a call to your friend or family member—any one of those large number of things can associate you with that phone."

Tracking cellphone detonators has been so effective that it's even been used by the NSA to identify IEDs in foreign war zones *before* they're detonated. By sifting through call records looking for phones in

potential target areas that have never before placed a call, NSA analysts can find powerful leads on where a bomb might be planted before the detonating call is placed.
So it's no surprise that bomb-detection phone-tracking techniques have found their way in to the domestic fight against terror. If the devices in our pocket are going to betray our privacy every moment they're switched on, it's only fair that they betray the terrorists trying to kill us, too.

Hoaxer told police he planted bomb in hospital - and said it would explode just two minutes later

Source: http://www.mirror.co.uk/news/uk-news/hoaxer-told-police-planted-bomb-8969017

Oct 03 – **A hoaxer called 999, claiming to have planted a bomb in a hospital - and said it was due to explode in two minutes.**
James Wilson followed it up with another emergency call 13 minutes later to complain about the treatment he had received as a patient at the same hospital - Newcastle's Royal Victoria Infirmary.
A court heard the pest was quickly traced and arrested and it was not necessary to evacuate the building.
Prosecutor Emma Dowling told Newcastle Crown Court: "The defendant said, in a very brief call, he had put a bomb in the hospital and it would go off in two minutes."
It was on June 24 that Wilson made the call about the bomb, at 4.26am, reports the Newcastle Chronicle.

A week after the scare, Wilson made another emergency call, claiming he had taken an overdose after drinking three bottles of wine.
When paramedics got to Fawdon, Newcastle, where he was living, they were greeted by him armed with a nine-inch kitchen knife, shouting abuse.
The court heard the medics tried to convince Wilson they were trying to help him but had to back away and call the police after he threw the knife at them.

When police officers arrived they were also greeted by Wilson shouting aggressively and continuously. He was tasered and arrested.
Wilson, who was on a suspended sentence for carrying a knife, pleaded guilty to communicating a bomb hoax and two charges of affray. He was jailed for 25 months.
Recorder Ian Harris said he was satisfied there was no "political or ideological" motivation behind the bomb hoax and accepted Wilson's explanation that it was a cry for help.
But the judge said the call was "mean, selfish and calculated".
He added: "It is fortunate for you that further steps were not taken by the authorities because it was realised rapidly that the call was not a serious call."
The judge said the confrontation with the emergency personnel a week later could have been "lethal" due to the alcohol and presence of the knife.
He added: "Those who are employed to protect and serve the public, ambulance service and police, are entitled to and will receive protection by the courts from people behaving as you did."
Andrew Rutter, defending, said drug and alcohol misuse lie behind Wilson's offending and without it he would be a "decent, ordinary, law abiding member of society."
Mr Rutter said Wilson is not heavily convicted and that professional input to combat his deep seated problems would better serve the public than a prison sentence.

Pentagon Confronts a New Threat From ISIS: Exploding Drones

Source: http://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?_r=0

Oct 11 – **Kurdish forces fighting the Islamic State in northern Iraq last week shot down a small drone the size of a model airplane. They believed it was like the dozens of drones the terrorist organization had been flying for reconnaissance in the area, and they transported it back to their outpost to examine it. But as they were taking it apart, it blew up, killing two Kurdish fighters in what is believed to be one of the first times the Islamic State has successfully used a drone with explosives to kill troops on the battlefield.**

In the last month, the Islamic State has tried to use small drones to launch attacks at least two other times, prompting American commanders in Iraq to issue a warning to forces fighting the group to treat any type of small flying aircraft as a potential explosive device.

The Islamic State has used surveillance drones on the battlefield for some time, but the attacks — all targeting Iraqi troops — have highlighted its success in adapting readily accessible technology into a potentially effective new weapon. American advisers say drones could be deployed against coalition forces by the terrorist group in the battle in Mosul.

For some American military analysts and drone experts, the episodes confirmed their view that the Pentagon — which is still struggling to come up with ways to bring down drones — was slow to anticipate that militants would turn drones into weapons.

"We should have been ready for this, and we weren't," said P. W. Singer, a specialist on robotic weaponry at New America, a think tank in Washington.

Military officials said that the Pentagon has dedicated significant resources to stopping drones, but that few Iraqi and Kurdish units have been provided with the sophisticated devices that the American troops have to disarm them. The officials said they have ordered the Pentagon agency in charge of dealing with explosive devices — known as the Joint Improvised-Threat Defeat Organization — to study ways to thwart hostile drones. This summer, the Pentagon requested an additional $20 million from Congress to help address the problem.

In recent months, the Central Intelligence Agency and the Defense Intelligence Agency both rushed to complete classified assessments about the Islamic State's drone use. And the secretary of the Army, Eric Fanning, recently assigned a special office he had created to respond to emerging threats and to study how to stop drones.

Unlike the American military, which flies drones as large as small passenger planes that need to take off and land on a runway, the Islamic State is using simpler, commercially available drones such as the DJI Phantom, which can be purchased on Amazon. The group attaches small explosive devices to them, essentially making them remotely piloted bombs.

"This is an enemy that learns as it goes along," said Lt. Gen. Sean MacFarland, the top American military commander in Iraq until August.

Of the three known drone attacks in Iraq, only the one involving the Kurdish soldiers caused casualties. "The explosive device inside was disguised as a battery — there was a very small amount of explosives in it, but it was enough to go off and kill them," said a senior American official who had been provided with a detailed report on the episode.

Last week, the Islamic State used a drone strapped with an explosive to attack a checkpoint. The device did not kill anyone but destroyed buildings. On Oct. 1, Iraqi troops shot down a drone that was only a foot long and a foot wide but had a small explosive attached to the top.

"The drone could only hold one small bomb in the middle of it — no bigger load could be on it," said Gen. Tahseen Sayid, a senior Iraqi officer in the area.

The Islamic State first used drones to film suicide car bomb attacks, which militants have posted online. But American and Iraqi commanders said that earlier this year it became clear the group was using drones to help them on the battlefield.

In March, General MacFarland and American military commanders in Baghdad received an intelligence report that the Islamic State had posted surveillance video online that had been taken by a small drone. The video footage showed a newly created series of bases in northern Iraq where American and Iraqi forces were stationed.

Just days after the video was put up, a Katyusha rocket landed in the middle of an outpost of more than 100 American Marines, killing one who was rushing to get others to

shelter in a nearby bunker. **The strike was so accurate that military officials described it as a "golden shot"** to pierce the defenses put in place, and there was speculation that a drone was used in the targeting.

General MacFarland said he did not believe the footage — which did not include positional data like GPS locations — helped militants.

"It couldn't be used for precise targeting," he said in a recent email exchange. "Its value was limited to propaganda."

In the weeks afterward, American forces in the area unleashed a barrage of retaliatory airstrikes against Islamic State fighters who had launched the drone.

"Whatever capability they had, they lost a lot of it," General MacFarland said, referring to the Islamic State's operations in the area.

Throughout the summer, however, American troops in Iraq and Syria reported seeing small **drones hovering near their bases** and around the front lines in northern Iraq. **In August, the Islamic State called on its followers to jury-rig small store-bought drones with grenades or other explosives and use them to launch attacks at the Olympics.** There were ultimately no such attacks at the Games.

On the battlefields in Iraq and Syria, the United States has dedicated resources to take out the Islamic State's drone capabilities. In the past 18 months, the United States has launched at least eight airstrikes that have destroyed Islamic State drones on the ground, according to news releases from the American military command in Baghdad.

Despite these efforts, military analysts believe that drones will continue to be a problem in Iraq, Syria and elsewhere. A new report by the Combating Terrorism Center at West Point says that in the future, off-the-shelf drones used by terrorist groups will be able to carry heavier payloads, fly and loiter longer, venture farther from their controller and employ secure communications links.

The center provided an advance copy of the report to The New York Times.

"The number and sophistication of drones used is also likely to enhance the scope and seriousness of the threat," said Don Rassler, the center's director of strategic initiatives.

Rafael's Innovative Explosives to Reduce Risk for Soldiers

Source: http://i-hls.com/2016/10/rafaels-innovative-explosives-to-reduce-risk-for-soldiers/

Oct 12 – Rafael – Advanced Defense Systems unveiled its new development, the IMPACK, an "indifferent" explosive device designated for use during engineering, infantry and explosion missions.

The device's enhanced security enables its storage, transportation and use without risking an unplanned explosion.

IMPACK was developed in accordance to the IDF's security requirements in order to decrease the risk for soldiers during missions entailing the use of explosives at a environments overloaded with threats.

The IMPACK's unique features conform the IM – STANAG 4439 standard for indifferent explosives and it is resistant to explosions that might be caused by small arms fire, shrapnels, hollow charges etc.

The IMPACK has a security condition in which it is impossible to detonate it. The arming of the explosives takes place during the mission and lasts only a few seconds.

This product was developed by Rafael on the basis of more than 30-year experience in the field.

There are two versions of the IMPACK – with weight of approx. five or 15 kg.

Pentagon: Future of Homemade Bombs Is High-Tech

Source: https://www.wired.com/2012/02/jieddo-high-tech-bombs/

Feb 2012 – Most improvised bombs used by insurgents are decidedly low-tech, jury-rigged affairs. A couple of command wires, some fertilizer chemicals and wooden pressure plates in Afghanistan; in Iraq, leftover mines or plastic explosives often detonated remotely by cellphone. But the Pentagon's bomb squad sees "ever more sophisticated" bombs on the way.

The next generations of homemade bombs, known as Improvised Explosive Devices or IEDs, will feature "hydrogen-based explosives; nanotechnology and flexible electronics," says the Pentagon's Joint IED Defeat Organization, JIEDDO.

That's for starters. "Future bomb makers" will use new energy sources for the bombs, like "microbial fuel cells, non-metallic and solar," JIEDDO writes in a strategy document released late Tuesday for its operations over the next four years. Also on deck for the bombs: "advanced communications (Bluetooth, 4G, Wi-Fi, broadband); optical initiators (using laser or telemetry more than infrared); and highly energetic and molecular materials." Sounds expensive, undercutting one of the bombs' major advantages.

JIEDDO expects the bombs to go off inside the U.S. — as the Times Square would-be-bomber attempted in May 2010 — and may occur "with concurrent cyber attacks." But while the bomb squad has lots of ideas about what the next generation of insurgent bombs contain, it offers few specifics about how to combat them.

JIEDDO has spent over $20 billion since 2004 on a variety of tech to stop the bombs, from sensors mounted on aircraft to find scampering teams of bomb-placers to "Wolfhound" devices to hunt their communications. But bomb attacks are at an all-time high in Afghanistan. And U.S. troops imperiled by the bombs still don't have a bomb detector that outperforms a dog's nose.

Whatever tech it's funded in the past to stop the bombs or find the bombmakers, JIEDDO isn't explaining what it plans on funding in the future. Instead, its strategy document lays out vagaries about what it'll emphasize between now and 2016: "research funding, collaborative development, policy direction, developmental contracts, information sharing, and venture capital investment."

"There is no single solution to defeat the IED," JIEDDO cautions, "because there is no single enemy IED network." There's no chance of actually *stopping* the bombs, which JIEDDO's chief, Army Lt. Gen. Michael Barbaro, likens to the artillery of the 21st century. But mitigating them is "an unceasing effort, making use of the latest technological advances," and requiring the Pentagon to "continually identify likely capability gaps and focus our supporting communities of interest to develop solutions."

In other words: JIEDDO isn't sure yet what technologies it'll fund to stop the bombs of the future. But it has created a handy chart detailing the military's "Future R&D Capability Gaps," which include "pre-detonation" detection; "the ability to locate, avoid, and neutralize IEDs containing nonstandard explosives compounds"; "the ability to neutralize IEDs before detonation or mitigate the effects following detonation"; and more.

"The goal is to provide fielded solutions to the warfighter between four and 24 months from requirements identification," JIEDDO says.

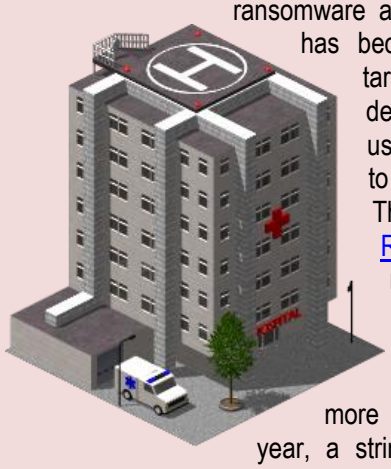
It will probably have less money to spend on closing those gaps, though. The new Pentagon budget cuts JIEDDO's $2.4 billion bankroll by $700 million. And the drawdown of U.S. troops from Afghanistan will likely raise questions in a Congress that has long been skeptical of the organization about the bomb squad's continued value.

Still, JIEDDO has been beating the drum for years on the global proliferation of IEDs, far beyond Iraq and Afghanistan. The reason? Homemade bombs are exceptionally cheap to construct, averaging $265 in 2009, making them cheaper than most iPhones.

And while it's likely that all of the high-tech components that JIEDDO envisions for the next generation of homemade bombs will inevitably get cheaper, it's a little curious that the bomb squad sees the insurgent bombs going high-end. "Flexible electronics" will require a lot more cash than Pakistani fertilizer, a few two-by-fours, wires, a gas can and aluminum foil from a pack of cigarettes. And the gear needed to stop those other bombs is sure to be even more expensive.

McAfee Labs Threats Report: Hospitals Increasingly Targeted by Ransomware

By Amanda Vicinanzo (Online Managing Editor)
Source: http://www.hstoday.us/single-article/mcafee-labs-threats-report-hospitals-increasingly-targeted-by-ransomware/88a600c6f0a76a61f09bde3d98ffdb59.html



Sep 15 – Although no industry is immune from ransomware attacks, the healthcare industry has become an increasingly popular target in 2016 due to medical devices with weak security and the use of legacy systems, according to a new report.

The "McAfee Labs Threats Report: September 2016" revealed explosive growth in ransomware attacks in the past year, with the number of new ransomware samples reaching more than 1.3 million. Earlier in the year, a string of ransomware attacks hit several hospitals across the United States, which impacted patient care and engendered significant financial repercussions.

Ransomware is a form of malware that shuts down a computer system until a ransom is paid. It is typically delivered through phishing or the use of exploit kits. According to the report, in the recent ransomware attacks on hospitals, an employee mistakenly opened a malicious email attachment, which then spurred a chain of events leading to a ransomware infection.

"As targets, hospitals represent an attractive combination of relatively weak data security, complex environments and the urgent need for access to data sources, sometimes in life or death situations," said Vincent Weafer, vice president for Intel Security's McAfee Labs. "The new revelations around the scale of ransomware networks and the emerging focus on hospitals remind us that the cybercrime economy has the capacity and motivation to exploit new industry sectors."

Targeting hospitals can be a very profitable endeavor for ransomware actors, generating as much as $100,000 in ransom payments, according to the report. In February 2016, a California hospital paid $17,000 to hackers to restore their computers systems.

The California hospital attack spurred discussions in underground forums over the ethics of attacks hospitals. The Russian underground, for example, follows a code of conduct that deems hospitals off-limits.

"The cybercriminals' motive is ease of monetization, with less risk," Weafer explained. "Corporations and individuals can easily cancel stolen payment cards soon after a breach is discovered. But you can't change your most personal data or easily replace business plans, contracts, and product designs."

Intel Security outlined several key policies and procedures to reduce the risk of hospitals falling victim to ransomware attacks. The recommendations included keeping patches up-to-date, having a plan of action in the event of an attack, and leveraging application whitelisting, which prevents unauthorized programs from running.

"We will always face challenges as we work to prevent the exfiltration of data, wherever it is stored and however it is handled," Weafer said. "But organizations can learn a great deal from this study's consistent theme of the value of greater visibility into events and incidents across the enterprise, and the longer-term value of the data drawn from this monitoring to construct stronger security postures."

Secure passwords can be sent through the human body, instead of air

Source: http://www.homelandsecuritynewswire.com/dr20160929-secure-passwords-can-be-sent-through-the-human-body-instead-of-air

Sep 29 – Sending a password or secret code over airborne radio waves like WiFi or Bluetooth means anyone can eavesdrop, making those transmissions vulnerable to hackers who can attempt to break the encrypted code.

Now, University of Washington computer scientists and electrical engineers have devised a way to send secure passwords through the human body — using benign, low-frequency transmissions generated by fingerprint sensors and touchpads on consumer devices.

"Fingerprint sensors have so far been used as an input device. What is cool is that we've shown for the first time that fingerprint sensors can be re-purposed to send out information that is confined to the body," said senior author Shyam Gollakota, UW assistant professor of computer science and engineering.

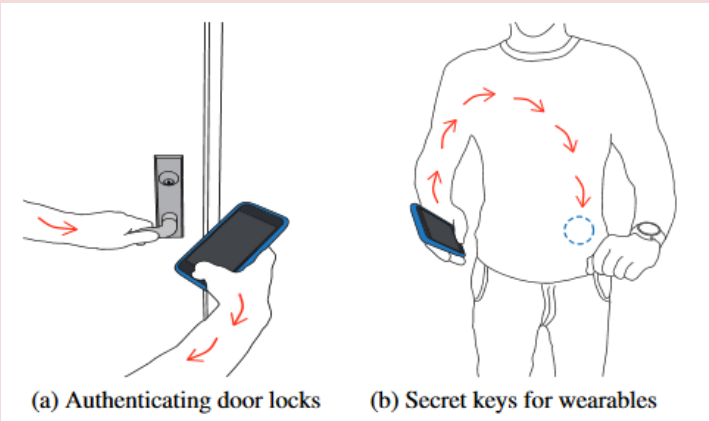


Figure 1: Example applications for on-body communication using the fingerprint sensors on smartphones. The smartphone can securely send information to doorknobs or glucose sensors over the body.

These "on-body" transmissions offer a more secure way to transmit authenticating information between devices that touch parts of your body — such as a smart door lock or wearable medical device — and a phone or device that confirms your identity by asking you to type in a password.

U Washington says that that this new technique, which leverages the signals already generated by fingerprint sensors on smartphones and laptop touchpads to transmit data in new ways, is described in a paper presented in September at the 2016 Association for Computing Machinery's International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2016) in Germany.

"Let's say I want to open a door using an electronic smart lock," said co-lead author Merhdad Hessar, a UW electrical engineering doctoral student. "I can touch the doorknob and touch the fingerprint sensor on my phone and transmit my secret credentials through my body to open the door, without leaking that personal information over the air."

The research team tested the technique on iPhone and other fingerprint sensors, as well as Lenovo laptop trackpads and the Adafruit capacitive touchpad. In tests with 10 different subjects, they were able to generate usable on-body transmissions on people of different heights, weights, and body types. The system also worked when subjects were in motion — including while they walked and moved their arms.

"We showed that it works in different postures like standing, sitting, and sleeping," said co-lead author Vikram Iyer, a UW electrical engineering doctoral student. "We can also get a strong signal throughout your body. The receivers can be anywhere — on your leg, chest, hands — and still work."

The research team from the UW's Networks and Mobile Systems Lab systematically analyzed smartphone sensors to understand which of them generates low-frequency transmissions below 30 megahertz that travel well through the human body but don't propagate over the air.

The researchers found that fingerprint sensors and touchpads generate signals in the 2 to 10 megahertz range and employ capacitive coupling to sense where your finger is in space, and to identify the ridges and valleys that form unique fingerprint patterns.

Normally, sensors use these signals to receive input about your finger. But the UW engineers devised a way to use these signals as output that corresponds to data contained in a password or access code. When entered on a smartphone, data that authenticates your identity can travel securely through your body to a receiver embedded in a device that needs to confirm who you are.

Their process employs a sequence of finger scans to encode and transmit data. Performing a finger scan correlates to a 1-bit of digital data and not performing the scan correlates to a 0-bit.

The technology could also be useful for secure key transmissions to medical devices such as glucose monitors or insulin pumps, which seek to confirm someone's identity before sending or sharing data.

UW notes that the team achieved bit rates of 50 bits per second on laptop touchpads and 25 bits per

second with fingerprint sensors — fast enough to send a simple password or numerical code through the body and to a receiver within seconds.

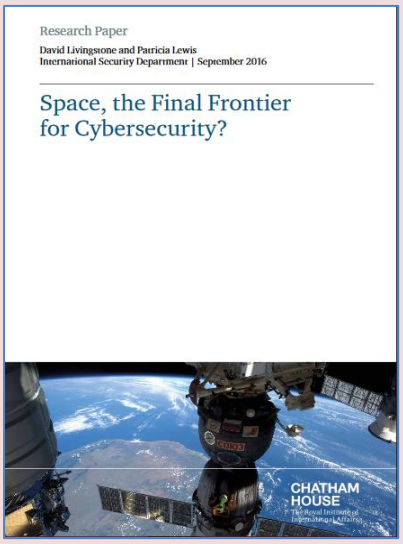
This represents only a first step, **the researchers say. Data can be transmitted through the body even faster if fingerprint sensor manufacturers provide more access to their software.**

— Read more in Mehrdad Hessar et al., "Enabling On-Body Transmissions with Commodity Devices" (paper presented at the UbiComp '16, 12-16 September 2016, Heidelberg, Germany).

Hacked in Space: Are Satellites the Next Cybersecurity Battleground?

Source: http://www.nbcnews.com/tech/security/hacked-space-are-satellites-next-cybersecurity-battleground-n658231

Oct 04 – So many of the mundane, earthly things we rely on, from GPS to making a credit card transaction, are made possible by satellites orbiting beyond that blue sky, thousands of miles outside of Earth.



Space may feel like an untouchable realm, but as the systems we have in place get older, they're becoming even more vulnerable to cybersecurity threats, according to experts.

It's something that needs to be addressed, said Jeff Matthews, director of venture strategy and research at the Space Frontier Foundation, a space advocacy nonprofit.

"Space allows for some very unique business-use cases and opportunities, and when done right, can really go a long way to protecting communication interests and national infrastructure," Matthews told NBC News.

"[However,] we have to be very aware about the information security side up in space and down here."

A recent report from Chatham House, an international affairs think tank, said, "the intersection of space security and cybersecurity is not a new problem, but it has remained largely unrecognized as a potentially significant vulnerability."

Old Systems Face New Threats

Since its introduction into the mainstream more than three decades ago, GPS has now made its way into almost everything, from our phones to our cars and watches.

Americans were given access to global positioning in 1983, after Korean Air Lines Flight 007, traveling to Seoul from New York City, strayed into Soviet airspace and was shot down, killing all 269 people on board. The tragedy prompted President Reagan to speed up his plan for civilian use of GPS.

"If the GPS constellation went down, things would stop flying, maps would stop working," Jim Cantrell, one of the founding members of SpaceX and now CEO of Vector Space Systems, told NBC News.

There are a myriad of uses for the satellites in space, from intelligence to communication, navigation and completing capital transactions, such as when you swipe your credit card at the gas pump.

"Disruption to that, even on a small scale, can have a wide-reaching impact," said Matthews.

What Are the Threats?

David Livingstone, one of the authors of the Chatham House report, told NBC News hackers could pull off a cyberattack by **taking remote control of a satellite or by spoofing or jamming its signals.**

"There is growing vulnerability although there is also growing diversity," Livingstone said. "The cyber threats, whether nation states or organized gangs or terrorists or individual hackers, they are all out there growing even more sophisticated."

Two of the cyber attacks Livingstone mentioned are spoofing and jamming. With spoofing, a hacker can send out fake signals to disguise their activity. Jamming is designed to flood a server with so much traffic it causes an interruption.

So could that 400-pound hacker sitting on his bed — to paraphrase Donald Trump — have the capability to hack a system in space?

"I doubt you would see a lone wolf," Matthews said. "It would have to be a really coordinated attack. I think the low hanging fruit for hackers will be the cube satellites."

The US National Oceanographic and Atmospheric Administration took its Satellite Data Information System offline in September 2014 after an apparent hacking incident, which kept weather agencies around the world from receiving necessary forecasting data for 48 hours, according to the report.

While there are risks with older infrastructure, Livingstone said sees real cybersecurity threats with "the commoditization of space."

Looking to the Future

Protecting the security of the existing infrastructure is one part of the problem.

"It's becoming ubiquitous, and so the question is how do we protect it?" Cantrell asked.

China may have one forward-looking solution. The country launched what is said to be world's first quantum communications satellite into orbit in August.

While many cybersecurity experts adhere to the belief that everything is hackable, a satellite using quantum communications could be pretty close to tamper-proof, thanks to physics.

Quantum entanglement is sort of like sending a message in a soap bubble. If the wrong person pops it, the message will go away, Gregoir Ribordy, co-founder of quantum cryptography firm ID Quantique, told the Wall Street Journal.

Quantum satellites are one viable option for the future, according to Matthews.

However, in the Chatham House report, Livingstone urged the creation of an "international space and cybersecurity regime" comprised of a "limited number of able states and other critical stakeholders," such as those in the space supply chain and insurance industries.

The proposed independent group would be tasked with fostering relationships between key members of the space cyber community, and "provide a vehicle for practical leadership in delivering enhanced security within the whole of the global space sector," the report said.

Getting to Space Is Becoming Easier

Getting to space historically hasn't been easy, but a number of private companies are now making it more cost effective and accessible for those seeking to bring a part of their business out of this world.

And, with new opportunities come new challenges for protecting cyber security in the private sector, such as Cantrell's Vector Space Systems' Galactic Sky program, which helps start-ups leverage the utility of micro satellites through software.

"It is going to be different, but one of the attractions of what we are doing and what makes it more secure is we have known and limited access points," he said. "It is a lot harder to get into the system."

Matthews, of the Space Frontier Foundation, said he wants to see more of a focus being put on cyber security in space and on the ground — whether it's for our older infrastructure or the newer satellites.

"We are on the potential for a revolution to drive space-based security," he said.

Yahoo stealthily scanned customer e-mails on behalf of U.S. intelligence agencies

Source: http://www.homelandsecuritynewswire.com/dr20161004-yahoo-stealthily-scanned-customer-emails-on-behalf-of-u-s-intelligence-agencies

Oct 04 – A report on Tuesday accuses Yahoo of secretly building a customized software program to search all of its customers' incoming e-mails for specific information provided by the U.S. intelligence company.

The Street reports that the company, complying with classified NSA and FBI directives, scanned hundreds of millions of Yahoo Mail accounts.

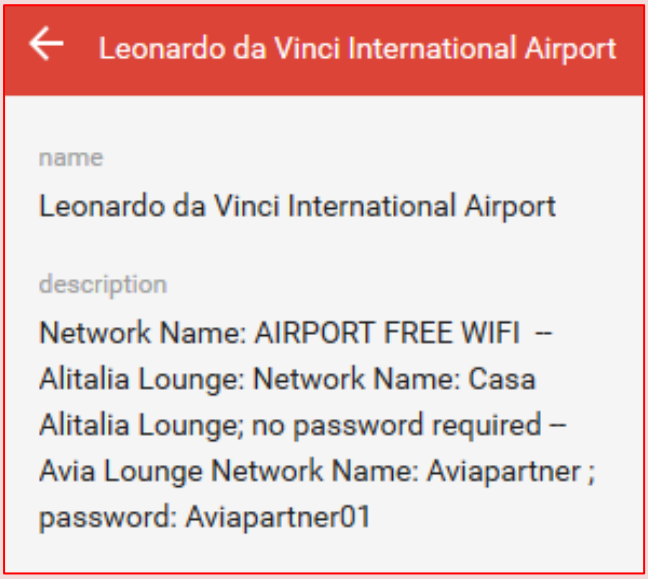
Reuters quoted surveillance experts who said this is the first case to surface of a U.S. Internet company agreeing to a demand by an intelligence agency to search all arriving messages, rather than examining stored messages or scanning a small number of accounts in real time.
Reuters notes that it is not clear what information the NSA and FBI were looking for, but they wanted Yahoo to look for a set of characters. This in all likelihood would be a phrase in an e-mail or an attachment. The new service said it could not say for sure what data Yahoo had handed over to the NSA and the FBI, and whether intelligence officials had made similar demands of other e-mail providers in addition to Yahoo.
The *Verge* reports that two former employees said that Yahoo Chief Executive Marissa Mayer's decision to comply with the directives was a cause of consternation among some senior executives, and that it led to the June 2015 resignation of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook.
"Yahoo is a law abiding company, and complies with the laws of the United States," the company said in a brief statement. Stamos declined to comment, as did the NSA.
The demand to search Yahoo Mail accounts came in the form of a classified directive sent to the company's legal team.
*The Street*notes that U.S. phone and Internet companies have handed over bulk customer data to intelligence agencies. Former government officials and private surveillance experts said, however, that they had not previously seen either such a broad directive for real-time Web collection or one that required the creation of a new computer program.
"I've never seen that, a wiretap in real time on a 'selector'," Albert Gidari, a lawyer who represented phone and Internet companies on surveillance, told Reuters. A selector refers to a type of search term used to zero in on specific information.
He added: "It would be really difficult for a provider to do that."

EDITOR'S COMMENT: Not bad! Now I am sure that NSA and FBI are also notified when a new issue of the Newsletter is uploaded!

Wi-Fi Passwords Of Airports Around The World In A Single Map

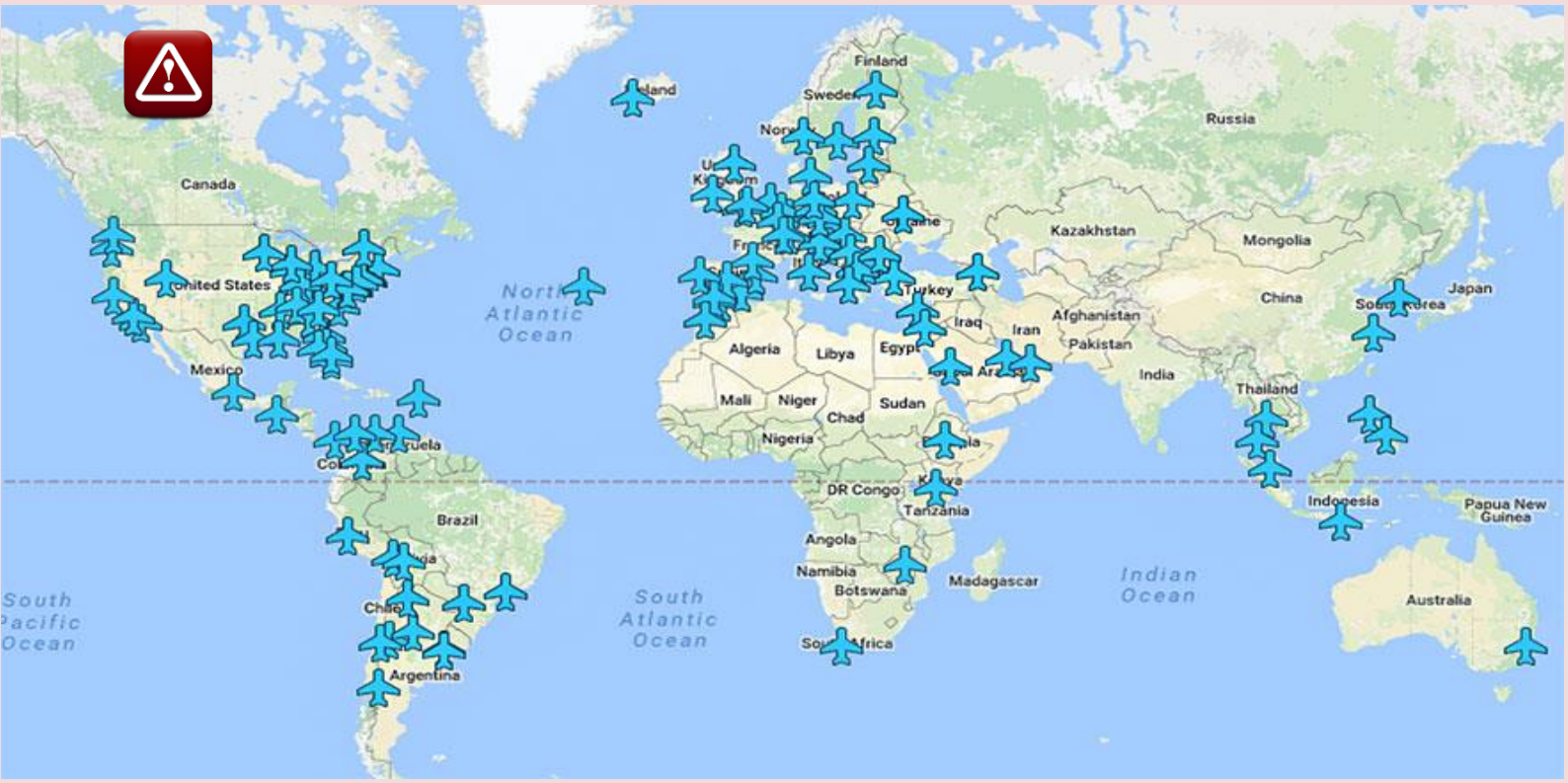
Source: http://www.boredpanda.com/airport-wifi-map-passwords-anil-polat/

Having to spend long hours in an airport without internet access is one of the worst travelling experiences. Luckily, one clever guy came up with a solution to this problem.



Computer security engineer and travel blogger Anil Polat launched an interactive map which offers its users WI-FI passwords of networks in airports all over the world. Also, it's really simple to use. You just have to click on a specific airport and the information about the available connections instantly pop up. Polat updates this map regularly and it already features more than 130 airports across the globe.
For those who will say that it's useless because you need to have internet access to find the WI-FI passwords in the first place, the creator of the map also provides its downloadable offline version as well.

Made by a computer security engineer, the map already has 130 airports, and it's regularly updated with new ones:



Samsung halts production of troubled Galaxy Note 7 phone

Source: http://money.cnn.com/2016/10/09/technology/samsung-galaxy-note-7/index.html

Oct 09 - Samsung has halted production of its Galaxy Note 7 smartphone as fears spread that even replacement versions of the device can burst into flames.

A person familiar with the matter confirmed the temporary suspension to CNN after South Korean news agency Yonhap first reported the news.

The announcement comes after cell phone carriers in the United States and Australia said they would stop offering replacement Note 7s amid concerns that

the new versions are no safer from fire risk than the originals.

Soon after the Galaxy Note 7 hit stores in August, some users reported that their phones were catching fire. Samsung (SSNLF) officially recalled the phones last month, blaming faulty batteries for overheating the phones and causing them to ignite.

Replacement phones were supposed to solve the issue, and users started swapping in their old devices. But some customers have been reporting the same dangerous problems with their new phones.
In the past week, an American user reported his replacement phone caught fire, even though it wasn't plugged in. And on Wednesday, smoke started billowing from a replacement Galaxy Note 7 aboard a Southwest Airline plane before it departed, prompting the flight's cancellation.

EDITOR'S COMMENT: I recently travelled with Alitalia and they make a specific notification before take off to entirely shut the Galaxy 7 down (not in flight mode).

Nuclear Power Plant Disrupted by Cyber Attack

Source: https://threatpost.com/nuclear-power-plant-disrupted-by-cyber-attack/121216/

Oct 11 – The head of an international nuclear energy consortium said this week that a cyber attack caused a "disruption" at a nuclear power plant at some point during the last several years. Yukiya Amano, the head of the International Atomic Energy Agency (IAEA) didn't go into detail about the attack, but warned about the potential of future attacks, stressing on Monday that the idea of cyber attacks that impact nuclear infrastructure isn't an "imaginary risk.'

"This issue of cyber attacks on nuclear-related facilities or activities should be taken very seriously. We never know if we know everything, or if it's the tip of the iceberg," Amano told reporters in Germany. Amano refused to disclose much about the attack, electing not to say where or when it happened, but said it managed to disrupt day-to-day operations at the plant. While it wasn't forced offline, the facility had to take what he called "precautionary measures" to mitigate the attack. It's unclear whether Amano will ever disclose which power plant was affected, or when the attack happened. He told Reuters it occurred "two to three years ago," and declined to get further into the incident, which was previously unknown. Dewan Chowdhury, the founder and CEO of MalCrawler, a service that protects ICS and SCADA systems from malware, said that since there's so little information around the attack, it's too early to pinpoint exactly what happened. "It could be ransomware, malware, a targeted attack; it's anyone's guess what it could be," Chowdhury said. Chowdhury said he hoped the IAEA's confirmation of an attack, even if it was years ago, would help generate awareness around cybersecurity and nuclear issues in the future. That said, he wasn't surprised with Amano's statement. "It's not a surprise that it's happening," Chowdhury said of the disruption. "Personally, I think people aren't disclosing it. It's probably happening more than people think."

Chowdhury pointed out high numbers in the Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) annual Year in Review reports, which regularly breaks down the most targeted critical infrastructure sectors. In 2015, the government organization responded to 295 incidents; the second highest number of incidents by sector, 46, pertained to energy Chowdhury also said the lack of independent agencies aboard, comparable to the United States' Nuclear Regulatory Commission, could be contributing to a diminished number of attack disclosures.

"If the attack had happened in the U.S., the plant would've had to report it to a regulatory board," Chowdhury said, "Overseas, this could be happening all the time but are they forced to tell the world? Tell the governing body of some agency?" "There's the issue, there's no transparency when it comes to a lot of this stuff, especially when it comes to nuclear cooperatives overseas," Chowdhury said. Michael Toecker, the head of Context Industrial Security, a consulting firm that specializes in the cyber security of industrial control systems, said it's unlikely that the IAEA was talking about a new event. He said that more than likely it was an event previously made public that was "run of the mill and handled by plant personnel." Whatever the case, Toecker warned that the IAEA's statement should be taken with a grain of salt. "Nuclear is a nice boogeyman to pair with the cyber boogeyman, and it's very easy to build up a run of the mill virus into an 'attack', especially when you give a nice teaser and no substance," Toecker said, "The public should be wary of individuals who engage in this practice."

It took a few months but ICS-CERT officially confirmed in February there was a connection between BlackEnergy malware and an

outage in Ukraine last December. Attackers obtained legitimate credentials for three regional electric power distribution companies in Ukraine via BlackEnergy-laden phishing emails as a vector. They went on to knock roughly 225,000 customers on the power grid offline. Chatham House, a London-based independent policy institute, warned last fall, prior to the Ukraine incident, that the risk around nuclear infrastructure cyber attacks was growing. **In a 52-page report, the think tank cautioned that the proliferation of supply chain vulnerabilities, paired with a lack of training in the industry, could lead to an attack sooner than later.** Amano claims the IAEA, a nuclear energy watchdog formed by the United Nations in the 1950s, is providing employees with cybersecurity training with radiation detection devices, and a specialized database that includes nuclear information from 131 countries to better educate its workers. The agency held a summit around cybersecurity, the International Conference on Cyber Security in a Nuclear World, in Vienna, in June 2015, to foster dialogue and discuss challenges related to in the industry. Amano told reporters on Monday that he plans to make it a primary topic at another summit, the International Conference on Nuclear Security: Commitments and Actions, slated for December.

Giant cyber wargame with 'dark scenario' of power cuts, ransomware and drones reaches its climax

Source: http://www.zdnet.com/article/giant-cyber-wargame-with-dark-scenario-of-power-cuts-ransomware-and-drones-reaches-its-climax/

Oct 15 – **More than 700 security experts from government agencies, banks, cloud companies, battle fictional cyber-foes.**

More than 700 security experts are battling a fictional cyber crisis featuring power cuts, drones and ransomware as part of the European Union's biggest cyber defence exercise to date. Cyber Europe 2016 kicked off back in April, as since then has been simulating the build up to a major cyber security crisis with a series of fictional attacks on European digital networks, culminating in this week's finale, where security industry experts from more than 300 organisations work together "to ensure business continuity and, ultimately, to safeguard the European Digital Single Market."

"Computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data, sabotage critical infrastructures," warns the scenario.

The cyber wargame involves more than 700 experts across 30 countries from organisations such as governmental Computer Security Incident Response Teams, cybersecurity agencies, plus cloud service providers, IT security companies, banks, energy companies and other critical infrastructure operators, and is organised by the EU Agency for Network and Information Security (ENISA).

It said the exercise "pictures a very dark scenario" inspired by events such as the hacker-generated blackout in Ukraine in 2015 and the dependence on technologies manufactured outside of the EU.

ENISA said the exercise features the Internet of Things, drones, cloud computing, innovative exfiltration vectors, mobile malware and ransomware. For the first time, it said, a fully fledged story was developed with actors, media coverage, simulated companies and social media, so as to make the scenario as realistic as possible to those participating.

Udo Helmbrecht, executive director of ENISA, said: "We are better prepared than we were, but that does not mean we have done enough and the work must continue. Cyber-attacks are more sophisticated than before. Cybersecurity is not a state, it is a process."

The outcomes of Cyber Europe 2016 will be analysed by ENISA and the member states, and detailed lessons learned will be shared with the participants to the exercise. The next Cyber Europe exercise will follow in 2018, with smaller scale exercises planned in between.

Because cyber defence is seen as an pressing international issue there are now a number of these large-scale exercises: NATO runs 'Locked Shields', which involves around 550 people across 26 nationalities, and is based in Tallinn. The US runs the 'Cyber Guard' event every year, which this year saw around 1,000 players dealing with a fictional attack on an oil refinery, power grids, and ports.

CyberSecurity: Now in Medical Equipment as Well

Source: http://i-hls.com/2016/10/cybersecurity-now-in-medical-equipment-as-well/

Oct 16 – **In a letter to diabetes patients, Johnson & Johnson said that OneTouch Ping insulin pump owners who are anxious about a potential hack can stop using the remote, or program the pump to limit the maximum dose of insulin. A security vulnerability was found in the insulin pump that a hacker could exploit to overdose diabetic patients with insulin, though the company describes the risk as low.**

Following the vulnerabilities revealed in 2011 and the 2012 demonstration of a hack at a security conference in Melbourne, Australia, the US Food and Drug Administration began in 2013 formulating cybersecurity guidance for medical device makers.

Since these attacks require technical expertise and sophisticated equipment, "the probability of unauthorized access to the OneTouch Ping system is extremely low", the company said in a warning letter to physicians and patients. In case of piracy, the pumps could see their programming changed to provide a higher than expected dose of insulin.

According to a 2011 Bloomberg News report , a cybersecurity flaw in the device could allow hackers to infuse potentially life-threatening additional doses of insulin without a patient's knowledge. In 2011, however, well-known hacker Jay Radcliffe stunned a Las Vegas tech show audience by gaining access to his own Medtronic insulin pump. They are sold by Animas Corporation, a subsidiary of Johnson & Johnson.

According to crcconnection.com, nearly 114,000 patients use the device in the United States and Canada. At issue is the so-called "Internet of things", according to BlackBerry Chief Security Officer David Kleidermacher and Security Expert Graham Murphy.

It is believed attacks against the medical device could take place from up to 10 meters away, but this could be extended to one or two kilometers with off-the-shelf radio kit. This research highlights why it is so important to wait for vendors, regulators and researchers to fully work on these highly complex devices.

Crisis Scan

Source: https://www.youtube.com/watch?v=f1rG6a_IFeo&feature=youtu.be

Calm Down: New Behavioral Testing Tool Found

Source: http://i-hls.com/2016/09/calm-down-new-behavioral-testing-tool-found/

Sep 25 – **In order to examine reasons for chaos during emergencies and which areas in a building are especially hazardous during an emergency, an international research team exposed 36 participants to an emergency in a three-dimensional virtual environment.**

Each participant simultaneously navigated an avatar through virtual space on a computer screen. The researchers studied the participants' behaviours in several experiments, setting them various tasks under high-stress conditions.

The researchers showed that participants' behaviour in the virtual environment was largely consistent with real-world behaviours. For example, participants were asked to move their avatar through a narrow corridor without bumping into any of the other avatars. The avoidance behaviours seen in the virtual environment were consistent with those observed in a real-life experiment: 95% of participants chose to pass each other on the right-hand side.

According to mpg.de, previous studies have shown that Europeans tend to intuitively walk on the right-hand side. Mehdi Moussaïd, researcher in the Center for Adaptive Rationality at the Max Planck Institute for Human Development explained: "Our experiments have shown that virtual environments can help us investigate human behaviour in emergency situations – something that isn't possible in the real world for ethical and safety reasons".

To find out how the participants reacted in an emergency situation, the researchers simulated an evacuation from a complex building with four exits, only one of which was usable. Although most of the group did not know which was the correct exit, some participants were directed to it by an arrow at the top of their computer screen. Participants knew that some group members were aware of the correct exit, but they did not know who those people were. In addition, the researchers increased the stress level by putting participants under time pressure: Participants had to escape the building within 50 seconds to avoid a substantial loss of points. At the end of the session, the points won were converted into monetary bonuses. Further stress-inducing elements were poor lighting, red blinking lights, and fires at the blocked exits.

The experiments showed that collisions and pushing increased quickly under stress. The most dangerous zones were places where decisions had to be made

and dead ends where participants were forced to turn around and walk back against the flow of the crowd.

"Our findings show that human behaviour in virtual environments is consistent with the behaviours seen in real life. Immersive virtual environments are thus promising tools for behavioural research and beyond. For example, urban planners and architects could use them to test evacuation plans" said Mehdi Moussaïd.

New Security Scanning Method under Development

Source: http://i-hls.com/2016/09/new-security-scanning-method-under-development/

Sep 24 – **Researchers from North Carolina State University have used computer models to demonstrate the possibility of a low-cost security imaging device that makes use of inexpensive radio components.** Functional prototypes are under development and would be orders of magnitude less expensive than existing imaging devices.

Currently, scanning devices that detect hidden weapons or contraband in airports rely on millimeter-wave cameras, which can cost more than $175,000. The cost of the technology is a significant limiting factor in determining where, and whether, to use these scanners.

Brian Floyd, an associate professor of electrical and computer engineering at NC State and lead researcher on the effort: "Our goal is to develop imaging technology that would be functional and affordable, making use of multi-antenna systems".

Before developing a prototype, Floyd wanted to be sure that the idea would work. So, he and a team of students developed both a computer model and algorithms to simulate how – and whether – the new method would produce useful images, it did.

"Our camera uses radio waves instead of light waves," Floyd says. " We can use that camera to see through clothing and identify things that should not be there, like weapons."

Floyd's idea is to create an array of low-cost antennas and radio detectors that can detect and measure the radio waves in a targeted space, effectively acting as an interferometer.

"Objects, such as weapons or smuggled goods, would appear in stark contrast to the human body," says Vikas Chauhan, a Ph.D. student in Floyd's lab who has been investigating the technology. "Based on our simulations, a device using the new technology will work as well as existing interferometers, but would be far less expensive and less bulky than existing millimeter-wave cameras."

According to news.ncsu.edu, the innovation is being developed as part of the NC State Chancellor's Innovation Fund, which funds innovative ideas within the university that could lead to new companies or licensing opportunities.

"We're building prototypes now and looking for corporate partners to help us move the technology to the marketplace," Floyd says.

Radon-222: A Potential Short-Term Earthquake Precursor

By Petraki E[1], Nikolopoulos D[2*], Panagiotaras D[3], Cantzos D[4], Yannakopoulos P[2], Nomicos C[5] and Stonham J[1]

[1]Brunel University, Department of Engineering and Design, Kingston Lane, Uxbridge, Middlesex UB8 3PH, London, UK

[2]TEI of Piraeus, Department of Electronic Computer Systems Engineering, Petrou Ralli and Thivon 250, GR-12244 Aigaleo, Athens, Greece

[3]Department of Mechanical Engineering, Technological Educational Institute (TEI) of Western Greece, Alexandrou 1, 263 34 Patras, Greece

[4]TEI of Piraeus, Department of Automation Engineering, Petrou Ralli and Thivon 250, GR-12244 Aigaleo, Greece

[5]TEI of Athens, Department of Electronic Engineering, Agiou Spyridonos, GR-12243, Aigaleo, Athens, Greece

Corresponding Author : Nikolopoulos D
TEI of Piraeus, Department of Electronic Computer Systems Engineering
Petrou Ralli and Thivon 250, GR-12244 Aigaleo, Athens, Greece
Tel: +0030-210-5381560
Email: dniko@teipir.gr

Received June 07, 2015; **Accepted** June 22, 2015; **Published** June 30, 2015
Citation: Petraki E, Nikolopoulos D, Panagiotaras D, Cantzos D, Yannakopoulos P, et al. (2015) Radon-222: A Potential Short-Term Earthquake Precursor. J Earth Sci Clim Change 6: 282. doi:10.4172/2157-7617.1000282

Source: http://www.omicsonline.org/open-access/radon222-a-potential-shortterm-earthquake-precursor-2157-7617-1000282.php?aid=57605

This paper attempts to survey and catalog published short-term pre-earthquake precursors based on radon gas emissions. A series of papers were searched to collect relevant data, such as the epicentral distance, the extent, time and duration of the radon disturbance and to analyze the precursory value of each observable. In general, enhanced radon emissions have been observed prior to earthquakes and this has been recorded all over the world. The abnormal radon exhalation from the interior of earth has been associated with earthquakes and is considered an important field of research. The proposed physical models attempt to relate the observed radon disturbances with deformations occurring in the earth's crust prior to forthcoming earthquakes. While the models provide some physical explanations, there are many parameters that require further investigation.

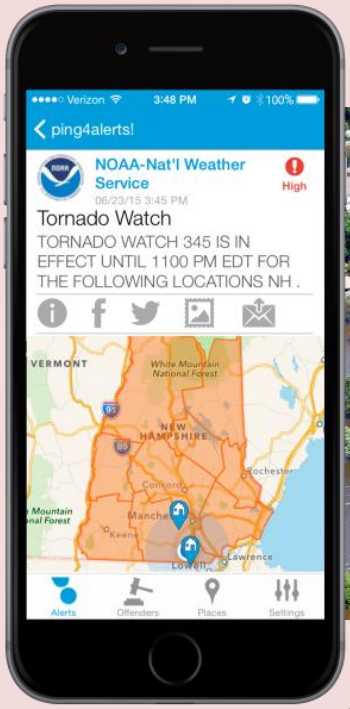
Communication Solution for Flood Threats?

Source: http://i-hls.com/2016/09/communication-solution-for-flood-threats/

Sep 30 – Mobile communications company Ping4Inc. has been awarded a development contract with the U.S. Department of Homeland Security's Science and Technology Directorate to assist first responders in flooding conditions.

As part of the agreement, Ping4 will deliver a geographically precise communications platform that will enable instant notification to first responders about rapidly changing flood conditions.

According to nhbr.com, the platform will send location-specific alerts to first responders' mobile devices in hopes it will prompt immediate action to reduce flood fatalities and property losses. By leveraging the location-based features of smartphones, referred to as geofencing, Ping4 can enable alerts to focus on areas as targeted as a single building, a section of a city, a stretch of highway or an area along an irregular border of the river. The messages will include any combination of text, images, audio and video, making it easier to share potentially life-saving information, says the company.



Dan Cotter, director of the First Responders Group, U.S. Department of Homeland Security: "After heat, floods are the leading cause of weather fatalities in the United States. Last year the National Weather Service reported 176 lives were lost due to floods. We are working with Ping4 to get better flood event information out to our first responders in time to make a difference and reduce the number of lives lost from floods each year. Ping4 brings technology to both geo-target alerts and leverage rich-media that can help make this happen".

Jim Bender, CEO, Ping4: "Emergency alerts are critical to keeping people safe. But if you send mass smartphone alerts to people who aren't directly impacted, they'll quickly get desensitized to these critical communications. That's why Ping4's unique solution—using granular, location-specific technology to alert only people who are in the geo-targeted area of the incident—is so effective. It's also why public safety agencies such as the Department of Homeland Security, and long-standing customers such as the Massachusetts Emergency Management Agency, are using Ping4. We make it easy to instantly send rich-media alerts based only on the relevance and location of mobile devices."

Since 2011, Ping4 has developed and deployed its "ping4alerts!" platform, which is used by multiple states and municipalities throughout the U.S. and globally, says the company.

DHS S&T Selects 10 Start-Ups for First Responder Innovation

Release Date: October 6, 2016

DHS Science & Technology Press Office

Contact: John Verrico, (202) 254-2385

Source: https://www.dhs.gov/science-and-technology/news/2016/10/06/news-release-dhs-st-selects-10-start-ups-first-responder

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has announced the selection of 10 startup companies to be part of *EMERGE 2016: Wearable Technology*, a program designed to bring startups, accelerators, and other strategic partners together in a common research and development effort.

EMERGE 2016: Wearable Technology is focused on wearable technology that can be modified specifically for first responders. First responders have a tremendous need for devices such as body-worn electronics, advance sensors, and integrated voice and data

communications embedded within their gear. Wearables can integrate multiple technologies and minimize additional equipment while maximizing effective response efforts.

"This is an important step for S&T to tap into the innovation ecosystem," said DHS Under Secretary for Science and Technology Dr. Reginald Brothers. "We need to find technologies for first responders that can be integrated directly into their existing gear. The entrepreneurial world is on the leading edge of those inventive solutions."

As part of the program, the 10 startups will have access to first responder feedback, industry partners and investors, and business development educational resources from mentors around the business world. The access and resources available will assist in early market validation efforts, test and evaluation opportunities, and the establishment of a path to introduce their technologies to a variety of markets, including government sector partners.

The selected startups are:

Augmate, New York, New York, developed a provisioning and management platform for wearable devices that helps IT departments track users and their devices, collect sensor data, communicate with workers, and control approved applications and situational connectivity.

CommandWear Systems, Vancouver, British Columbia, Canada, developed a software platform that integrates location and biometrics data from devices to provide personnel tracking, two-way text communication and video sharing to facilitate planning, mission execution, and review operations among teams.

HAAS Alert, Chicago, Illinois / Detroit, Michigan, has a mobile vehicle-to-vehicle communication platform that uses acoustic sensors to pick up environmental and situational noise, and location data to connect people, vehicles, and things in cities, streamlining the disaster and emergency notification process to keep communities safe.

Human Systems Integration, Boston, Massachusetts, developed an integrated system that includes remote physiological monitoring. The system provide a plug and play wearable situational awareness and communications platform.

Lumenus, Los Angeles, California, created smart clothing that uses LED lighting and connectivity to improve visibility of consumers and industrial workers.

LuminAID, Chicago, Illinois, created durable, low cost, and low profile inflatable solar lamps that can be stored efficiently and easily deployed.

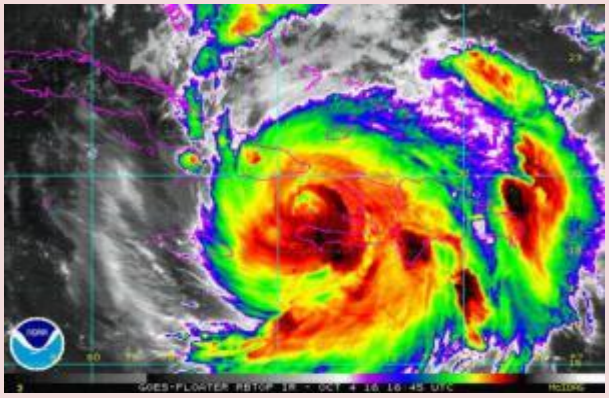
Pear Sports, Los Angeles, California, has a coaching and training application that uses biometric signals like heart rate, VO2 max, location, and environmental data to build training programs that improve the long-term health of users.

Six15 Technologies, Henrietta, New York, produced rugged wearable devices for military and industrial use that stream video and display data using augmented reality overlays for better situational awareness.
Vault RMS, San Diego, California, created a software platform that leverages biometric and situational data from wearable devices and other inputs to build a long-term health profile of workers exposed to health-compromising environments, driving improvements in health, safety, and overall worker productivity.
Visual Semantics, Austin, Texas, created software that integrates with cloud-enabled wearable cameras and heads up displays to provide real-time facial recognition and alerts to help first responders more intelligently assess and react to situations in the field.
The program will conclude with opportunities to explore pilot and path-to-market opportunities with the first responder, corporate, and investor communities later this year.

EMERGE 2016: Wearable Technology is a partnership with the Center for Innovative Technology, a nonprofit corporation in Virginia that is a driver of innovation and entrepreneurship; TechNexus, a venture collaborative that works in conjunction with leading corporations and the global entrepreneurial ecosystem; and the U.S. Department of Energy Pacific Northwest National Laboratory, whose expertise ranges from energy and the environment to national security issues.

Hurricane Matthew's losses could reach $15 billion

Source: http://www.homelandsecuritynewswire.com/dr20161006-hurricane-matthew-s-losses-could-reach-15-billion



Oct 06 – As Hurricane Matthew approaches Florida and the Carolinas, experts estimate that the losses may be as high as $15 billion. They warned that winds, heavy rain, and a storm surge could kill, wash out roads, cut communication links, and cause outages lasting weeks. Twelve U.S. power generators, including two nuclear plants, are in the storm's path. One nuclear facility, NextEra Energy Inc.'s Turkey Point in south Florida, is located just outside of the storm's track.

Deploying robots to Italy's earthquake-ravaged towns

Source: http://www.telegraph.co.uk/news/2016/09/06/italian-firefighters-deploy-drones-and-robots-to-help-earthquake/

Oct 13 – In the aftermath of the earthquake that struck the Italian town of Amatrice and its surrounding region on 24 August 2016, Italian authorities requested the help of the EU-funded TRADR project. The project stepped up to the plate and quickly deployed two Unmanned Ground Vehicles (UGVs) and three Unmanned Aerial Vehicles (UAVs) to the devastated region.

The project, which is developing solutions for robot-assisted disaster management, quickly assembled a multinational team comprising project members from Germany, Italy, and the Czech Republic on short notice and arrived at the earthquake zone on 1 September. This was within forty-eight hours of receiving the official request for assistance from the Italian Fire Brigade.
Cordis says that the team's mission: to use their UGVs and UAVs to provide 3D textured models of two churches located in Amatrice, the Churches of San Francesco and Sant' Agostino, national heritage monuments from the Fourteenth Century. Following the earthquake, they were in a state of partial collapse and in need of shoring up to prevent

potential further destruction, as well as ensure their preservation and restoration as important national monuments. The models would assist Italian authorities plan the shoring operations and assess the state of various objects of cultural value inside the churches, such as valuable frescos.

Mapping the damage

The project team deployed two UGVs into the San Francesco Church, teleoperating them entirely out of line of sight, and partially in collaboration with each other — one UGV provided a view of the other one. This allowed

for easy maneuvering in a very constrained space with low connection bandwidth. One of the UGVs operated in the church continuously for four hours. A UAV was also present for a short time in parallel and provided additional views of the UGVs.

Several flights were carried out on the outside, and one flight inside of each of the two churches. The project team reported that entering the building with a UAV was a tough challenge, which was manageable thanks to collaboration between three UAVs operated in parallel. While one drone was entering through a hole in the roof, the other two were providing simultaneous video feed from different angles that the pilot was able to use as an additional source of orientation. An assistant was continuously watching the video and giving verbal instructions on how to fly.

Mission accomplished

Cordis said thatmost importantly, the mission fulfilled its goal to collect enough data for the construction of high quality textured 3D models that will be invaluable in assessing and repairing the damaged churches over the coming months. The models have been delivered to the Italian Fire Brigade and the Italian Ministry of Culture. The project team also views their ability to quickly come together and deploy a team to the disaster area at such short notice as an important achievement.

Dr. Ivana Kruijff-Korbayová, TRADR project coordinator, has written since the mission to Amatrice that this is the first time to the project's knowledge that several different kinds of robots have been used in collaboration in a real disaster response deployment. She wrote that the Italian Fire Brigade has since expressed their high appreciation for the success of the TRADR mission in Amatrice and have expressed their intention to continue and further deepen their collaborative efforts with the project.

A report about the TRADR deployment to Amatrice will be presented at the 2016 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR) from 23 to 27 October 2016 in Lausanne, Switzerland.

Thousands of people didn't evacuate before Hurricane Matthew. Why not?

By Jennifer Horney

Source: http://www.homelandsecuritynewswire.com/dr20161018-thousands-of-people-didn-t-evacuate-before-hurricane-matthew-why-not

Oct 18 – As Hurricane Matthew approached the Atlantic coast earlier this month, more than 2.5 million people were told to evacuate in Florida, Georgia, South Carolina and North Carolina. Further orders were issued last week in eastern North Carolina, where devastating floods have killed 26 people.

Many residents followed these orders, but others stayed in place. In South Carolina, for example, estimates indicate that about 35 percent of residents under evacuation orders actually left their homes. In highly threatened coastal areas around Charleston and Beaufort the rate was about 50 percent. Florida Governor Rick Scott held multiple briefings urging people to leave storm zones. "Do not surf. Do not go to the beach. This [storm] will kill you," Scott warned.

Hurricane Matthew illustrates the challenges of managing disaster evacuations effectively. Multiple factors influence decisions about evacuating, including residents' genders, how long they have lived in their homes, and their feelings of responsibility for friends and family members who decide not to move. Often people who remain are poor and highly vulnerable.

I study how communities prepare for, respond to and recover from disasters, including hurricanes and wildfires. As a public health researcher, I focus on potential health impacts and look for ways to use data to make communities and individuals more resilient against future disasters.

By understanding who is likely to obey or ignore evacuation orders, authorities can use data to reduce the number of false alarms and concentrate limited resources on groups who are most likely to choose to shelter in place. There is always a potential trade-off between mitigating risk and false alarms, but improved forecasting and better predisaster planning can dramatically reduce potential financial and opportunity costs of evacuating.

Gauging risk

Research shows that several factors strongly influence the decision to evacuate. One of the most important is previous disaster experience. Matthew was the first major hurricane to make landfall on the Atlantic coast of Florida since Wilma in 2005, so it probably was the first such experience for many people who moved there over the following decade.

People's expectations and perceptions of risk also strongly influence their willingness to leave storm zones. Authorities issuing evacuation orders count on residents to remember positive experiences with evacuation or negative experiences from not evacuating.

The problem is that many people have short memories – even in highly vulnerable areas. In Charleston, hurricane evacuation experience during Hurricane Hugo in 1988 strongly predicted evacuation decisions four years later during Hurricane Emily. However, when Hurricane Fran made landfall some 170 miles to the north eight years later, many residents had adjusted their risk perceptions and decided not to evacuate. After all, there hadn't been a bad hurricane in nearly 10 years.

A similar pattern occurred during Hurricane Katrina in 2005. After hundreds of thousands of Louisiana and Mississippi residents evacuated ahead of Hurricane Ivan in 2004, the storm weakened from Category 5 to Category 3 and moved east, making landfall in Baldwin, Alabama and causing minimal damage in Louisiana and Mississippi. As a result, many residents questioned the need to evacuate a year later as Katrina approached.

Protecting the most vulnerable

Cost is typically a weaker predictor of behavior. Generally, up to 75 percent of evacuees can stay with friends or family. But for those who cannot, the costs of fuel, hotel rooms and lost wages can significantly impact family budgets. One recent study calculated that evacuating before a Category 3 hurricane would cost a household approximately US$340 to $525. Timing matters too: Weekend evacuations can cost less, particularly for those without paid sick leave or vacation time.

While these costs may seem modest compared to the risks of staying in place, households that cannot afford to evacuate are also vulnerable in other ways. They are more likely to be located in flood plains or to live in mobile homes, and to lack reliable family transportation.

This is particularly true in the southeastern United States. Between 2000 and 2012 populations in the southeastern Atlantic and Gulf Coast census regions increased nearly twice as fast as the national average. Along with this growth, the proportion of coastal residents who are socially vulnerable – for example, who are elderly, work in low-wage service industry jobs or belong to racial and ethnic minorities – also rose. In eastern North Carolina, a high-poverty region, many residents displaced by post-Matthew flooding cannot afford to replace damaged goods or repair their homes.

But it's not all about money. Residents who have personal transportation and the financial means to evacuate do not always go. Having a strong social support

network tends to correlate positively with good health: For example, if you have a larger and stronger social network you have a lower risk of age-adjusted mortality. But in disasters those social support networks may actually represent responsibilities that prevent people from moving out of harm's way.

This dynamic was clear in New Orleans during Hurricane Katrina. While many residents were criticized for failing to evacuate, they made this decision based on shared norms, local culture and traditions, responsibilities to social networks and a collective history that led them to trust their social networks rather than following instructions from authorities.

While the evacuation of New Orleans for Katrina was widely viewed as a debacle, it actually succeeded on many counts. According to the National Academy of Engineering, more people were able to leave the city in a shorter time than was even thought possible.

However, many who couldn't move were triply vulnerable: they had low incomes or lacked transportation, lived in older homes in flood-prone neighborhoods and had little access to or influence on the development or implementation of local disaster plans and policies. We need to do more work to translate bad experiences like this into policies that can protect residents' health and safety, while also respecting inherent community strengths that sometimes lead to evacuation failures.

Preparing for the next storm

It remains to be seen how well evacuations ahead of Hurricane Matthew succeeded. Available information indicates that 35 to 50 percent of people affected by mandatory evacuation orders throughout the storm zone complied. These rates are comparable to prior evacuations. And as in past storms, some coastal residents moved away from storm zones only to be trapped there by inland flooding.

As of October 16, 44 deaths had been attributed to Hurricane Matthew in the United States. They include residents who drowned after driving onto flooded roads; crush injuries and trauma from trees falling on homes and cars; and inappropriate use of generators. There will be more deaths and injuries as residents return home to clean up and are exposed to fallen power lines, mold and other stresses that exacerbate existing chronic health conditions.

It will take longer to calculate how many deaths and injuries could have been avoided if more people had followed evacuation orders, and to repair storm damage. Rebuilding, and making hard choices about where not to build again, will challenge residents and policymakers. But it is critical to grapple with these issues so we can do a better job responding to the next storm, which likely won't be ten years away.

Jennifer Horney *is Associate Professor of Epidemiology and Biostatictics, Texas A&M University.*

Emergency training for UAE school bus drivers

Source: http://www.thenational.ae/uae/transport/emergency-training-for-uae-school-bus-drivers

Oct 18 – School bus drivers are being given extra training on dealing with emergencies after a serious accident last month.

Forty-seven people, many of them children, were injured in the crash involving two school buses and a public transport bus on Al Khaleej Al Arabi Street.

The school buses involved in the crash were opeated by Al Dhafra Private School and Belvedere British School in Mohammed bin Zayed City, not Emirates Transport.

Thousands of Emirates Transport's school bus drivers have been given training to respond to such incidents in an effort to enhance traffic safety.

The curriculum covers dealing with emergencies and accidents, techniques on safe evacuation of the bus, identifying possible evacuation routes, and ensuring passenger safety, according to Abdullah Al Madhani, the manager of the Emirates Transport training centre.

Emirates Transport, which serves public and private schools, employs 5,072 bus drivers across the country. Of those, 175 were hired in time for the current academic year.

Road safety experts welcomed the course.

"I would hope no driver sets out on the road before the training is complete," said Judith Finnemore,

of Focal Point Management Consultancy.
"I would not like to think of any child, or adult for that matter, setting out on a bus journey with

only part of the training completed. **If it takes three months intensive theory plus practise under the supervision of properly qualified instructors, followed by a very exacting practical examination that has zero tolerance of any misapplication of the learning from the intensive course, I would say it's worth it."**
After the crash last month, Sheikh Mohammed bin Zayed, Crown Prince of Abu Dhabi and Deputy Supreme Commander of the Armed Forces, stressed the importance of school transport safety.
"The relevant authorities are required to put in place an efficient mechanism to ensure the safety and security of schoolchildren and motorists, and prevent the recurrence of such unfortunate incidents," he said.
After an initial investigation, police blamed driver inattention, speeding and tailgating for the three-bus crash.
Thomas Edelmann, founder of Road Safety UAE, also welcomed the extra training for drivers.
"Only selected, qualified, tested and well-trained drivers should be behind the wheel. School bus operators and bus fleet operators invest a lot of money and effort in trying to -establish and maintain high safety levels for their buses and their drivers," he said.
Drivers should undergo a stringent selection process, a detailed assessment of their qualification and driving history, a thorough test of their driving and psychological abilities, and a comprehensive and continuing training regime, he said.

NICS Information Sharing Tool for First Responders Now Available Worldwide

Source: http://www.hstoday.us/single-article/nics-information-sharing-tool-for-first-responders-now-available-worldwide/9255e445b1fd09f6dcae7478da0080a2.html

Oct 08 – **The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) announced on August 8 the availability of a new information sharing tool for first responders across the globe.**
The tool, known as the **Next-Generation Incident Command System (NICS)** is a web-based communication platform that gives first responders real time access to remote experts such as university researchers and topographic experts. This also provides experts with the

opportunity to observe incidents as they develop and volunteer relevant material and resources where necessary.

After successful beta implementation, NICS transitioned to the open-source community for wider accessibly. The platform is now available to any interested party.

"Through strong partnerships within the State of California, responder organizations across the United States, and the State of Victoria in Australia, NICS software is deployed as an operational tool in many first responder communities," said Dan Cotter, director of S&T's First Responders Group. "And now that the platform code has been made available to the open-source community, first responders can leverage this tool from anywhere in the world."

In developing NICS, DHS S&T received contributions from the US Coast Guard Research and Development Center at the Massachusetts Institute of Technology Lincoln Laboratory.

NICS has now been in use for a number of years. Emergency Management Victoria launched NICS back in 2014 when the product was still in the process of research and development. By April 2016, the California Governor's Office of Emergency Services (Cal OES) had also deployed NICS software for California emergency responders.

The NICS vision has been advanced even further through Cal OES, the California Department of Forestry and Fire Protection and various other local fire and law enforcement and emergency management agencies within California and across the United States.

DHS S&T successfully transitioned NICS to operational capability from its stages in research and development in September 2013 during the "Rim" wildland fire in Yosemite National Park where a number of organizations deployed NICS while trying to contain the burning 235,000 acres. NICS was used to make collaborative decisions and to aid in the dissemination of constantly developing information.

NICS code is currently or will soon be available through three venues: GitHub, the US government's open source code repository site; Worldwide Incident Command Services Corporation, which has made the code available under the name RAVEN; and the DHS Homeland Security Information Network.

Survey: 2016 Global Advanced Threat Landscape Survey

Source: http://www.cyberark.com/resource/2016-global-advanced-threat-landscape-survey/

The 10th annual CyberArk Global Advanced Threat Landscape Survey 2016, themed "Cyber Security: Past, Present & Future," examines whether global enterprises are learning and applying lessons from high-profile cyber attacks, and how security priorities and business decision-making are being influenced.
The report is the result of surveys conducted with 750 IT and IT security decision makers from around the world, including C-level executives, directors and department heads, among enterprise organizations, to identify global cyber security trends. Respondents represent a range of public and private organizations across multiple vertical industries from the United States, Europe (France, Germany, United Kingdom), Israel and Asia Pacific (Australia, New Zealand, Singapore).

Highlights include:

- An examination of the impact of increased cyber security awareness on implementation and enforcement of security best practices
- Details on the persistence of bad security habits in critical areas
- Overview of emerging threats, including those impacting critical infrastructure

▶ **Download the full report for more details (source's URL).**

A military view on climate change: It's eroding our national security and we should prepare for it

By David Titley

Source: http://www.homelandsecuritynewswire.com/dr20161007-a-military-view-on-climate-change-it-s-eroding-our-national-security-and-we-should-prepare-for-it

Oct 07 – In this presidential election year we have heard much about some issues, such as immigration and trade, and less about others. **For example, climate change was discussed for an estimated eighty-two seconds in the first presidential debate last week, and for just thirty-seven minutes in all presidential and vice presidential debates since the year 2000.**
Many observers think climate change deserves more attention. They might be surprised to learn that U.S. military leaders and defense planners agree. The armed forces have been studying climate change for years from a perspective that rarely is mentioned in the news: as a national security threat. And they agree that it poses serious risks.
I spent thirty-two years as a meteorologist in the U.S. Navy, where I initiated and led the Navy's Task Force on Climate Change. Here is how military planners see this issue: We know that the climate is changing, we know why it's changing, and we understand that change will have large impacts on our national security. Yet as a nation we still only begrudgingly take precautions.
The Obama administration recently announced several actions that create a framework for addressing climate-driven security threats. But much of the hard work lies ahead – assuming that our next president understands the risks and chooses to act on them.

Climate-related disruptions

Climate change affects our security in two ways. First, it causes stresses such as water shortages and crop failures, which can exacerbate or inflame existing tensions within or between states. These problems can lead to state failure, uncontrolled migration, and ungoverned spaces.
On 21 September the National Intelligence Council issued its most recent report on implications of climate change for U.S. national

security. This document represents the U.S. intelligence community's strategic-level view. It does not come from the Intergovermental Panel on Climate Change, politicians of either party or an advocacy group, but from nonpartisan, senior U.S. intelligence professionals.

The NIC report emphasizes that the problem is not simply climate change, but the interaction of climate with other large-scale demographic and migration trends; its impacts on food, energy and health; and the stresses it will place on societies, especially fragile ones.

As examples the report cites diverse events, ranging from mass protests and violence triggered by water shortages in Mauritania to the possibility that thawing in the Arctic could threaten Russian oil pipelines in the region. Other studies have identified climate change as a contributing factor to events including the civil war in Syria and the Arab Spring uprisings.

Second, climate change is putting our military bases and associated domestic infrastructure in the United States under growing pressure from rising sea levels, "nuisance flooding," increasingly destructive storm surges, intense rainfalls and droughts, and indirect impacts from wildfires. All of these trends make it harder to train our soldiers, sailors, airmen, and marines to deploy and fight the "away" game and to keep our forces ready to deploy.

These changes are not hypothetical. Consider Hurricane Matthew: although we cannot directly attribute this storm to climate change, scientists tell us that as climate change worsens, major hurricanes will become more severe. As Matthew moves up the Atlantic coast, the armed forces are evacuating thousands of service members and dependents out of its path, and the Navy is moving ships out to sea. Other units are preparing to deliver hurricane relief to hard-hit areas.

Many of us who work in this field have written and talked about risks like these for years. Along with 24 other retired senior officers, civilian defense officials from Republican and Democratic administrations, and well-respected academics, I recently signed a consensus statement that calls climate change a strategically significant risk to our national security and international stability. We called for "a robust agenda to both prevent and prepare for climate change risks," and warned that "inaction is not an option."

The "change" part of climate change is critical: The more ability we have to adapt to and manage changes and the rate of change in our climate, the greater our chances are to avoid catastrophic chaos and instability.

Meeting the challenge

Simultaneously with the NIC report on 21 September, the White House released a Presidential Memorandum, or PM, on climate change and national security. This document formally states the administration's position that climate change impacts national security.

Building on past executive orders and policies, it directs senior climate officials at twenty federal agencies to form a working group on climate change and national security, co-chaired by the president's national security adviser and science adviser. This working group will analyze questions such as which countries and regions are most vulnerable to climate change impacts in the near, medium and long term.

That's high-level attention! In the words of a senior administration official, the PM "gives permission" for career civil servants and military professionals to work on this challenge, just as they address myriad other security challenges daily.

But we need to do much more. I am a member of the Climate and Security Advisory Group – a voluntary, nonpartisan group of forty-three U.S.-based military, national security, homeland security, intelligence, and foreign policy experts from a broad range of institutions. We have produced a comprehensive briefing book for the next administration that makes detailed recommendations about how to expand our efforts to address security risks associated with climate change.

Our top-line recommendation is to "mainstream" this issue by ensuring that U.S. leaders consider climate change on an equal basis with more traditional security issues, such as changing demographics, economics, political dynamics and other indicators of instability – as well as with low-probability, high-consequence threats like nuclear proliferation. We also recommend that the next president should designate senior officials in key departments, the intelligence community, the National Security Council and within the Executive Office of the President itself to ensure this intent is carried out.

What's next? As a retired naval officer, I find myself drawing on the words of American naval heroes like Admiral Chester Nimitz. In 1945, while he was commander in

chief of the U.S. Pacific Fleet, Nimitz wrote about a devastating storm near the Philippines that had sunk three ships and seriously damaged more than twenty others, killing and injuring hundreds of sailors. He concluded by observing that:

"The time for taking all measures for a ship's safety is while still able to do so. Nothing is more dangerous than for a seaman to be grudging in taking precautions lest they turn out to have been unnecessary. Safety at sea for a thousand years has depended on exactly the opposite philosophy."

The next president will have a choice to make. One option is to continue down the path that the Obama administration has defined and develop policies, budgets, plans, and programs that flesh out the institutional framework now in place. Alternatively, he or she can call climate change a hoax manufactured by foreign governments and ignore the flashing red lights of increasing risk.

The world's ice caps will not care who is elected or what is said. They will simply continue to melt, as dictated by laws of physics. But Americans will care deeply about our policy response. Our nation's security is at stake.

David Titley *is Professor of Practice in Meteorology & Director Center for Solutions to Weather and Climate Risk, Adjunct Senior Fellow, Center for New American Security, Pennsylvania State University.*

Future of asymmetric warfare: Cyberjacking or ships as WMD?

Source: http://www.sundayguardianlive.com/news/6875-future-asymmetric-warfare-cyberjacking-or-ships-wmd

Oct 09 – Even as the threat of terror looms large on the world, and the global forces prepare themselves for asymmetric warfare, experts fear that terrorists might use new tricks. One of them might be hijacking of tanker merchant vessels and using them as weapons of mass destruction (WMD).

"Countries need to brace themselves for such threats," Deepak Shetty, Director General of Shipping and Secretary to Government of India, Ministry of Shipping, said. He was addressing a select gathering of Indian Naval officers and intelligensia at the Maritime History Society's seminar on ports of India. He also expressed fear of cyberjacking.

But top sources in the Indian Navy told this correspondent that the government already has a contingency plan in place for such an eventuality. A committee called the Committee of Secretaries on Anti-Piracy and Hijacking (COSAPH) at sea has been put in place.

"Just like there is a task force for taking care of plane hijacks, the government has put into operation a similar mechanism for ships, around two years ago. There is an anti-hijack task group in Delhi which deals with piracy and hijacking cases. We are ready for any hijacking scenario," a top official of the Indian Navy said.

Cyberjacking of autonomous, unmanned and remotely controlled ships will be the future threats, he said. He was talking about MUNIN – Maritime Unmanned Navigation through Intelligence in Networks — which is a collaborative research project funded by the European Commission.

"MUNIN aims to develop and verify a concept for an autonomous ship, which is defined as a vessel primarily guided by automated on-board decision systems, but controlled by a remote operator in a shore side control station," its website states. Till date, EU has invested a whopping 20 million Euros for developing the unmanned vessels which can be navigated through drones and other remote controlled equipment.

"If that is one model of what the future holds, it is not immune to cyberjacking. Attackers might just introduce a virus in the system. ," he said.

"The international security environment is fragile due to the threat of terrorism. **It is no more in the realm of fantasy that a merchant tanker can get hijacked and can be used as a Weapon of Mass Destruction (WMD),"** Shetty said.

Maritime power

"For any country to become a maritime power, three factors are crucial. One is a strong network of ports and related infrastructure, the second is flourishing merchant navy and the third is a strong combative Navy," said Commodore G. Prasad.

India was one of the leading countries in the fight againt Somalian pirates for over five years. At one point, India had stationed 42 naval assets to fight the piracy menace in the Gulf of Aden. Safe escorts were provided by Indian Naval warships for merchant vessels.

"There hasn't been a single successful hijack of any ship since 10 July 2012. But a worrying factor now is the resurgence of piracy on the west coast of Africa," he said.

Read also ▶

Paradign shift in legislation

There is a paradigm shift in the outlook towards legislations now, he said. The government is now modifying many legislations, and doing away with many.

"The focus is on ease of doing business. We are at the cusp of rewriting the Merchant Shipping Act. It seeks to replace the existing one even the Coastal Shipping Act is being modified. We are moving ahead with the mantra of simplification, rationalisation and codification to make growth easier," he said.