Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

March 2017

www.cbne-terrorism-newsletter.com

ISIS Targeted Nuclear Reactor Getting Shipment Of Weapons-Grade Uranium

Source: http://dailycaller.com/2017/02/21/isis-targeted-nuclear-reactor-getting-shipment-of-weapons-grade-uranium/

Feb 21 – The U.S. Nuclear Regulatory Commission (NRC) approved the shipment of enough enriched uranium to build five nuclear weapons to a Belgian nuclear facility that was previously targeted by Islamic State-linked terrorists.

Belgium plans to bring 317 pounds of weapons-grade uranium to a nuclear research center in Mol. Security footage caught terrorists casing the facility more than a year ago, according to The New York Times.

Police found surveillance footage of a senior Belgian nuclear official in a raid on the Brussels apartment of alleged terrorist Mohamed Bakkali last February. The footage caused officials to worry ISIS may try to target nuclear infrastructure.

"This will be at least 29 shipments which will have to occur by 2023," Dr. Alan Kuperman, coordinator of the Nuclear Proliferation Prevention Project at the University of Texas, told The Daily Caller News Foundation. "This is the largest amount of bomb grade uranium approved for export in 5 years. It's gonna be used for reactor fuel at this reactor targeted by ISIS."

A successful attempt to steal uranium from a nuclear power plant could have catastrophic consequences, however unlikely.

"There have been other reported threats to Belgian nuclear facilities," Kuperman said. "How hard it would be to make a bomb would depend on how much uranium they get. If you got over 55 pounds of this stuff you could make a Hiroshima like 'gun-type' nuclear weapon relatively easily. If you have less than that, making a bomb is harder, but not impossible for a sophisticated terrorist group."

"This is uranium you could hold in your hand without much real danger to yourself, so it would be easy to transport," Kuperman continued. "If you just put some lead around it, you could get this stuff through most radiation detectors. Any amount of uranium of more than 11 pounds is considered to be a serious risk by the U.S. government."

Last August, Kuperman filed a petition against the uranium export application, claiming that aspects of it were illegal. U.S. officials canceled the shipment last February, about one month before a series of deadly terror attacks in Brussels.

"Under U.S. law, the NRC has the authority to say yes or no to this," Kuperman noted. "The NRC decided to be deferential to the industry. They did take some action to limit the license, reducing it from 11 to 6 years."

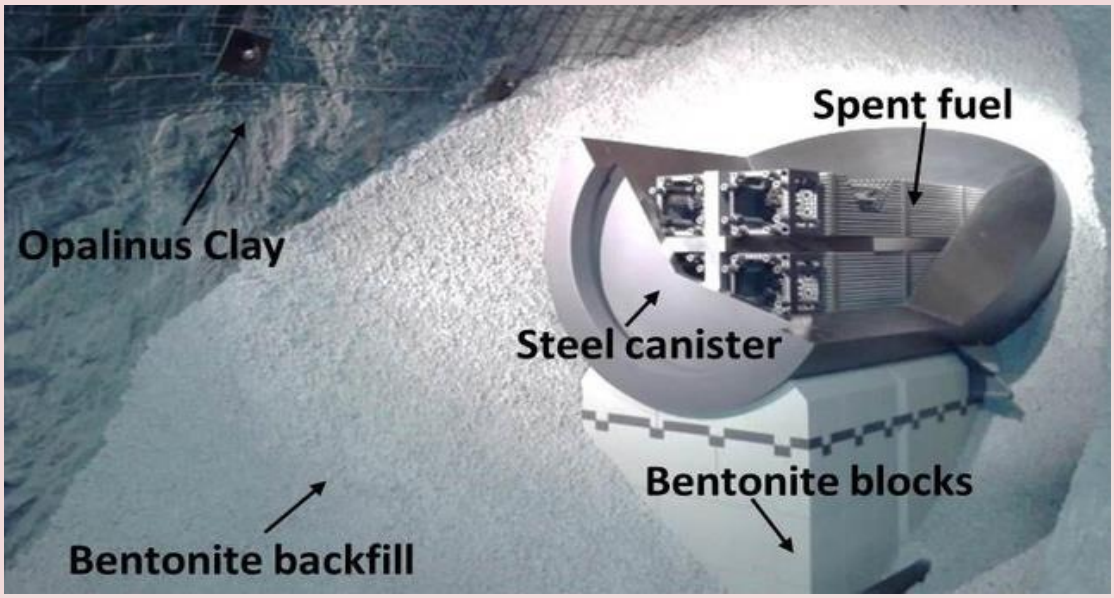
Official correspondences shows the Belgian government asked America's NRC and National Nuclear Security Administration to suspend its weapons-grade uranium order to fuel a nuclear research center in Mol. Belgian officials only cancelled the uranium order so the country could restructure how it would receive the enriched uranium.

France has a similar high performance reactor that runs on highly enriched American-supplied uranium.

Identifying the right sites for storing radioactive waste

Source: http://www.homelandsecuritynewswire.com/dr20170224-identifying-the-right-sites-for-storing-radioactive-waste

Feb 24 – **An EPFL research project has developed a detailed profile of the sites selected to store radioactive waste from Swiss nuclear power plants.** The project also helps identify sites that meet both safety and feasibility requirements.



"Radioactive waste containers are safer the deeper they are buried in rock, but that makes the process much more technically challenging too. I had to consider both of these factors in my thesis, while maintaining a very long-term perspective," says Valentina Favero, a civil engineer and a researcher in EPFL's Laboratory of Soil Mechanics (LMS) who passed her Ph.D. oral exam on 16 January. Her public defense will take place on 3 March at EPFL.

"Favero's findings will play a role in selecting radioactive waste storage sites in Switzerland," says Professor Lyesse Laloui, one of her Ph.D. advisors and head of the LMS. "Her work is sure to have major scientific implications and a significant impact on society."

EPFL notes that in 2008, the National Cooperative for the Disposal of Radioactive Waste (NAGRA) identified six regions in Switzerland, approved by the Federal Council, which could be used to store radioactive waste. Since then, the list has been whittled down to two regions – northeast Zurich and eastern Jura (Aargau) – on the basis of work done by Favero for her Ph.D.. According to Favero, these two sites meet the safety and feasibility requirements of storing highly radioactive waste from Swiss nuclear power plants, as well as low-activity waste, which is produced by medical, research and engineering activities. But Favero's contributions do not end there: her research will also be used in a more detailed study of the sites

approved by the Federal Council during the next step of the selection process. This study was granted financial support from NAGRA.

Detailed analysis of Opalinus clay

What was Favero's approach in her Ph.D.? First, she learned more about the properties of Opalinus clay, which is the type of rock commonly used in Switzerland for storing radioactive waste. She studied the clay's characteristics at different depths in the six regions short-listed by NAGRA. This was meticulous work, as the clay's properties vary with depth.

Favero noted all of the clay's physical, mechanical, and chemical features, and studied how the heat given off by radioactive waste containers affects both the clay and the materials (such as bentonite) used to surround the canisters – materials that may expand or contract in the presence of heat. She also identified the chemical composition of the liquid found in the clay's pores, since the composition may change in response to heat. She needed to investigate other hydraulic properties of rocks as well, including "suction," which refers to rocks decreasing in volume when they become partially saturated. In order to see the big picture – how these properties, taken together, could lead to radiation leaks – Favero had to crosslink her data. That was a laborious task, but it led to one of the key outcomes of her Ph.D.

Desaturation and convergence

"The deeper you go, the more rigid and impermeable the rocks are. And that's exactly what we want – a solid barrier between us and the radioactive waste. But the technical challenges also increase the further down you go," says Favero. Even the process of drilling the tunnel that the radioactive waste containers will go through will affect how the surrounding rocks behave.

This led Favero to analyze how the materials will react during the various phases of this process: "Rocks located at the upper end of the tunnel will be exposed to air," she explains. "That will lead to desaturation, in which some of the water held in the rocks evaporates. As they dry out, the materials could crack, which would make them more permeable. Yet we need impermeable rocks to achieve an effective seal."

EPFL says that the researcher carefully studied this phenomenon and the related risks. Leaving no stone unturned, Favero also looked at the redistribution of forces when the tunnel is dug. This is called convergence, and it refers to the tunnel's tendency to collapse on itself. The deeper the tunnel, the greater the convergence.

Favero's exhaustive research was instrumental for the NAGRA in selecting the best two sites for storing radioactive waste in Switzerland and determining the safest and most technically feasible depth at which to place the steel canisters.

US 'nuclear sniffer' plane flies to Norway - where radiation particles spreading across Europe were first detected - as mystery still surrounds the source

Source: http://www.dailymail.co.uk/news/article-4250098/US-nuclear-sniffer-plane-flies-Norway.html#ixzz4ZyHfp6U8

Feb 22 – **A US Air Force 'sniffer' plane which took off from Sussex today was on a mission to find evidence of nuclear activity or explosion, according to strong rumours.**

The **WC-135 Constant Phoenix**, which is specially modified to collect atmospheric samples, flew out of RAF Mildenhall on operational sorties.

The specialist equipment enables the crew to detect radioactive debris 'clouds' in real time is believed to be heading towards northern Europe and the Barents Sea.

News of the deployment comes amid claims Russia may be testing

nuclear weapons, either to the east or in the arctic, after a spike in radioactivity was reported.
According to spotters a second 'spy' plane was also deployed from Mildenhall.
It is not the first time the Constant Phoenix has visited the British airbase, but the latest deployment reflects growing concern about an alleged spike in iodine levels recorded in northern Europe.
This has fuelled speculation that the WC-135 has been called in to investigate the cause of the higher-than-normal levels of Iodine-131.

Air quality stations across the continent detected traces of radioactive Iodine-131 in January and February, which seem to have come from eastern Europe.
The high levels of Iodine-131 has led some to suggest Putin is testing nuclear weapons in Novaya Zemlya near the Arctic.
However, the CTBTO (Comprehensive Nuclear-Test-Ban Treaty Organisation) ruled out a nuclear test had recently taken place.
Similar aircraft were used in the wake of the Chernobyl nuclear plant disaster in the Soviet Union in 1986 and the Fukushima incident in Japan six years ago by collecting particles and chemical substances in the atmosphere, days, weeks and months after they were dispersed.
The aircraft is equipped with external flow-through devices which collect particulates on filter paper and on board among its crew are special equipment operators from the Air Force Technical Applications Center.
On operational sorties like today's from RAF Mildenhall the crew is normally minimized to pilots, navigator, and special equipment operators, to reduce radiation exposure to mission-essential personnel only.
In a statement on Monday, the CTBTO said: 'If a nuclear test were to take place that releases I-131 it would also be expected to release many other radioactive isotopes
'Thus the CTBTO measures isotopes. No other nuclear fission isotopes have been measured at elevated levels in conjunction with I-131 in Europe so far.'
The organisation, which operates a worldwide monitoring system, said that it was not concerned about the reports of Iodine-131 in Europe.
'No detections above typical local historical levels have been observed,' the CTBTO said.
The deployment of the WC-135 aircraft, which detects and identifies explosions from the air and was used after the Chernobyl disaster in the Soviet Ukraine in 1986, adds weight to the argument.

It's arrival comes amid tense times between Russia and the West, with America's highest ranking military officer General Joe Dunford comparing the political climate to that during the Cold War.
He said that his meeting with General Valeriy Gerasimov, his counterpart in the Kremlin, is 'absolutely critical' as the tension between the two nations verges on breaking point.
It comes after two Russian jets flew low over a Royal Navy destroyer docked off the coast of Romania in a show of force branded 'unsafe and unprofessional' by Navy officers.
And a Russian spy ship armed with surface-to-air missiles with a crew of 200 sailed within 30 miles of a key US submarine base on the Connecticut coastline.
Scores of people filmed a mysterious light travelling through the sky at the weekend and the US Navy released a statement saying its testing of two Trident missiles was 'not in response to any world events'

WHY IS IODINE-131 DANGEROUS?

Iodine-131 has a very short half life of just eight days, making it very radioactive.

When it is present in high levels in the environment, it contaminates food.

After it is swallowed it will accumulate in the thyroid.

As it decays, it damages body tissue and can cause thyroid cancer.

However levels present in the atmosphere today are too low to be damaging.

The US Navy have been contacted for comment on the WC-135 but it has not yet released any official comment on the purpose of its mission.
And while it is not unheard of for the planes to fly to Europe, missions are rare and its arrival coincides with the detection of Iodine-131.
It was first recorded in Norway and have now been found in Poland, Czech Republic, Germany, France and Spain.
The isotope has a half-life of only eight days, which suggests the particles must have entered the atmosphere after a recent event.
The pattern of movement of the particles suggests they may have originated in Eastern Europe, according to the Norwegian Radiation Protection Authority (NRPA).
'It was rough weather in the period when the measurements were made, so we can't trace the release back to a particular location,' Astrid Liland, head of emergency preparedness at the NRPA, told the Barents Observer.
'Measurements from several places in Europe might indicate it comes from Eastern Europe.
'Increased levels of radioactive iodine in air were made in northern-Norway, northern-Finland and Poland in week two, and in other European countries the following two weeks.'
She said it is difficult to pinpoint where the radioactive material came from.
It's possible that the particles could have come from an incident at a nuclear reactor.
An explosion at a plant run by French firm EDF – just 75 miles across the Channel – added to concerns over nuclear safety earlier this month.
The company, which is planning Britain's first nuclear power station in a generation, was forced to shut down its nuclear reactor at the Flamanville plant in Normandy after the blast caused a fire that left five people suffering from smoke inhalation.
But the compounds may also have also come from an Iodine plant. The isotope Iodine-131 is used in medicine to treat to thyroid problems and is produced commercially across Europe.
Iodine-131 can cause harm because it has a very short half life of just eight days, making it very radioactive.
When it is present in high levels in the environment, it can contaminate food and after it is swallowed it accumulates in the thyroid.
As it decays, it damages body tissue and can cause thyroid cancer.
However levels present in the atmosphere today are too low to be damaging, according to Ms Liland.
She said: 'We do measure small amounts of radioactivity in air from time to time because we have very sensitive measuring equipment.
'The measurements at Svanhovd in January were very, very low. So were the measurements made in neighbouring countries, like Finland.
'The levels raise no concern for humans or the environment.'

HOW THE 'SNIFFER' TESTS THE AIR

The WC-135 is known as the 'sniffer' or 'weather bird' by its crews because of its unique role in the sky.
It gathers effluent gasses with two scoops on the sides of the fuselage, which then trap fallout particles on filters that the crew can analyse in real time.
They can then use the data to confirm the presence of nuclear fallout and possibly determine the characteristics of the warhead involved.
It can use the materials in the air to confirm the type of explosion, for example, whether it is from a warhead or a power plant.
The WC-135 can also be used to track radioactive activity, which it did after the Chernobyl disaster in the Soviet Union in 1986 and Fukushima in 2011.
One was also deployed near North Korea in anticipation of Kim Jong-un's rocket launches.
A WC-135 was also seen transiting into UK airspace in August 2013 raising speculation it was used in Syria after claims chemical weapons have been used.
The plane has a maximum crew of 33. However, it usually flies with a minimal crew to lessen the risk of chemical exposure.

What's New on REMM?

U.S. Department of Health & Human Services
REMM RADIATION EMERGENCY MEDICAL MANAGEMENT
Guidance on Diagnosis and Treatment for Healthcare Providers
• Understand Radiation
• Plan Ahead
• Practice Teamwork
• Work Safely

August, 2016

- New York City gave REMM permission to host and publish their "Field Guide for Health and Safety Officers: Radiological Incidents".
  - This is an extraordinary asset for local planners and first responders.
- Scientific Experiments to Operational Tactics for the First 100 Minutes After an Outdoor Explosive Radiological Dispersal Device
  - REMM links to Dr. Stephen Musolino's outstanding lecture at the 2016 NCRP Annual Meeting, Bethesda, MD. (YouTube 29:04)
- Major update to the Myeloid Cytokines page reflecting FDA approval of a new drug for neutropenia. This was accompanied by required changes to
  - REMM's prototype Hospital Orders for radiation injury admission
  - Mobile REMM countermeasures page
- Significant updates to the Protective Action Guides (PAGs) page, reflecting ongoing updates to the EPA guidance
- Major update to REMM's Potassium Iodide page
  - Reflects FDA guidance on liquid countermeasures for children and other prescribing information.
- Major addition to the multimedia assets content with tools created by CDC
- Major update to the content on the Nuclear Power Plant page
- Complete redrafting of the Labels and Placards page, with key, new graphics
- Major update to the Planners page, including reorganized references to the National Response Framework
- Link to important new document about Electromagnetic Pulse (EMP) is included on the REMM nuclear detonation page
- Link to very important new reference from HHS (Coleman CN, Koerner JF) about using biodosimetry following a large scale radiation incident is included on the REMM biodosimetry references page.
- Update to the retrospective assessment of dose information on the software tools page
- Update of HHS information including TRACIE (Technical Resources, Assistance Center and Information Exchange)

- New links to complete set of IOM (National Academies) monographs on "Crisis Standards of Care", (see volumes 1-7). Links are on REMM Crisis Standards of Care page.

How US nuclear force modernization is undermining strategic stability: The burst-height compensating super-fuze

By Hans M. Kristensen, Matthew McKinzie and Theodore A. Posto

Source: http://thebulletin.org/how-us-nuclear-force-modernization-undermining-strategic-stability-burst-height-compensating-super10578

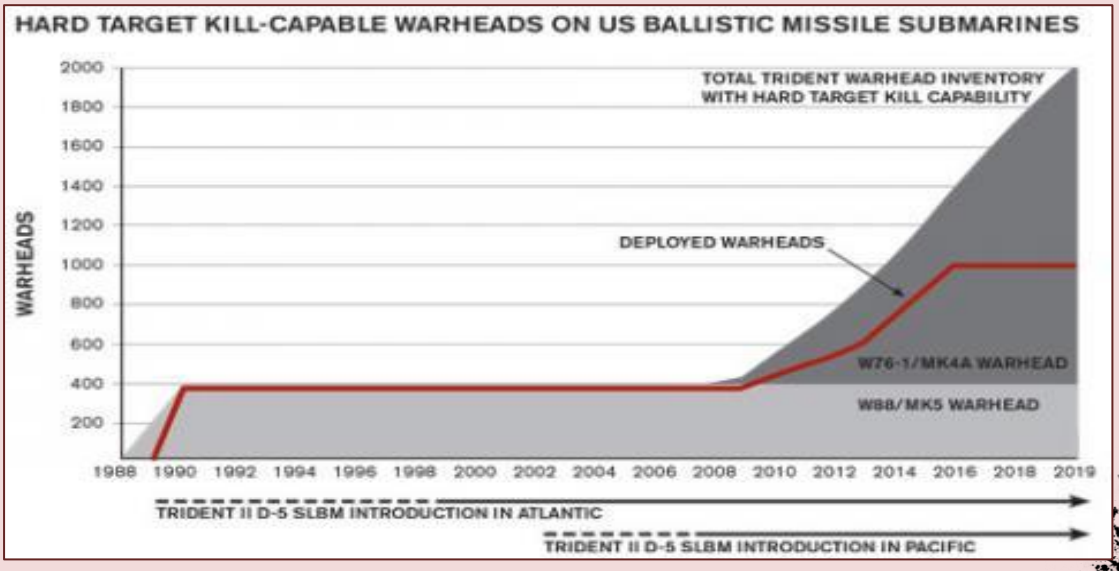
Mar 01 – The US nuclear forces modernization program has been portrayed to the public as an effort to ensure the reliability and safety of warheads in the US nuclear arsenal, rather than to enhance their military capabilities. In reality, however, that program has implemented revolutionary new technologies that will vastly increase the targeting capability of the US ballistic missile arsenal. This increase in capability is astonishing—boosting the overall killing power of existing US ballistic missile forces by a factor of roughly three—and it creates exactly what one would expect to see, if a nuclear-armed state were planning to have the capacity to fight and win a nuclear war by disarming enemies with a surprise first strike.

Because of improvements in the killing power of US submarine-launched ballistic missiles, those submarines now patrol with more than three times the number of warheads needed to destroy the entire fleet of Russian land-based missiles in their silos. US submarine-based missiles can carry multiple warheads, so hundreds of others, now in storage, could be added to the submarine-based missile force, making it all the more lethal.

The revolutionary increase in the lethality of submarine-borne US nuclear forces comes from a "super-fuze" device that since 2009 has been incorporated into the Navy's W76-1/Mk4A warhead as part of a decade-long life-extension program. We estimate that all warheads deployed on US ballistic missile submarines now have this fuzing capability. Because the innovations in the super-fuze appear, to the non-technical eye, to be minor, policymakers outside of the US government (and probably inside the government as well) have completely missed its revolutionary impact on military capabilities and its important implications for global security.

Before the invention of this new fuzing mechanism, even the most accurate ballistic missile warheads might not detonate close enough to targets hardened against nuclear attack to destroy them. But the new super-fuze is designed to destroy fixed targets by detonating above and around a target in a much more effective way. Warheads that would otherwise overfly a target and land too far away will now, because of the new fuzing system, detonate above the target.

FIGURE 1. The deployment of the new MC4700 arming, fuzing, and firing system on the W76-1/Mk4A significantly increases the number of hard target kill-capable warheads on US ballistic missile submarines.



The result of this fuzing scheme is a significant increase in the probability that a warhead will explode close enough to destroy the target even though the accuracy of the missile-warhead system has itself not improved.

As a consequence, the US submarine force today is much more capable than it was previously against hardened targets such as Russian ICBM silos. A decade ago, only about 20 percent of US submarine warheads had hard-target kill capability; today they all do. (See Figure 1.)

This vast increase in US nuclear targeting capability, which has largely been concealed from the general public, has serious implications for strategic stability and perceptions of US nuclear strategy and intentions.

Russian planners will almost surely see the advance in fuzing capability as empowering an increasingly feasible US preemptive nuclear strike capability—a capability that would require Russia to undertake countermeasures that would further increase the already dangerously high readiness of Russian nuclear forces. Tense nuclear postures based on worst-case planning assumptions already pose the possibility of a nuclear response to false warning of attack. The new kill capability created by super-fuzing increases the tension and the risk that US or Russian nuclear forces will be used in response to early warning of an attack—even when an attack has not occurred.

The increased capability of the US submarine force will likely be seen as even more threatening because Russia does not have a functioning space-based infrared early warning system but relies primarily on ground-based early warning radars to detect a US missile attack. Since these radars cannot see over the horizon, Russia has less than half as much early-warning time as the United States. (The United States has about 30 minutes, Russia 15 minutes or less.)

The inability of Russia to globally monitor missile launches from space means that Russian military and political leaders would have no "situational awareness" to help them assess whether an early-warning radar indication of a surprise attack is real or the result of a technical error.

The combination of this lack of Russian situational awareness, dangerously short warning times, high-readiness alert postures, and the increasing US strike capacity has created a deeply destabilizing and dangerous strategic nuclear situation.

When viewed in the alarming context of deteriorating political relations between Russia and the West, and the threats and counter-threats that are now becoming the norm for both sides in this evolving standoff, it may well be that the danger of an accident leading to nuclear war is as high now as it was in periods of peak crisis during the Cold War.

How the new accuracy-enhancing fuze works

The significant increase in the ability of the W76-1/Mk4A warhead to destroy hardened targets—including Russian silo-based ICBMs—derives from a simple physical fact: Explosions that occur near and above the ground over a target can be lethal to it. This above-target area is known as a "lethal volume"; the detonation of a warhead of appropriate yield in this volume will result in the destruction of the target.

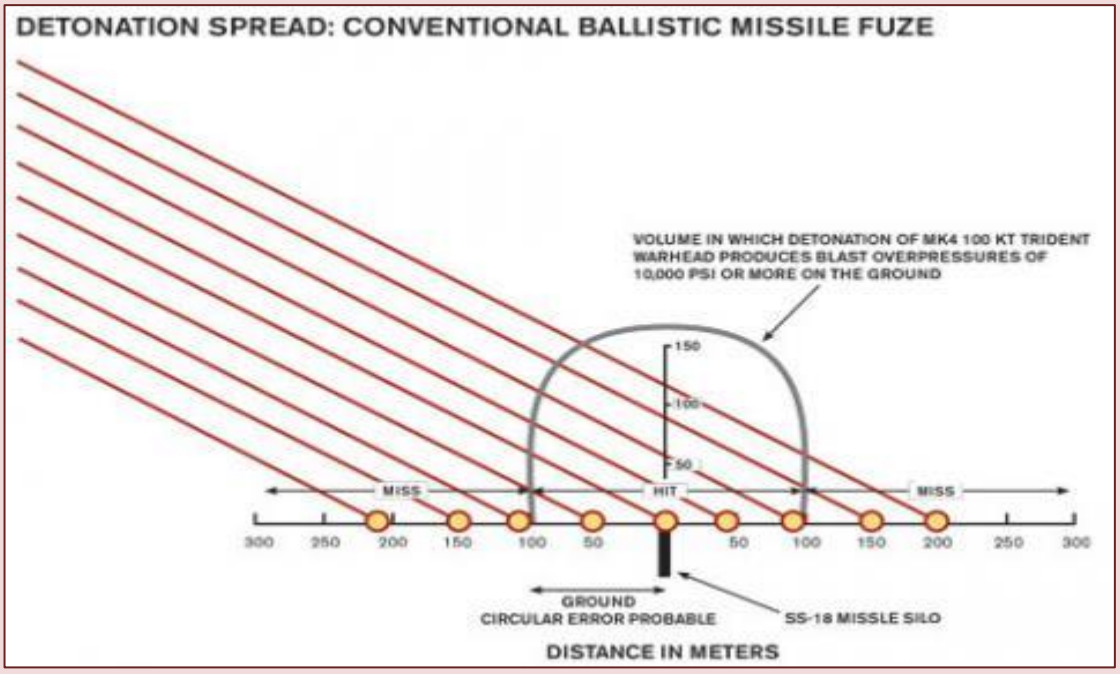
The recognition that the killing power of the W76 warhead could be vastly increased by equipping it with a new fuze was discussed in a 1994 alternate warhead study conducted by the Defense and Energy departments. The study calculated the number of warheads that would be needed for the W76 to attack the Russian target base, if START II were implemented. At the time, W76/Mk4 warheads had a fixed height-of-burst fuze (meaning the fuze could not adjust its detonation at an optimal location if it were falling short or long of a target). With those fixed-height fuzes, submarine-launched nuclear missiles were mainly aimed at softer targets such as military bases.

But the study found that an enhanced Mk4A reentry-body with a new fuze that provided for an adjustable height-of-burst as it arrives would have significant capabilities against harder targets, compared to warheads with the earlier fuzes. The study assumed that a smaller number of Mk4 nuclear warheads with higher killing power per warhead could cover the Russian target base and be more effective than multiple attacks on targets with less destructive warheads. In other words, an enhanced fuze would allow the United States to reduce the number of warheads on its ballistic missile submarines, but increase the targeting effectiveness of the fleet.

Figure 2 illustrates the kill distribution of US submarine-launched nuclear missiles equipped with the earlier, fixed height-of-burst fuzes. The dome-shaped volume outlined in gray shows the lethal volume within which a 100-kiloton nuclear explosion will generate 10,000 pounds per

square inch or more of blast pressure on the ground. In other words, if a target on the ground cannot survive a blast of 10,000 pounds per square inch or more, it will be destroyed if a 100-kt nuclear weapon detonates anywhere within that dome-shaped volume.

FIGURE 2. Missiles with fixed height-of-burst fuzes can overshoot or undershoot the "lethal volume" (shown here by a gray, dome-shaped line), limiting their ability to destroy hardened targets.



To show the physical relationship of the lethal volume for a particular ground target of interest—in this case a Russian SS-18 ICBM silo—Figure 2 was drawn to scale. Also shown to scale is the approximate spread of warhead trajectories that correspond to a missile that is accurate to 100 meters, a miss distance roughly the same as what is achieved by the Trident II sea-launched ballistic missile.

Miss distances are typically characterized in terms of a quantity called the "circular error probable," or CEP, which is defined as the radius of a circle around the aim point within which half of the warheads aimed at a target are expected to impact. In the case of a Trident II 100-kt W76-1 ballistic missile warhead, the lethal distance on the ground and the CEP are roughly equal. As a result, roughly half of the warheads equipped with the old, fixed-height fuze system could be expected to fall close enough to detonate on the ground within the lethal range.

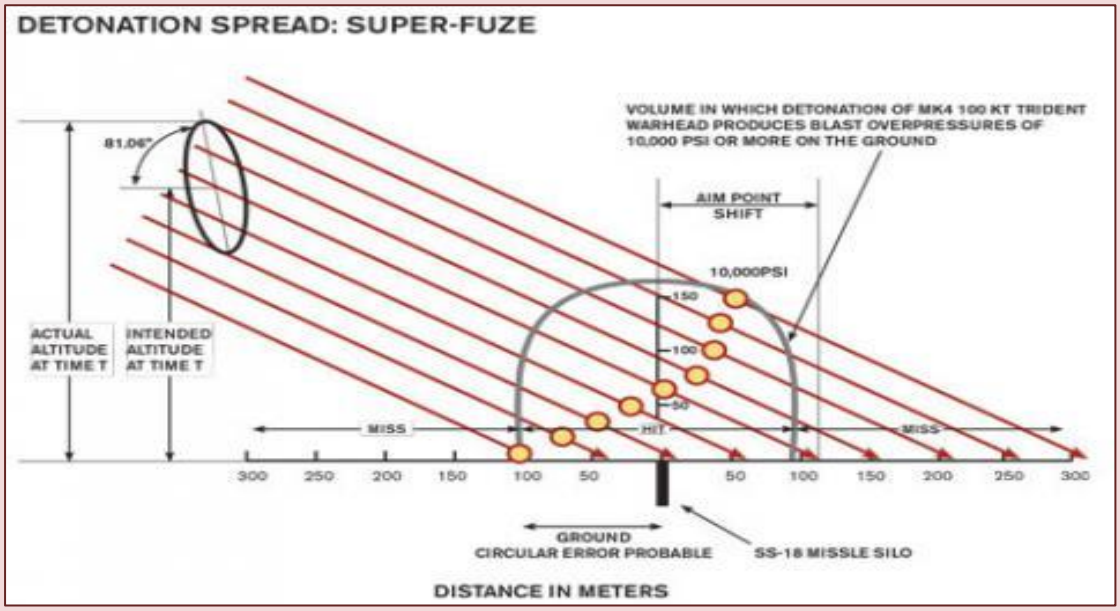
The new super-fuze for W76-1/Mk4A has a flexible height-of-burst capability that enables it to detonate at any height within the lethal volume over a target. Figure 3 shows how the new fuze vastly increases the chances that the target will be destroyed, even though the arriving warheads have essentially the same ballistic accuracy.

The super-fuze is designed to measure its altitude well before it arrives near the target and while it is still outside the atmosphere. This measurement would typically be taken at an altitude of 60 to 80 kilometers, where the effects of atmospheric drag are very small. At this point, the intended trajectory is known to very high precision before the warhead begins to substantially slow from atmospheric drag. If the warhead altitude measured by the super-fuze at that time were exactly equal to the altitude expected for the intended trajectory, the warhead would be exactly on target. But if the altitude were higher than expected, the warhead could be expected to hit beyond the intended aim point. Likewise, if the altitude is lower than that expected, the warhead would likely hit short of the intended aim point.

Testing has established the statistical shape and orientation of the expected spread of warhead locations as they fly towards the target. In the case of Trident II, the spread of trajectories around the intended trajectory is so small that the best way to increase the chances of detonating inside the lethal volume is to intentionally shift the aim point slightly beyond the location of the target. (Note that the intended trajectory in Figure 3 is shifted slightly down range.)

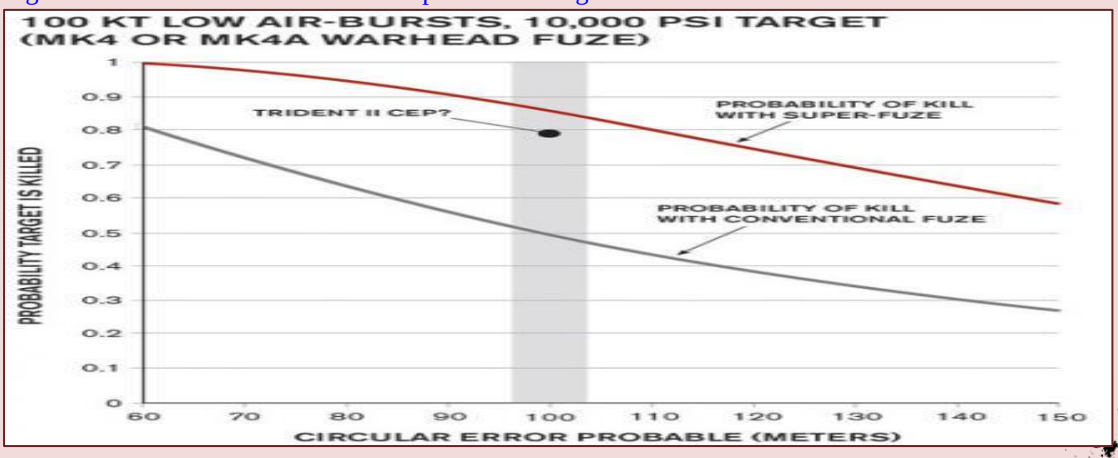
By shifting the aim point down range by a distance roughly equal to a CEP, warheads that would otherwise fall short or long of the target using the conventional Mk4 fuze instead will detonate—at different heights dictated by the super fuze—within the lethal volume above a target. This shift in the down-range aim point will result in a very high percentage of warheads that overfly the target detonating in the lethal volume. The end result is that with the new Mk4A super-fuze, a substantially higher percentage of launched warheads detonate inside the lethal volume, resulting in a considerable increase in the likelihood that the target is destroyed.

FIGURE 3. The tilted ellipse in the left upper corner of Figure 3 depicts the spatial distribution of incoming warheads at the time the super-fuze measures its altitude. In this particular case, the orientation of the ellipsoid indicates that the errors leading to a miss at the target are mostly due to a mix of small discrepancies in the velocity and direction of the warheads when they are deployed from the rocket upper stage outside the atmosphere. The orientation and dimensions of this ellipse are well known to a ballistic missile designer, so the altitude measurement can provide information that leads to an estimate of the distance from the lethal volume above the target.



The ultimate effect of the super fuze's flexible burst-height capability is a significantly increased target kill probability of the new W76-1/Mk4A warhead compared with the conventional warhead of the same type. Figure 4 shows the probability that warheads will detonate close enough to destroy the ground-target for both the conventional fuze and the super-fuze.

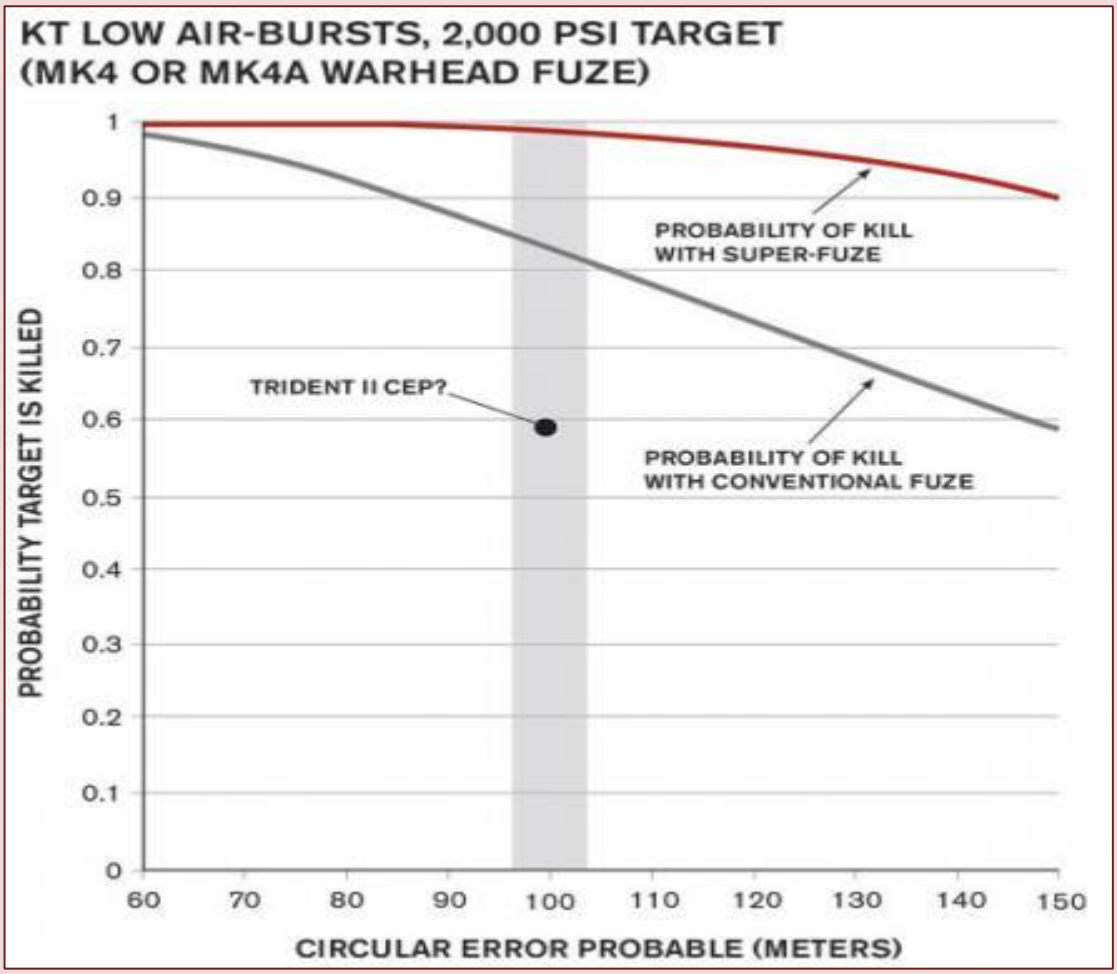
FIGURE 4. The probability of destroying a fully hardened Russian target with the super-fuzed W76-1/Mk4A warhead atop an American submarine-launched ballistic missile is about 86 percent—far higher than would be the case with the previous fuzing for the warhead.



As can be seen from figure 4, the probability of kill using a submarine-launched warhead with the new super-fuze (W76-1/Mk4A) is about 0.86. This 86 percent probability is very close to what could be achieved using three warheads with conventional fuzes to attack the same target. To put it differently: In the case of the 100-kt Trident II warhead, the super fuze triples the killing power of the nuclear force it has been applied to.

Many Russian targets are not hardened to 10,000 pounds per square inch blast overpressure. Figure 5 shows the same probability of kill curves for the case of a target that is only hard to 2,000 pounds per square inch or more of blast overpressure, which is the actual case for almost all targets hardened to nuclear attack—ICBMs and supporting command posts, hardened structures at strategic airbases, submarines at pierside or in protected tunnels, hardened command posts at road mobile missile bases and elsewhere, etc. In this case, the super-fuze achieves a probability of kill of about 0.99—or very near certainty. This case also is equivalent to achieving a probability of kill associated with using three warheads with a 0.83 probability to achieve a 0.99 probability of kill.

FIGURE 5. The likelihood that a submarine-launched ballistic missile will destroy all but the most hardened targets approaches 100 percent.



The probability of kills revealed by figures 4 and 5 have enormous security ramifications.

The US military assumes that Russian SS-18 and TOPOL missile silos are hardened to withstand a pressure of 10,000 pounds per square inch or more. Since with the new super-fuze, the probability of kill against these silos is near 0.9, the entire force of 100-kt W76-1/Mk4A Trident II warheads now "qualifies" for use against the hardest of Russian silos. This, in turn, means that essentially all of the higher-yield nuclear weapons (such as the W88/Mk5) that were formerly assigned to these Russian hard targets can now be focused on other, more demanding missions, including attacks against deeply-buried underground command facilities. In effect, the significant increase in the killing power of the W76 warhead allows the United States to use its submarine-based weapons

more decisively in a wider range of missions than was the case before the introduction of this fuze.

The history of the US super-fuze program

The super-fuze is officially known as the arming, fuzing and firing (AF&F) system. It consists of a fuze, an arming subsystem (which includes the radar), a firing subsystem, and a thermal battery that powers the system. The AF&F is located in the tip of the cone-shaped reentry body above the nuclear explosive package itself. The AF&F developed for the new W76-1/Mk4A is known as MC4700 and forms part of the W76 life-extension program intended to extend the service life of the W76—the most numerous warhead in the US stockpile—out to the time period 2040-2050.

The new super-fuze uses a technology first deployed on the high-yield W88/Mk5 Trident II warhead. The Navy's Strategic Systems Program contracted with the Lockheed Missile and Space Corporation in the early 1980s to develop a new fuze that included "a radar-updated, path-length compensating fuze … that could adjust for trajectory errors and significantly improve the ability to destroy a target. This was an early and sophisticated use of artificial intelligence in a weapon."

It was the radar-updated, path-length compensating fuze—combined with the increased accuracy of the Trident II missile—that gave an SLBM the ability to hold a hardened target at risk.

Efforts to incorporate the W88/Mk5 fuze capability into the W76/Mk4 was part of the Energy Department's Warhead Protection Program in the mid-1990s to permit "Mk5 fuzing functionality (including *radar-updated path length fuzing*, and radar proximity fuzing) as an option to replacement of the much smaller Mk4 AF&F," according to the partially declassified 1996 Stockpile Stewardship and Management Plan (emphasis added).

Apart from the inherent drive to improve military capabilities whenever possible, the motivation for increasing the target kill capability of the submarine-borne W76 was that the Air Force's hard-target killer, the MX Peacekeeper ICBM, was scheduled to be retired under the START II treaty. The Navy only had 400 W88 hard-target kill warheads, so a decision was made to add the capability to the W76.

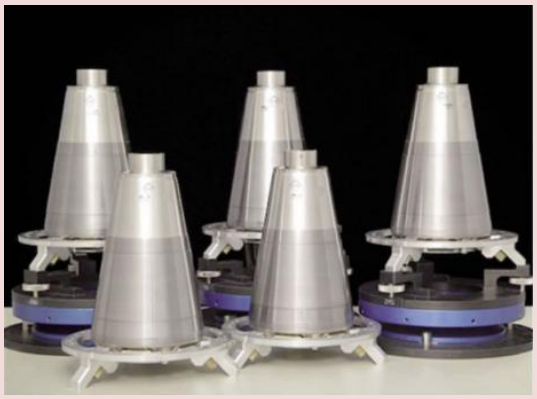


FIGURE 6. The first of the new MC4700 AF&F super-fuzes for the W76-1 were completed at the Kansas City Plant in 2007. Delivery of the W76-1/Mk4A warhead to the Navy began in 2009.

In an article in April 1997, Strategic Systems Program director Rear Adm. George P. Nanos publicly explained that "just by changing the fuze in the Mk4 reentry body, you get a significant improvement. The Mk4, with a modified fuze and Trident II accuracy, can meet the original D5 [submarine-borne missile] hard target requirement," Nanos stated.

Later that same year, the Energy Department's Stockpile Stewardship and Management Plan formally described the objective of the fuze modernization program "to enable W76 to take advantage of [the] higher accuracy of [the] D5 missile."

By 1998, the fuze modernization effort became a formal project, with five SLBM flight tests planned for 2001-2008. Full-scale production of the super-fuze equipped W76-1/Mk4A began in September 2008, with the first warhead delivered to the Navy in February 2009. By the end of 2016, roughly 1,200 of an estimated 1,600 planned W76-1/Mk4As had been produced, of which about 506 are currently deployed on ballistic missile submarines.

The implications

The newly created capability to destroy Russian silo-based nuclear forces with 100-kt W76-1/Mk4A warheads—the most numerous in the US stockpile—vastly expands the nuclear warfighting capabilities of US nuclear forces. Since only part of the W76 force would be needed to eliminate Russia's silo-based ICBMs, the United States will be left with an enormous number of higher-yield warheads that would then be available to be reprogrammed for other missions.

Approximately 890 warheads are deployed on US ballistic missile submarines (506 W76-1/Mk4A and 384 W88/Mk5). Assuming that the 506 deployed W76-1s equipped with the super-

fuze were used against Russian silo-based ICBMs, essentially all 136 Russian silo-based ICBMs could be potentially eliminated by attacking each silo with two W76-1 warheads—a total of 272 warheads. This would consume only 54 percent of the deployed W76-1 warheads, leaving roughly 234 of the 500 warheads free to be targeted on yet other installations. And hundreds of additional submarine warheads are in storage for increasing the missile warhead loading if so ordered. The Trident II missiles that are deployed today carry an average of four to five W76-1 warheads each. However, each missile could carry eight such warheads if the US were to suddenly decide to carry a maximum load of W76 warheads on its deployed Trident II ballistic missiles. And the missile was tested with up to 12 warheads.

Essentially all the 384 W88 "heavy" Trident II warheads, with yields of 455 kt, would also be available for use against deeply-buried targets. In addition, about 400 Minuteman III warheads, with yields of about 300 kt, could be used to target hardened Russian targets. In all, the entire Russian silo-based forces could potentially be destroyed while leaving the US with 79 percent of its ballistic missile warheads unused.

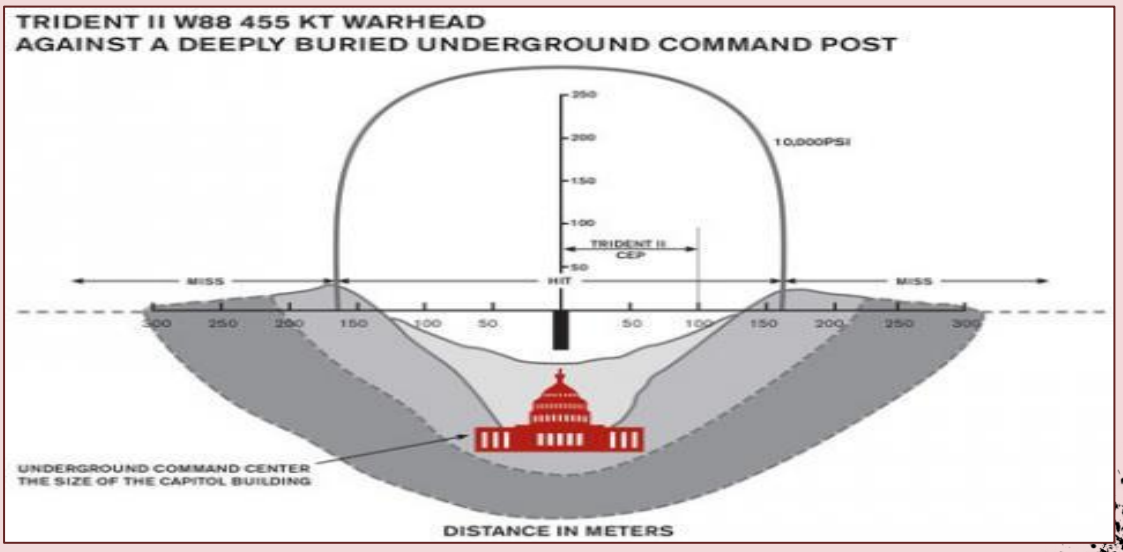
Even after Russia's silo-based missiles were attacked, the US nuclear firepower remaining would be staggering—and certainly of concern to Russia or any other country worried about a US first strike.

Because of the new kill capabilities of US submarine-launched ballistic missiles (SLBMs), the United States would be able to target huge portions of its nuclear force against non-hardened targets, the destruction of which would be crucial to a "successful" first strike. One such mission would likely involve the destruction of road-mobile ICBMs that had left their garrisons to hide in Russia's vast forests in anticipation of attack. The garrisons and their support facilities would probably be destroyed quickly, and some of the dispersed road-mobile launchers would also be quickly destroyed as they were in the process of dispersing. To destroy or expose the remaining launchers, United States planners would have the nuclear forces needed to undertake truly scorched-earth tactics: Just 125 US Minuteman III warheads could set fire to some 8,000 square miles of forest area where the road-mobile missiles are most likely to be deployed. This would be the equivalent of a circular area with a diameter of 100 miles.

Such an attack would be potentially aimed at destroying all road-mobile launchers either as they disperse or after they have taken up position some short distance from roads that give them access to forested areas.

Many of the nearly 300 remaining deployed W76 warheads could be used to attack all command posts associated with Russian ICBMs. A very small number of Russia's major leadership command posts are deeply buried, to protect them from direct destruction by nuclear attack. The US military would likely reserve the highest-yield warheads for those targets. Figure 7 below shows an example of a structure that is roughly the size of the US Capitol building that is postulated to have rooms and tunnels as deep as 800 feet or more. Shelters that have rooms and tunnels at even greater depths could be sealed by using multiple nuclear warheads to crater every location where an entrance or exit might conceivably have been built.

FIGURE 7.



The situation with regard to the retaliatory potential of Russia's ballistic missile submarines is problematic from the point of view of a conservative Russian planner. Although Russia currently has 11 ballistic missile submarines, currently two or three of these missile-carrying submarines are in overhaul and do not carry nuclear warheads. If the full force of available operating submarines not in overhaul could be deployed to sea, Russia could deliver roughly 592 of the full 768 warheads theoretically deployed in its submarine force. At some as yet unforeseen time in the future, Russia might be able to deploy 600 to 700 submarine-based warheads to sea, but a realistic number given the limited availability of crews and equipment might instead be 400 to 500 warheads.

By 2030 to 2040, the United States could easily have built enough Aegis ships to carry 500 to 700 of the newly introduced SM-3 Block IIA interceptor. These new interceptors have a 50 percent higher burnout speed than the older SM-3 Block IA interceptors, giving the Block IIA a greater engagement range and theoretically making it possible to provide missile defense for the continental United States via Aegis ships stationed off the country's Atlantic and Pacific coasts.

For all practical purposes, the intercept capability of the SM-3 Block IIA is negligible. Both the infrared homing sensors on these interceptors and the US early warning tracking radars that cue the interceptors to their targets have no practical ability to distinguish between warheads, pieces of rocket upper stages, and decoys. But the appearance created by the vast expansion of this missile defense program can and will contribute to perceptions among Russians that the United States is seeking nuclear dominance.

The Russians have most recently reacted to this ongoing program by publicly displaying and implementing a new and novel sea-based nuclear weapons delivery device as a hedge against US missile defenses.

In particular, Russia is now in the process of testing a 40-ton nuclear-powered underwater unmanned vehicle (UUV) that could robotically deliver, across thousands of kilometers, a 100-megaton nuclear warhead against the coastal cities and ports of the United States. The technical details of this bizarre system were released by Putin himself in September 2015—apparently intentionally—and testing began in December 2016. Such actions by the Russian government clearly indicate a grave concern about the unpredictable character of ongoing US missile defense programs.

In addition to upgrading the hard-target kill capability of the W76 warhead, the US military also appears to be working to increase the targeting capability of the warheads on the land-based Minuteman III ICBM force. The Minuteman III is much less accurate than Trident II, with a CEP of about 160 meters, compared to the roughly 100-meter CEP now achieved by Trident II. These differences mean that the probability of kill could be two to two-and-a-half times higher for the same weapon carried by a Trident II with a 100-meter CEP versus a Minuteman III with a 160-meter CEP. Without a major guidance upgrade, Minuteman III could not be expected to achieve nearly the nuclear warfighting capacity of the Trident II.

The Air Force is working on an upgrade to the AF&F used on the Mk21 reentry vehicle containing the W87 warhead. The W87/Mk21 warhead arms about half of the ICBM force, with the other half carrying the W78/Mk12A.

Our analysis shows that fitting Minuteman III warheads with super-fuzes will give the Minuteman III essentially the same hard target kill capability as the MX had with its cutting-edge Advanced Inertial Reference Sphere (AIRS) guidance system; the MX was retired in 2005. The first production unit Mk21 fuze is planned for early 2020s with production expected to continue through 2029. The Air Force is planning to use the W87/Mk21 on a new ICBM planned for deployment in 2030.

Shortfalls in Russia's early warning system

In January 1995, a lone sounding rocket was launched from an isolated Island off the Northwest Coast of Norway. Even though the rocket was heading toward the North Pole, not at Russia, we now know that as it rose over the horizon of the curved Earth, it was tracked by the Russian early warning radar on the Kola Peninsula at Olenegorsk. Because it was on a near-vertical trajectory, the automated tracking algorithms utilized by the radar interpreted the characteristics of the trajectory as matching a Trident submarine-launched ballistic missile on a mission to detonate a nuclear weapon in front of the radar's field of view, making the radar incapable of detecting nuclear warheads coming from longer range.

That the Russian early warning system reacted to this innocuous launch unambiguously indicates that the Russian warning system has at least some measures within it to alert Russian forces to events that could indicate an evolving US nuclear preemptive attack.

If the United States were to execute such an attack against Russia, Russia would certainly know that the most dangerous and most quickly arriving nuclear warheads would come from US submarine-launched ballistic missiles on station in the North Atlantic. Given the extremely high lethality of essentially all US submarine-based warheads, a well-coordinated US attack would not need to employ US land-based Minuteman ICBMs if its initial aim was to simply destroy Russia's silo-based ICBMs before they could be launched.

Such a "warfighting attack" would likely begin with the detonation of a nuclear warhead in front of key early-warning radars. An explosion of a 455 kiloton Trident II warhead at an altitude of 1,300 to 1,400 kilometers would create an area of radar "blackout" that would prevent all Russian radars looking toward the United States and into the northern parts of the North Atlantic from observing US ballistic missiles as they rose over the radar horizon.

US missile launches from the North Atlantic would be coordinated to rise over the radar horizon only after the Russian radars had been blinded. Even if the radars were not rendered ineffective, the Russians could reasonably expect to have no more than seven to 10 minutes of warning before Moscow was destroyed. (See the table showing decision-making timelines below.)

The false alert of 1995 would not have occurred if Russia had a reliable and working global space-based satellite early warning system. Russian analysts would have been able to observe that there were no US ballistic missile launches from the North Atlantic. The availability of such a system would have caused the initial alert to be called off within minutes or even more quickly.

Detailed analyses, initially stimulated by questions about why the alert went on for so long, showed that a specialized space-based Russian early warning system called Prognoz was then under development. Analysis of the Prognoz satellite constellation and of available Russian infrared sensor technologies indicated that even if the satellite system had been working, it would not have been able to provide surveillance of the North Atlantic. Today, Russia has stopped launching satellites into this constellation and has instead focused enormous resources exclusively into building a highly robust and redundant network of ground-based radars. It is now very clear that Russia's extreme de-emphasis on satellite early warning systems and its extreme focus on building numerous, technologically varied ground-based radar warning systems is due to the lack of critical technologies needed to implement a space-based ballistic missile warning system.

Operations Associated With Assessing the Circumstances Associated with a Possible Nuclear Attack	Time Needed for Operation
Time for attacking missiles to rise over the horizon into the line-of-sight of early warning radars	1 minute
Time for radars to detect, track, and characterize detected targets, and to estimate the size and direction of motion of targets	1 minute
Military and civil command conference to determine response	1 to 3 minutes
Time for command and unit elements of silo-based forces to encode, transmit, receive, decode, and authenticate a launch order	2 to 4 minute
Time for missile crews to go through full launch procedures	1 to 3 minutes
Time for launched missile to reach a safe distance from its launch-silo	1 minute
Total time consumed in unavoidable and essential operations	7 to 13 minutes

Facing the existential threat of a short-warning attack with accurate and powerful sea-launched, nuclear-armed ballistic missiles and no ability to quickly detect their launch with space-based early warning systems, Russian leadership would seem to have little choice but to pre-delegate nuclear launch authority to lower levels of command. Many possible ways of pre-delegating authority are possible, but none of them are free of dangers that could increase the chances of

accidents that could ultimately result in the mistaken launch of Russian nuclear forces. Forcing this situation upon the Russian government seems likely to be detrimental to the security interests of the United States and its Western allies.

Our conclusions

Under the veil of an otherwise-legitimate warhead life-extension program, the US military has quietly engaged in a vast expansion of the killing power of the most numerous warhead in the US nuclear arsenal: the W76, deployed on the Navy's ballistic missile submarines. This improvement in kill power means that all US sea-based warheads now have the capability to destroy hardened targets such as Russian missile silos, a capability previously reserved for only the highest-yield warheads in the US arsenal.

The capability upgrade has happened outside the attention of most government officials, who have been preoccupied with reducing nuclear warhead numbers. The result is a nuclear arsenal that is being transformed into a force that has the unambiguous characteristics of being optimized for surprise attacks against Russia and for fighting and winning nuclear wars. While the lethality and firepower of the US force has been greatly increased, the numbers of weapons in both US and Russian forces have decreased, resulting in a dramatic increase in the vulnerability of Russian nuclear forces to a US first strike. We estimate that the results of arms reductions with the increase in US nuclear capacity means that the US military can now destroy all of Russia's ICBM silos using only about 20 percent of the warheads deployed on US land- and sea-based ballistic missiles.

Eventually, super-fuze upgrades will make it possible for every SLBM and ICBM warhead in the US arsenal to perform the hard-target kill missions that were initially envisioned to be exclusively reserved to MX Peacekeeper ICBM warheads.

The W76 upgrade reflects a 25-year shift of the focus of US hard-target kill capability from land-based to sea-based ballistic missiles. Moreover, by shifting the capability to submarines that can move to missile launch positions much closer to their targets than land-based missiles, the US military has achieved a significantly greater capacity to conduct a surprise first strike against Russian ICBM silos.

The decision by the Obama administration in 2009 to deploy the Aegis ship-based European Phased Adaptive Approach (EPAA) missile defense system has created a program under which the United States could eventually have between 500 to 700 anti-missile interceptors that could in theory be used to defend the continental United States from ships off the country's coasts. In spite of its severe limitations, this growing defense system could appear to both Russia and China as a US attempt to reduce the consequences of a ragged Russian or Chinese retaliation to a US first strike against them.

We cannot foresee a situation in which a competent and properly informed US president would order a surprise first strike against Russia or China. But our conclusion makes the increased sea-based offensive and defensive capabilities we have described seem all the more bizarre as a strategy for reducing the chances of nuclear war with either Russia or China.

That Russian silos are more vulnerable to W76-1/Mk4A warheads will not come as an earth-shattering revelation to Russian military officials; they would have to expect that the silos would be destroyed anyway, by US land-based ICBMs. But the growing capability of the US forward-deployed sea-based nuclear missiles could raise serious questions in the minds of Russian military planners and political leadership about US intentions—especially when seen in context of growing US cyber, advanced conventional, and missile defense capabilities—almost certainly deepening mistrust and encouraging worst-case planning assumptions in Moscow.

We end this article with quotes from Vladimir Putin, talking impromptu to a group of journalists during the St. Petersburg International Economic Forum in June 2016. His unrehearsed remarks are clear and candid predictors of how he will assess the implications of the super-fuze:

No matter what we said to our American partners [to curb the production of weaponry], they refused to cooperate with us, they rejected our offers, and continue to do their own thing.

... They rejected everything we had to offer.

... the Iranian threat does not exist, but missile defense systems are continuing to be positioned...

That means we were right when we said that they are lying to us.

Their reasons were not genuine, in reference to the "Iranian nuclear threat."
Your people [the populations of the Western alliance] … do not feel a sense of the impending danger—this is what worries me.
A missile defense system is one element of the whole system of offensive military potential.
It works as part of a whole that includes offensive missile launchers.
One complex blocks, the other launches high precision weapons, the third blocks a potential nuclear strike, and the fourth sends out its own nuclear weapon in response.
This is all designed to be part of one system.
I don't know how this is all going to end.
What I do know is that we will need to defend ourselves.

Hans M. Kristensen *is the director of the Nuclear Information Project at the Federation of American Scientists and the co-author of the Nuclear Notebook in the* Bulletin of the Atomic Scientists.
Matthew G. McKinzie *is the director of the Nuclear Program of the Natural Resources Defense Council (NRDC) in Washington, DC. He holds a PhD in experimental nuclear physics from the University of Pennsylvania and has conducted research at Los Alamos National Laboratory.*
Theodore A. Postol *is a physicist and professor of science, technology, and national security policy at MIT. His expertise is in ballistic missile defense technologies and ballistic missiles more generally. He is a former analyst at the Office of Technology Assessment and science and policy adviser to the chief of naval operations.*

What's a Health Department to Do? Staying Relevant in the Field of Radiological Response

By Mark L. Maiello
Source: http://www.cbrneportal.com/whats-a-health-department-to-do-how-to-stay-relevant-in-the-field-of-radiological-response/

Mar 06 – These days, first response organizations like fire and police departments can be well-equipped with radiological detection equipment. In addition, the relevant personnel in these departments have received operational training in the measurement of radiation and the basic analysis of radioactivity readings. The level of expertise in the detection of radiation – if not the interpretation of the readings – is now no longer exclusively the purview of specialists working in local health departments. This measurement capability once was exclusive to health physicists. Now the expertise resides in many agencies with an interest or a mandate to respond to a radiological incident. If this knowledge has expanded to agencies other than health departments, can the latter still significantly support radiological incident response?
There are in fact several ways that a local health department can support a jurisdiction-wide radiological response. For example, to serve interagency collaboration, a health department can coordinate such emergency planning at a grass root level without interfering with the overarching functions of an emergency management agency. In New York City for example, a Radiological Response and Recovery Committee (RRRC) serves as an interagency planning platform while pursuing refinements to the citywide radiological response plan. Currently, a NYC Department of Health representative co-chairs the RRRC, sets meeting agendas, and determines post-meeting follow-up actions of the RRRC.

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

Mark L. Maiello, PhD *is a radiological emergency planner with NYC Department of Health and Mental Hygiene. He served in the radiation safety office for Wyeth pharmaceuticals and its successor Pfizer for 17 years. Mark was educated at Manhattan College and New York University. He is co-editor of Radioactive Air Sampling Methods, published in 2011 by CRC Press, Inc.*

Responding to radiation

By Andy Oppenheimer
Source: http://www.cbrneportal.com/responding-to-radiation/

Feb 21 – The immediate and long-term impact of a radiation dispersal event (RDE) on the health and wellbeing of a population, as well as the country's food chain, drinking water, property and national critical infrastructure mark out such an event from other emergencies requiring medical response.

As well as acute physical injury an RDE from a bomb or nuclear facility explosion would also contaminate affected persons externally and internally – due to the spread of radioactive emission through the surrounding area and potentially, beyond – depending on weather conditions, wind direction and level and locations of particle deposition. The use of even an improvised radiological weapon could affect an entire country or region for a long time, economically, medically, and psychologically.

An RDE caused by an exploding device, facility leak or meltdown, or other release is therefore a complex event for rescue/healthcare systems – and radiation protection authorities, police and the joint command chain – to deal with.

Differing effects

The harm caused depends on the type of radioisotope used and the type of ionizing radiation emitted. To assess this, the isotope would have to be identified very quickly. Gamma emitters (e.g. cesium-137*) penetrate body tissue and may be lethal; beta emitters (e.g. strontium-90**) can penetrate and burn the skin; and alpha emitters (e.g. plutonium-239***; polonium-210****) have to be ingested or inhaled, and once they are, may be lethal.

*used in medicine and industry
**emitted in the Windscale fire
***weapons-grade material for nuclear weapons
****used to kill Alexander Litvinenko

Effects depend on the absorbed dose and range. At the high end, Acute Radiation Syndrome (ARS) is caused by a high dose (4-6 Gy), with victims showing severe symptoms within hours. As well as vomiting and diarrhoea, which could be mistaken for severe food poisoning, the clinchers are hair loss, skin redness, burns and moist peeling, haemorrhaging, then necrosis (cell death) and multiple organ failure. Many more people could be exposed to a mild to moderate dose (1-4 Gy) within days or weeks, with no symptoms but a heightened risk of cancer, which as one of the world's most common illnesses is hard to attribute.

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

***Andy Oppenheimer AIExpE MIABTI** is Editor of CBNW (Chemical, Biological & Nuclear Warfare) journal and a consultant in CBRNE and counter-terrorism. He is author of IRA: The Bombs and the Bullets (Irish Academic Press, 2008) and of the CBRN and IEDs module courses for the St Andrews University Certificate in Terrorism Studies.*

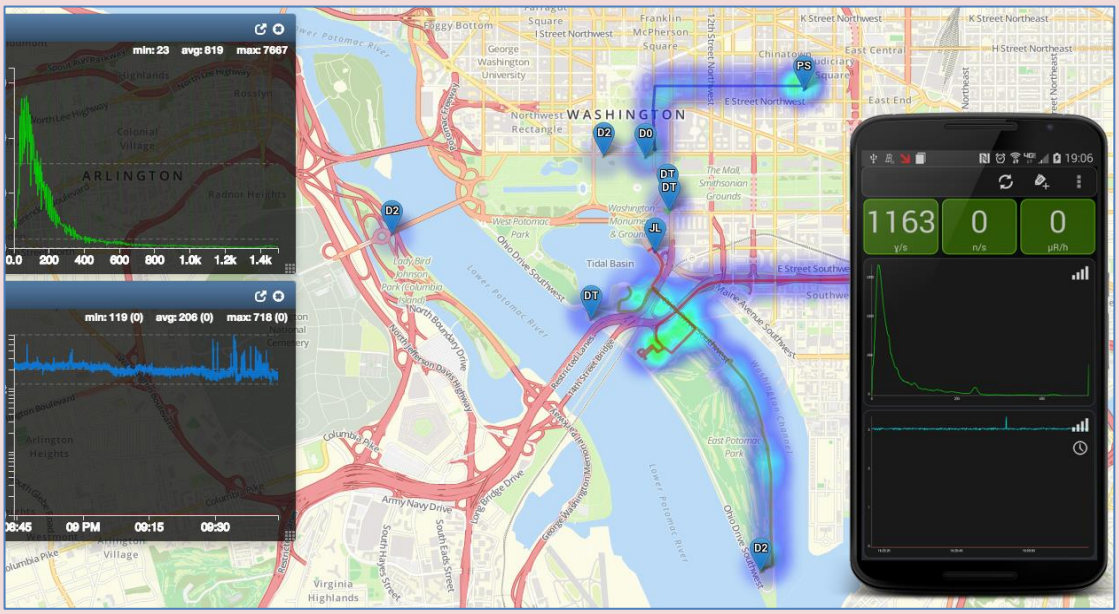
Radiation threat detection system successfully tested in Washington, D.C.

Source: http://www.homelandsecuritynewswire.com/dr20170307-radiation-threat-detection-system-successfully-tested-in-washington-d-c

Mar 07 – DARPA's SIGMA program — whose goal is to prevent attacks involving radiological "dirty bombs" and other nuclear threats — concluded its biggest and longest test deployment of vehicle-mounted radiation detectors in Washington, D.C., in February.

DARPA says that for approximately seven months starting in July 2016, the fleet of D.C. Fire and Emergency Medical Services ambulances was outfitted with DARPA-developed nuclear and radiological

detectors, providing the first city-scale, dynamic, real-time map of background radiation levels throughout the Capital as well as identifying any unusual spikes that could indicate a threat.



Because medical and fire emergencies occur in every corner of the District every day, emergency vehicles equipped with radiation detectors provide an excellent means of achieving a large-scale scan for radiological risks. In the just-completed test deployment, up to 73 large detectors were installed on emergency vehicles that together logged well over 100,000 hours of detector operation covering more than 150,000 miles, and identified in real-time thousands of radiation

sources. Items as innocuous as natural granite used in construction, as well as lingering radiation after certain medical treatments, can trigger positive responses. SIGMA detectors can readily distinguish between these kinds of benign sources and threatening ones. Equally important, the SIGMA detectors provided detailed background radiation maps of the District against which future sources may be more easily detected. The deployment also offered an opportunity to test and refine the wireless data fusion aspects of the system, which constantly fed information about vehicle location and radiation readings to a central command post.

"D.C. Fire and EMS was an invaluable partner and testbed for SIGMA's vehicle-scale detectors," said Vincent Tang, DARPA program manager. "The data gathered during the D.C. deployment are helping to further fine-tune the SIGMA system for potential deployment in major cities across the country and for emergency use by active-duty military units and National Guard civil support teams." While ambulances were used in the D.C. test, the program envisions the possibility of using other options for getting distributed coverage in future deployments in other cities.

"Historically, increases to detection capabilities came from improved individual detectors," said John Donnelly, D.C. Fire and EMS deputy fire chief. "The most significant capability gain since 9/11 was

spectroscopic detectors for first responders. D.C. Fire and EMS was interested in the SIGMA program because DARPA approached the problem differently. By not only putting more spectrometers into the field but also networking them so that the data is continuously collected and analyzed with other, and prior, information as a whole, SIGMA laid the groundwork for a monitoring system that can incorporate intelligence holistically into risk assessment. Incorporating more data will further improve the ability of the SIGMA system to differentiate between 'safe' and illicit radiation sources, and increase our capabilities to monitor wide-areas for radiological and nuclear threats."

DARPA notes that SIGMA system has developed two types of radiation detectors — a larger size like those recently deployed in the emergency vehicle tests and inexpensive, smartphone-sized mobile devices that can be worn on a belt by police officers or others. The devices run on advanced software that can detect the tiniest traces of radioactive materials. Those devices, networked with detectors along major roadways, bridges, and other fixed infrastructure, promise significantly enhanced awareness of radiation sources and greater advance warning of possible threats. The SIGMA detectors themselves do not emit radiation but detect gamma and neutron radiation emanating from sources.

In October 2016, DARPA oversaw a successful one-day test deployment of more than 1,000 smartphone-sized mobile SIGMA detectors, during which volunteers walked for several hours in the vicinity of the National Mall with the small detectors tucked inside backpacks. Other tests in the past year in the Washington, D.C., metropolitan area and other locations have also demonstrated the networked system's efficacy.

DARPA says it plans to further test SIGMA's wide-area monitoring capability and transition the operational system to local, state, and federal entities in 2017 and 2018.

Weapons of mass destruction: the Russian challenge

By Adrian Alvarado

Source: http://thebulletin.org/weapons-mass-destruction-russian-challenge10596

Mar 09 – More than 12 years have passed since the United Nations Security Council adopted Resolution 1540, which affirms that the proliferation of weapons of mass destruction is a threat to international peace and security, and recognizes the need to keep such weapons out of the hands of non-state actors—particularly extremist and terrorist groups. To deal with this common threat, UN member states pledged to adopt national legislation and establish domestic controls.

Resolution 1540 represents an enduring challenge for the Russian Federation, a country that possesses the know-how and the means to design, make, and deliver weapons of mass destruction. Russia is capable of creating nuclear, chemical, and biological weapons. To secure these capabilities, and to meet its commitments under Resolution 1540, Russia should create a special program to seek out radioactive material within Soviet-era facilities, and should work with other members of the Eurasian Economic Union to establish a common response to the threat of radicalized groups.

The real risks

Today, the most plausible risks related to weapons of mass destruction in the Russian Federation do not come from movie-like scenarios, such as an irresponsible government approach to nuclear deterrence (like that in the film "Dr. Strangelove"), or a rogue military faction using chemical weapons (as depicted in "The Rock"). Rather, the risks come from non-state actors seeking the easiest way to obtain a chemical, biological, or radiological weapon. For example, there is some evidence that the Islamic State has already obtained chemical weapons by seizing a stockpile from the Syrian government army, and has used these weapons repeatedly in the battle for the Iraqi city of Mosul.

This vulnerability to non-state actors is the reason why, during the next few years, the Russian government should develop an action plan to reassess post-Soviet civilian infrastructures. A considerable effort was already made during the first decade of this century to secure the most sensitive infrastructures (such as military facilities with nuclear warheads and materials, and nuclear power plants), but new security measures should be added to safeguard private laboratories, research centers, universities, and hospitals.

This task should be considered as a very important national interest for the Russian Federation, even if the risk is limited to a single attack with a small quantity of radiological, biological, or chemical material. Although human losses and injures can be modest during such a situation, post-attack health issues and contingency costs can be long-lasting and high.

In France, for example, the state of emergency declared after the November 2015 Paris terrorist attacks has been extended five times, most recently until July 2017. The French defense minister estimated in 2015 that the nation's security alert system, called Vigipirate, costs about one million euros each day. There is a human cost as well: The continuing emergency grants extra powers to the police, which increases the threat to human rights and privacy.

The Paris attackers used conventional bombs and guns. A terrorist attack with a radiological weapon (such as a radioactive "dirty bomb") would probably have a more severe psychological impact on the media, society, markets, and popular culture. In the immediate aftermath of such a disastrous attack, few people in social media or everyday life are likely to make careful distinctions between a low-yield radiological weapon and a high-yield nuclear explosion, or between the lethality of sarin gas and far more deadly Novichok-class nerve agents.

Stronger together

International cooperation is crucial if states want to enhance security levels and promote a security culture within organizations handling radioactive source materials (such as hospitals) or carrying out sensitive chemical and biological activities (such as private laboratories, universities, and research centers). Governments and their agencies have limited knowledge and

financial resources, so it is essential to seek common ground where states can agree on cooperation schemes for safety and capacity building.

For the Russian government, the most immediate field of action for international cooperation and assistance is the post-Soviet space. A not-so-politically-sensitive initiative could be the creation of a special program within the framework of the Commonwealth of Independent States – the former Soviet republics excluding Ukraine, Turkmenistan, and the Baltic states – to seek lost and orphaned sources of radioactive material within Soviet-era military, industrial, medical, and research infrastructures.

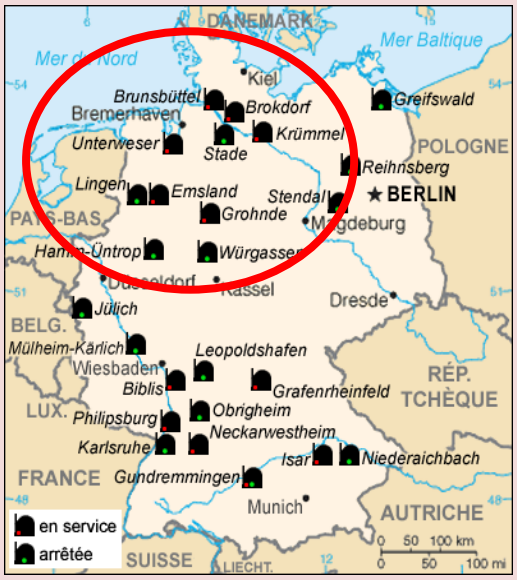
Furthermore, a regional approach to effectively implement the UN Resolution 1540 mandates should be a priority for the international assistance agenda of Russia and its neighbors. An initiative within the Eurasian Economic Union – which includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia – could be negotiated to agree on a common response to the threat of radicalized groups seeking to accomplish terrorist acts with weapons of mass destruction. Member states would reduce their vulnerabilities by establishing common security and export controls. A common and harmonized border control in the Eurasian Economic Union makes sense and would reinforce the political project of regional integration in this part of Eurasia.

Despite the recent crisis in relations between Russia, the United States, and the European Union, international cooperation to preclude the proliferation of weapons of mass destruction to non-state actors should continue to be a "sanctuarized" field in diplomatic channels – one that is sheltered from other disagreements in international politics. Terrorist or extremist groups with weapons of mass destruction represent not just a threat of destabilization for national governments and entire regions, but they may even endanger the very foundations of the current international order.

Adrian Alvarado *is a PhD candidate at Université de Lyon, writing on "Russia in the occidental Arctic: State strategies and interactions among players." He has a double master's degree in geopolitics from Ecole Normale Supérieure de Paris and Université de Paris 1 Panthéon-Sorbonne, and completed a five-year program in international relations at Universidad Iberoamericana in Mexico City. He currently resides in Paris and has participated in research seminars on nuclear deterrence and strategic affairs, and ethics and nuclear arms, at Ecole Normale Supérieure de Paris.*

Germany: Loss of communication with commercial aircraft resulted in evacuation of five nuclear power plants

Source: http://world.24-my.info/in-germany-due-to-loss-of-communication-with-the-aircraft-was-evacuated-five-nuclear-power-plants-2/



Mar 11 – In five nuclear power plants in Germany were evacuated because of the plane in the air space of the country with which communication was lost.

According to DW, we are talking about nuclear power plants in the Federal States of Schleswig-Holstein (at Brunsbüttel and Brockdorff) and lower Saxony (Grohnde, Lingen and Unterweser).

The situation in the Brockdorff demanded police involvement because the evacuation coincided with the protests and blockades of nuclear power plants.

After the evacuation of on-site stations were only a minimal part of employees, as provided for emergency cases.

Reportedly, the contact with the plane, which was flying to London, he stopped over Hungary, and then in the airspace of the Czech Republic into the sky was raised by two of

the interceptor.
Further, over Germany, escort aircraft took the Belgian air force.
In the Ministry of environmental protection and the transition to alternative energy sources in Schleswig-Holstein claim that the situation is quickly smoothed over.
Interruption of communication from the plane could be due to technical malfunction or misuse.

List of films about nuclear issues

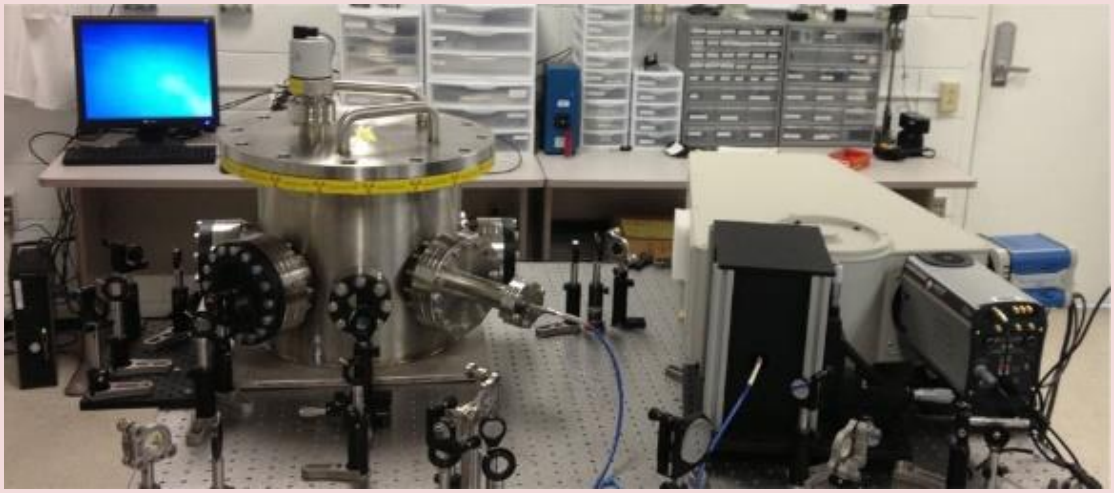
Source: http://wikivisually.com/wiki/List_of_films_about_nuclear_issues

Detecting weapons-grade uranium from afar

Source: http://www.homelandsecuritynewswire.com/dr20170310-detecting-weaponsgrade-uranium-from-afar

Mar 10 – **A technique for detecting enriched uranium with lasers could help regulators sniff out illicit nuclear activities from as far as a couple of miles away.**
It is hard enough to identify nuclear materials when you can directly scan a suspicious suitcase or shipping container. But if you cannot get close?
U-M says that now, researchers have shown that a technique often used to identify chemicals at a distance can also distinguish between ordinary uranium-238 and the fission-prone uranium-235. Just three fewer neutrons make a big difference in the element's potential for destruction.
"It's a much harder problem to try to measure different isotopes of the same element," said Igor Jovanovic, professor of nuclear engineering and radiological sciences at the University of Michigan, who conducted parts of the research while at Pennsylvania State University. "Different isotopes are very important in the case of uranium because some of them can be used for the production of nuclear weapons."

With ordinary chemical detection—the approach used by the Mars Curiosity rover, for instance — a laser strikes a surface and causes electrons to jump off the atoms and molecules, forming a plasma. When the electrons jump back into the atoms and molecules, and then come down from higher-energy states within them, they emit light in a particular set of colors that serve as a fingerprint for that atom or molecule.



Jovanovic and his team — Kyle Hartig, assistant professor of nuclear engineering at the University of Florida, and Isaac Ghebregziabher, a postdoctoral scholar at Penn State — showed that this technique can tell the difference between uranium-235 and uranium-238 when the uranium is bonded with oxygen.
"Not only is it possible to make measurements in air, but some constituents of air in fact make this detection more readily achievable," Jovanovic said.
The technique takes advantage of a phenomenon known as laser filamentation. When very short —

and very intense — laser pulses run through the air, they create a plasma channel along the beam line. The channel serves as a sort of an optical fiber, keeping the laser pulses focused so that they strike their targets in a small spot, even at distances of a kilometer or more.

The intense laser pulses create a plasma from the uranium as well as the air, which gives uranium plenty of opportunity to bond with oxygen. When it does, the energy stored in the bond between the oxygen and the uranium-235 or -238 is just different enough to be detectable.

"These molecules radiate just slightly different colors, depending on whether we are looking at uranium-235 or uranium-238," Jovanovic said.

Often, detection systems aim to catch radiation from spontaneous fissions of uranium-235 — or they cause the fissions by shooting neutrons into the suspicious item. These conventional methods can see through packaging and even some shielding intended to keep radiation from getting out.

This new method would need the uranium to be exposed — perhaps in the dust around the loading bay at a secret enrichment facility. But it could be spotted from off site: The system could fit into the back of a truck, a backpack kit, or even a drone, Jovanovic says.

Jovanovic and colleagues had access to weapons-grade nuclear materials right at Penn State, which still runs a research reactor. To find out whether they could tell uranium-235 from uranium-238, they loaded the sample into a chamber with the laser positioned a few meters away. The laser produced a plasma of air and uranium at the surface of the sample. The team picked up light from the plasma from a light-detecting system one meter from the sample.

Jovanovic anticipates that the method would be useful in other scenarios, such as nuclear forensics. If a nuclear bomb were detonated, governments would want to know what was in it and where it came from. For the most accurate analysis, scientists would need samples collected from the blast site. But it would be safer and quicker to run this style of analysis at a distance.

Or it might be helpful at legitimate nuclear facilities, such monitoring the production of nuclear fuel and ensuring the right level of enrichment.

U-M notes that this study was funded through the Consortium for Verification Technology, a $25 million project headed by U-M to develop new methods for nuclear nonproliferation.

N. Korea 62% likely to conduct nuclear or missile test in next 30 days: think tank

Source: http://www.koreaherald.com/view.php?ud=20170313000150

Mar 13 – North Korea is 62 percent likely to conduct a nuclear test or a missile launch in the next 30 days, a US think tank has predicted based on analysis of big data on the communist nation.

The study, conducted jointly by the Center for Strategic and International Studies and big data firm Predata, analyzed how often the North is discussed on the Internet to predict future possibilities, with a higher frequency meaning stronger "signals."

Signals on the North's weapons of mass destruction showed a "notable spike" beginning March 4, just two days before the North's firing of a salvo of four ballistic missiles toward the East Sea, according to Beyond Parallel, the CSIS website specializing in North Korea issues.

Those signals have since remained elevated, indicating there are more March missile tests to come from North Korea, it said.

"There is a 43 percent chance of North Korean WMD activity taking place in the next 14 days. In the next 30 days, there is a 62 percent chance for North Korean WMD activity. Beyond Parallel defines WMD activity as

nuclear tests and ballistic missile launches," it said.

The North's March 6 missile launches represent the second major provocative act by Pyongyang since US President Donald Trump took office. In its first provocation under Trump, the North test-fired a newly developed intermediate-range ballistic missile on Feb. 12.

The latest launches were seen as a show of force by Pyongyang in response to the ongoing annual joint military exercises between South Korea and the United States that the North has long denounced as a rehearsal for an invasion of the country.

Concerns have persisted that Pyongyang could carry out more missile launches, including a test-firing of an intercontinental ballistic missile capable of striking the continental US that North Korean leader Kim Jong-un threatened to conduct.

Commercial satellite imagery has also shown continued activity at the North's Punggye-ri nuclear test site, a possible indication that Pyongyang may be preparing to conduct its sixth nuclear test after two nuclear tests last year.

Nuclear expert: "Real risk" that Iran and N. Korea cooperating on nuclear matters

Source: http://www.homelandsecuritynewswire.com/dr20170313-nuclear-expert-real-risk-that-iran-and-n-korea-cooperating-on-nuclear-matters

Mar 13 – **There is a "real risk" that Iran and North Korea are engaged in illicit nuclear cooperation,** a former United Nations weapons inspector and nuclear non-proliferation expert told *The Algemeiner* on Thursday.

David Albright, president of the Institute for Science and International Security, called on the Trump administration to investigate any potential nuclear collaboration between the two nations.

"I think the main thing is to try to discover it," Albright said. "We know it [cooperation] happens in the missile and conventional weapons areas. As for the nuclear area, we look at it as an open question. We haven't seen enough evidence yet to make an actual accusation, we just don't know. But I think there is a real risk that Iran and North Korea could cooperate on nuclear matters. It requires a lot of attention from our intelligence services."

He added that such cooperation could be a violation of the 2015 nuclear agreement between Iran and world powers. If Iran is found to be circumventing the deal by advancing its nuclear program with the help of North Korea, that revelation would "be quite damaging to Iran," Albright observed.

Pyongyang and Tehran could be sharing two types of nuclear technology. The **first**, according to Albright, would be "more traditional information about building nuclear weapons and testing nuclear weapons, which North Korea certainly has plenty of to give to Iran." It has been reported that an Iranian delegation observed North Korea's 2013 nuclear test.

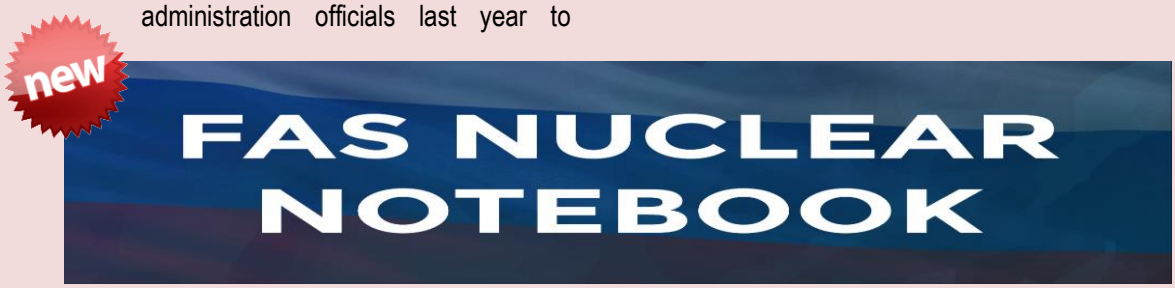
The **second** potential realm of nuclear cooperation would involve "reentry vehicle technology for a nuclear warhead." This is an area where Iran can likely aid North Korea. U.S. officials determined in 2006 that Iran had modified the nose cone of the Shahab-3 ballistic missile to accommodate a nuclear warhead.

Earlier this month, Lt. Col. (ret.) Dr. Refael Ofek and Lt. Col. (res.) Dr. Dany Shoham, experts at the Begin Sadat Center for Strategic Studies, assessed that nuclear cooperation between Iran and North Korea was "likely."

Ofek and Shoham noted that the countries developed complementary technologies, concluding:

The chronology, contents, and features of the overt interface between Iran and NK mark an ongoing evolutionary process in terms of weapons technologies at the highest strategic level. The two countries have followed fairly similar nuclear and ballistic courses, with considerable, largely intended, reciprocal technological complementarity. The numerous technological common denominators that underlie the NW and ballistic missile programs of Iran and NK cannot be regarded as coincidental. Rather, they likely indicate – in conjunction with geopolitical and economic drives –a much broader

degree of undisclosed interaction between Tehran and Pyongyang.
Sen. Ted Cruz (R – Texas) urged three Obama administration officials last year to reveal what the intelligence community knew about nuclear cooperation between Iran and North Korea.



Russian Nuclear Forces (2017)
Source:http://www.tandfonline.com/doi/full/10.1080/00963402.2017.1290375

Federation of American Scientists (FAS) experts **Hans Kristensen** and **Robert S. Norris** added another entry to their longstanding Nuclear Notebook series by delving into the nuclear forces of Russia. Russia is currently in the midst of a "broad modernization of its strategic and nonstrategic nuclear forces," and Kristensen and Norris most recently estimated (early 2017) that **Russia's military stockpile contains approximately 4,300 nuclear warheads**, with 45% (≈1,950 warheads) currently deployed on ballistic missiles and/or heavy bomber bases.
With the latest estimates, insight, and analysis from two of FAS's most prolific experts, this Nuclear Notebook is intended to **educate and empower the public debate about the status, background, and outlook of Russia's nuclear arsenal**. With the current East-West crisis, it is crucial that the debate about the implications of Russia's nuclear modernization is both balanced and especially fact-based.

Hans M. Kristensen *is the director of the Nuclear Information Project with the Federation of American Scientists in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a coauthor of the world nuclear forces overview in the SIPRI Yearbook (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has coauthored Nuclear Notebook since 2001.*
Robert S. Norris *is a senior fellow with the Federation of American Scientists in Washington, DC. A former senior research associate with the Natural Resources Defense Council, his principal areas of expertise include writing and research on all aspects of the nuclear weapons programs of the United States, the Soviet Union and Russia, the United Kingdom, France, and China, as well as India, Pakistan, and Israel. He is the author of Racing for the Bomb: General Leslie R. Groves, the Manhattan Project's Indispensable Man (Steerforth) and coauthor of Making the Russian Bomb: From Stalin to Yeltsin (Westview). He coauthored or contributed to the chapter on nuclear weapons in the 1985–2000 editions of the SIPRI Yearbook (Oxford University Press) and has coauthored Nuclear Notebook since 1987.*

The truth about Satan: Nuclear war in the 21st century

By David Szondy
Source: http://newatlas.com/nuclear-weapons-satan-missile/46845/

Mar 15 – Late last year, the world's news services were abuzz with articles about Russia's new super weapon, an **ICBM called Satan 2** that is alleged to have the capability to fly at 17 times the speed of sound, penetrate US ICBM defenses, and destroy an area the size of Texas. But do these claims hold water, and just how big is the nuclear threat that the world really faces in the 21st century? **What is the truth about Satan 2?**

▶▶ **Read the full article at soource's URL.**

David Szondy *is a freelance writer based in Monroe, Washington. An award-winning playwright, he has contributed to Charged and iQ magazine and is the author of the website* Tales of Future Past.

Nextgen robots for nuclear clean-up

Source: http://www.homelandsecuritynewswire.com/dr20170320-nextgen-robots-for-nuclear-cleanup

Mar 20 - The cost of cleaning up the U.K.'s existing nuclear facilities has been estimated to be between £95 billion, and £219 billion over the next 120 years or so. The harsh conditions within these facilities means that human access is highly restricted and much of the work will need to be completed by robots. Present robotics technology is simply not capable of completing many of the tasks that will be required. Whilst robotic systems have proven to be of great benefit at Fukushima Daiichi NPP, their limitations, which include relatively straightforward tasks such as turning valves, navigating staircases and moving over rough terrain, have also been highlighted.

U Manchester says that the new group comprising Manchester, the University of Birmingham, University of the West of England (UWE) and industrial partners Sellafield Ltd, EDF, UKAEA, and NuGen has been funded with £4.6m from the Engineering and Physical Sciences Research Council.

It will develop robots which have improved, power, sensing, communications, and processing power. They will also develop systems which are able to address issues around grasping and manipulation, computer vision and perception. Importantly the robots will be autonomous – able to operate without direct supervision by humans.

The University of Manchester's Professor Barry Lennox, who is leading this project, said: "This program of work will enable us to fundamentally improve RAS capabilities, allowing technologies to be reliably deployed in to harsh environments, keeping humans away from the dangers of radiation."

Within the next five years, the researchers will produce prototype robots which will then be trialed in both active and inactive environments. It is anticipated that these trials will include using robotic manipulators to autonomously sort and segregate waste materials and to use multiple robots, working collaboratively, to characterize facilities that may not have been accessed for 40 years or more.

The technology will not only have potential for improving robots used at nuclear sites, but also in other hostile environments such as space, sub-sea, and mining. Or in situations such as bomb-disposal and healthcare which are dangerous or difficult for humans.

The University of Manchester notes that the university has already developed small submersible and ground-based vehicles that can be deployed to survey nuclear facilities which will be used in this project, allied with the skills and knowledge of the other partners.

Professor Lennox added: "If we are to be realistic about clearing up contaminated sites, then we have to invest in this type of technology. These environments are some of the most extreme that exist, so the benefits of developing this technology can also apply to a wide range of other scenarios."

CDC Releases New Radiation Resources and Tools

- Communicating in Radiation Emergencies: Myths of Radiation, a new training that introduces participants to some common myths of radiation and identifies communications strategies to combat these and other myths.
- Radiation Thermometer, a new tool to help put common radiation doses in perspective. It is the radiation dose, or the amount of radiation, that is the critical issue in determining health consequences.
- Radiation Hazard Scale, an emergency communication tool that provides a frame of reference for relative hazards of radiation, conveying meaning without using radiation measurements or units that are unfamiliar to people.
- Radiation Emergency Training for Poison Center Staff, an informational and educational resource about radiation exposure and illness for poison control staff.
- Radiation Emergencies Media Toolkit , an online Radiation Emergencies media toolkit that provides important content and materials in an easily accessible format to key audiences.

NUCLEAR TURKEY? Imam close to Erdogan calls for weapons NOW amid tensions with EU

Source: http://www.express.co.uk/news/world/780240/TURKEY-Imam-Erdogan-nuclear-weapons-NOW-EU-tension-Germany-Netherlands

Mar 16 – The worrying advice has been called weeks ahead of a Turkish referendum aimed at giving more power to President Erdogan - and in the midst of a keeping fallout between Ankara and EU leaders.

Hayrettin Karaman, the Turkish AK Party's go-to religious leader, attacked 'the West' in a letter which insisted Erdogan should immediately invest in weapons of mass destruction.

In the online post the imam accused Christian countries in the West of egotism and racism - stating the bad attitude towards Turkey has been "accelerated".

President Erdogan is in the midst of a deep fall out with European nations including Germany and the Netherlands after both countries banned rallies and kicked out his ministers who had sworn to campaign for his referendum.

Mr Erdogan retaliated by comparing them to Nazis and protests were held outside the Dutch embassy in Ankara.

The fallout threatens the £5billion one-for-one migrant deal.

But, if Mr Erdogan listens to his favourite religious leader, the tensions could be ramped up even further.

«L'Africa resta la meta dei rifiuti tossici»

Source: https://www.avvenire.it/attualita/pagine/lafrica-resta-la-meta-dei-rifiuti-tossici

ISIS strap suicide vests to PUPPIES in horror footage of sick front line bomb tactic

Source: http://www.express.co.uk/news/world/772017/ISIS-puppies-dogs-suicide-bombs-belts-Iraq-Mosul-fight-Jihadi

Feb 27 – The authenticity of the video is currently unclear but it appears to show Islamic State jihadis, known for their improvisations on the battlefield, have wrapped the tiny animal's torso with explosives before sending it across the front line.

The horrifying video was apparently uploaded online by fighters with the Iraqi Popular Mobilisation Units.

The PMU, or Al-Hashd Al-Sha'abi, is a group of militia, brought together and state-sponsored to battle with jihadis in Iraq.

In 2014 the group was incorporated into the country's armed forces to help fight on the battlefield as major cities were overtaken by terrorists.

Three PMU fighters crouch over the small animal in the video, one resting a knife on the ground as they speak to the camera about the find.

They tell the camera the dog is strapped to four bottles, likely filled with shrapnel.

Accoring to the men, if detonated it could kill three of four people.

The trio claimed the dog was sent around the corner to where they were positioned.

PMU members said the dog was fitted with explosives which are remotely detonated

Express.co.uk is working on verifying the claims in the footage.

Seven things no one tells you before you become a bomb disposal expert

Source: http://www.telegraph.co.uk/men/the-filter/seven-things-no-one-tells-become-bomb-disposal-expert/

Feb 24 – During his ten year career in the British Forces, Andy Torbet served in the Army's Underwater Bomb Disposal Team, helping to disarm explosives in Iraq and Afghanistan. Now an adventurer and cave diver, he spoke to Telegraph Men about his high-pressure former career and how it helps him approach journeys into unknown worlds...

1. Forget everything you've seen in the movies

There's never a red or a blue wire. And there's never a clock – who would put a clock on a bomb? Your go-to response is 'blow in-situ', where you put a charge next to the device, push the button and blow the charge up. A lot of the time, bomb disposal equates to blowing stuff up.

Kathryn Bigelow's The Hurt Locker

2. Bomb suits are rare

Suits are built to protect your head and your torso – to keep you alive, not for movement. They've got a fold down skirt at the front, basically to save your balls.

But most of the time, you don't wear a bomb suit. It's heavy and in Iraq, it's about 54 degrees celsius. And if you're defusing an undetonated World War 2 bomb that's been found in London, it might be 250kg of explosive. If that went off a bomb suit isn't going to do very much.

3. The 'long walk' is very zen

Approaching the bomb – the 'long walk' – is incredibly calming. You take a breath and relax, nothing else matters. You enter this bubble and it's just you. It's called the long walk: you feel the adrenaline and you're incredibly focused.

Long term, it's an extremely high pressured job – in Afghanistan, the guys were working 24/7. But in that moment, when you walk towards the device there's a degree of calm and clarity.

And the other thing is that a lot of these devices are so big, that if they do go off, you'd never know.

4. Bomb disposal units are a force for good

It doesn't matter what political stance you want to take, there's no way a sane person can say defusing bombs and clearing minefields is a bad thing. It's good for everybody – not just the British soldiers but also the local inhabitants. You're fortunate in bomb disposal because no matter what side you're on, we're doing something good.

5. There's a lot of responsibility when you're a captain

Fatalities among bomb disposal experts were relatively rare during my time in the Army – but it got worse in Iraq. And in Afghanistan, there were a lot more IEDs. We lost significantly more guys.

I was a captain, the senior bomb disposal officer in the British Army out in Iraq, so I was mostly co-ordinating. There are three things to do: you had to do your job, you had to look after your men and make sure they all went home safely, and then you had to go home yourself in one piece. That wasn't always possible. I was fortunate that whenever I was posted somewhere, all the men I took out came back. That's not my accolade – it's because they were so good.
You feel a huge amount of protection and responsibility.

6. Sewers are an unfortunate downside of the job
With underwater bomb disposal, the Navy takes everything from the highwater mark below; the Army takes everything else. That's why the Army has an underwater bomb disposal unit. We're in charge of fresh water: rivers, lakes and – unfortunately – sewers. Guys would have to go into sewers in Bazra, which was fairly unpleasant. You wear a scuba suit and there are times when you have to fully submerge. It's pretty minging.

THE FEW AND THE BRAVE

7. Mentally, you never lose the lessons you learned
I'm now a cave diver, but my approach is no different to when I was disposing bombs. Preparation is everything.
In Finland last December, we were doing three hour dives – we had to smash the ice to get into the lake. And three hours later, when you come back you have to smash it again, using your fist or a bottle.
Being submerged in such cold waters for so long takes a lot of forethought, and technology. We used a Cat S60 thermal imaging smart phone, which showed us how well insulated our equipment was. If you took photos of someone in full diving kit and you could see hotspots, that meant they weren't insulated and heat was getting out. A problem. If they're completely black, it's all being trapped by the suit.
In a sense, bomb disposal and cave diving are very similar. No-one gets injured when you're cave diving – you're either OK or you're dead. Same with disposing a bomb. It's black and white, and it's great because it focuses you. It can be done extremely safely if you approach it with the right mentality.
Everyone thinks I'm an adrenaline junkie but I'm not – I'm the most cautious and paranoid man in the room. **My priority is to come back in one piece.**

25-year-old Somali man charged with producing a bomb in Denmark

Source: http://cphpost.dk/news/25-year-old-somali-man-charged-with-producing-a-bomb-in-denmark.html

Feb 24 – A 25-year-old Somali man in Aarhus has denied charges that he was involved in the production of bombs that were found in the basement of a house in Denmark's second largest city.

Police have been secretly investigating the case for four months.
And now the prosecution has lifted a bit of the veil.

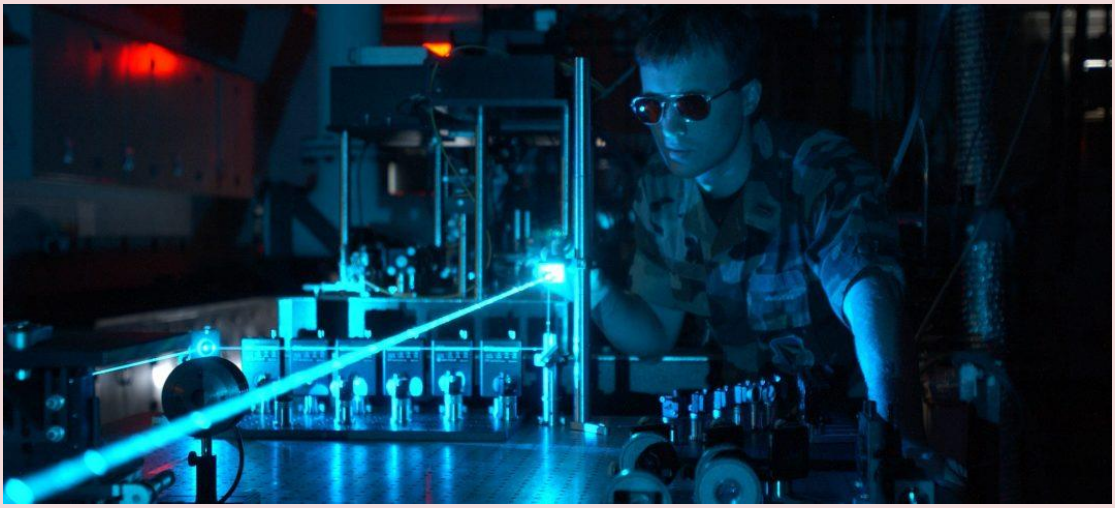
Denies the charges
According to the charge sheet, the **bomb consisted of two explosive devices of 200 grams each, fuses and a detonator.**
"My client denies the charges," said Lars Henriksen, who is defending the 25-year-old man.

He declined to further comment, and the judge in the case has decided that the hearing will be held behind closed doors.

The defendant did admit guilt on three other counts: possession of a small knife, possession of 650 grams of cannabis and 23 ampoules of doping substances.

Improvised Explosive Detection – New Approach

Source: http://i-hls.com/2017/03/improvised-explosive-detection-new-approach/



Mar 02 – On the first floor of the Robert H. Mollohan Research Facility is a small team of researchers who are quietly developing a new, game-changing technology that could potentially eliminate the threat of the Improvised Explosive Devices (IEDs).

These weapons are typically hidden or buried in extremely difficult to detect areas and are responsible for thousands of injuries and deaths to coalition forces from 2001 to 2014, according to U.S. Department of Defense statistics.

The team of three who are trying to eliminate the growing threat are led by High Tech Foundation principal scientist Balakishore Yellampalle, and have been perfecting a device that detects trace levels of explosives from a distance using a mechanism called **"deep ultraviolet laser beam."**

In this approach, Yellampalle told theet.com, that beam is pointed at a surface, and the scattered light is then reflected back, collected and analyzed by the sensor. A computer program then determines if the spectrum indicates the presence of explosives.

Another team member, Robert Martin, said the real benefit of the Deep Ultraviolet Resonance Raman Explosive Detector is how it could ultimately save lives. "If there's a bomb in range, our system can help keep a warfighter out of harm's way," he said.

In order to find traces or potentially microscopic explosive elements, an operator would fire a laser signal from the detector to a target of interest. Almost instantly, the reflected light senses or reads materials on the target.

"Whether there's background interference, sand, salt or whatever it is that overtop the target, we want to see if there is an explosive there. Then, the operator can hopefully take down whatever bomb threat there might be" Martin said.

However, the laser is more than just an intense beam of coherent monochromatic light. According to Martin, the system they've developed is smart. "It's called, 'spectroscopy,'" he said. "We shoot the sample, and the spectrometer sees the light that is reflected back. So, it looks at the whole spectrum of light".

From there, he explained, the device actually detects all sorts of tiny bits of material from the laser light that is reflected back from the object. The real trick is how the system deciphers precisely what the laser is seeing. "We shoot a bunch of stuff and build a library," Martin said.

The library Martin is talking about is a large, intuitive computer database the team developed. The data is made up of what all types of tested items would look like, such as salt, sand, sugar, water, TNT or even

salt with TNT. Once the system recognizes or "remembers" more explosive substances, the recognition process is easier. meaning that the system gains knowledge and can apply it in later uses.

"So when we're out in the field and get data, whatever it might be, we can see if it matches what we've seen before," he said. The Deep Ultra Violet Resonance Raman Explosive Detector project is actually a continuation of an earlier one started in February 2012.

"We've been developing the technology in stages to meet our customer requirements," Yellampalle said. "The current phase of the project was awarded May of 2016 for two years."

The award phase the team is working on today is called phase three. During the second phase, the team developed a compact prototype they tested in the lab.

"Phase three of the project is getting the system down to 20 pounds or less and can be mounted on a wider variety of devices," Martin said. Eventually, however, the plan is to shrink the detector down to a hand-held size, which Yellampalle said could make it more attractive to both military and civilian users.

"We're building a portable detector as opposed to other competing technologies that are heavy," Yellampalle said.

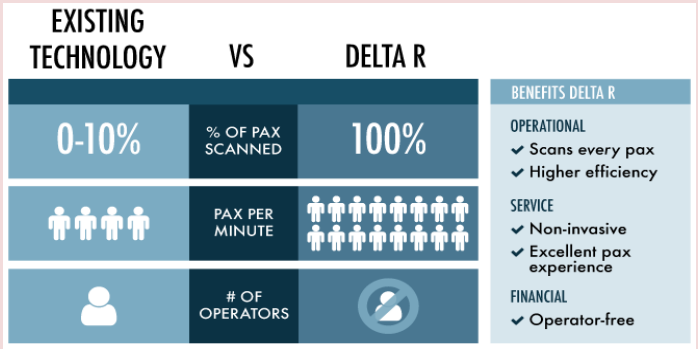
No Need to Remove Shoes for Airport Security Checks

Source: http://i-hls.com/2017/03/no-need-remove-shoes-airport-security-checks/

Mar 04 – **A new airport security technology developed. Amsterdam Airport Schiphol is to be the first to use new ultraviolet scanners, eliminating the need for passengers to remove their shoes for security checks.**

The **Delta R shoe scanner** was developed by Dutch startup, Stage Gate 11 (SG11), who specialize in technological product development for the security industry. The scanner has a detection unit that uses UV light, meaning airport security staff can more easily pick out passengers who have hidden unsafe substances, such as drugs or explosives, in their shoes. The technology is suitable for many different applications, like parcel scanning.

The need for such technology follows the attempted bombing of an American Airlines flight in 2001 with an explosive concealed in a hollowed-out shoe heel. According to passengerterminaltoday.com, the **shoe scanner detects traces of substances using UV reflection, comparing the emitted beam of light with the reflected one that has bounced off a surface. Since all substances have their own unique patterns, the technology quickly and accurately recognizes traces of illegal or threatening substances.**



SG11 worked with interior specialists INTOS in the design of the product. Michiel Poppink, co-owner of SG11, commented, "We have the technology and application possibilities, but we really needed INTOS as a knowledge partner to design the show scanner. Their experience at

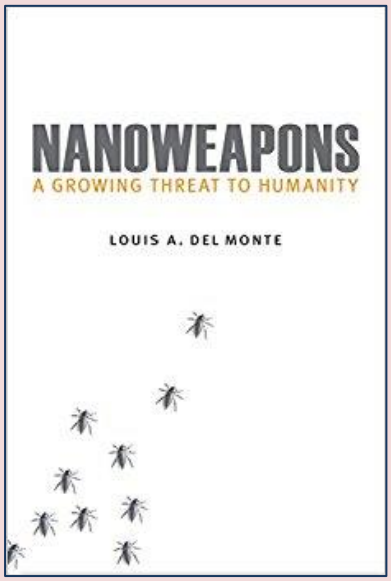
international airports meant that INTOS knew exactly which requirements a product had to meet for optimum performance. All of this led to the perfect transformation of our ideas into an aesthetic concept and ultimately a functional product".

Nearly Invisible Weapons of Mass Destruction Spark New Arms Race

By Louis A. Del Monte

Source: http://finance.yahoo.com/news/nearly-invisible-weapons-mass-destruction-134000087.html

Mar 07 – Nanoweapons just might render humanity extinct in the near future—a notion that is frightening and shocking, but also more likely as the technology advances. In ***Nanoweapons: A Growing Threat to Humanity***, the first book about this new class of weapons, Louis A. Del Monte describes the most deadly generation of military weapons the world has ever encountered. With dimensions one-thousandth the diameter of a single strand of human hair, this technology threatens to eradicate humanity as it incites world governments to compete in the deadliest arms race ever.



"*Nanoweapons* opens the cloak of secrecy on the developing area of nanotechnologies and how societies may use them in the future for good and evil," said Tamara Bratland, engineer for a Fortune 500 medical device company. "A very captivating topic."

In his insightful and prescient account of this risky and radical technology, Del Monte predicts that nanoweapons will dominate the battlefield of the future and may ultimately prove more problematic than nuclear weapons. He traces the emergence of nanotechnology, discusses the current development of nanoweapons—**such as the "mini-nuke," which weighs five pounds and carries the power of one hundred tons of TNT**—and offers concrete recommendations, founded in historical precedent, for controlling their proliferation and avoiding human annihilation. Most critically, *Nanoweapons* addresses the question: Will it be possible to develop, deploy, and use nanoweapons in warfare without rendering humanity extinct?

Louis A. Del Monte *is an award-winning physicist, featured speaker, and the chief executive officer of Del Monte and Associates, Inc. During his thirty-year career as a physicist and business executive at IBM and Honeywell, he led the development of microelectronics and sensors and developed patents fundamental to the fabrication of integrated circuits. He is the author of The Artificial Intelligence Revolution: Will Artificial Intelligence Serve Us or Replace Us? and How to Time Travel: Explore the Science, Paradoxes, and Evidence.*

5,000 schoolchildren are evacuated after hoax bomb threats in 11 counties

Source: http://www.dailymail.co.uk/news/article-4293578/Primary-schools-Devon-Suffolk-evacuated.html

Mar 08 – **Nearly 5,000 children were evacuated today after at least 15 schools across 11 counties in Britain allegedly received bomb threats.**

Pupils at schools in Suffolk, Devon, Sussex, Hampshire, Surrey, Dorset, East Yorkshire, Essex, Somerset and Warwickshire were told to leave the building with parents being asked to collect their children urgently today.

Parents of pupils at one school in Ipswich received a text saying: 'Please don't worry. We have had to evacuate school. Everyone has been accounted for.'

However, all of the threats made so far - including one in Cornwall - are being treated as hoaxes, with no suspicious devices found at any of the schools involved.

Parents linked the evacuation of Whitehouse Community Primary School in Ipswich - which left pupils crying - to an alleged bomb threat made in a telephone call.
Kirsty Youngs, 33, whose ten-year-old son was one of the evacuees, said: 'They were scared. Around 500 children were in the hall, there were lots of tears.
'They (teachers) refused to say anything at all about what happened. We were just told to take our children.
'The children said the fire alarms went off and that instead of going to line up on the playground they went to the hall.'
The school was in lockdown this afternoon and forensic police officers were spotted entering the building.
A Suffolk Police spokesman said: 'We were called by the school reporting a bomb threat. they took the decision to evacuate. We are treating it as a hoax.
'A number of other police forces are also investigating malicious communications to schools and we're working together to determine who was responsible and whether the threats were linked.'
In Essex, pupils at Milton Hall Primary School in Westcliff were evacuated to a nearby school following a hoax call over 'a device' in a classroom at 11.30am.
Parkfield School in Taunton, Somerset, also received a telephone bomb threat today, leading to pupils being sent home and police sniffer dogs sent in.
A similar incident happened at Southill School in Weymouth, Dorset, which was also evacuated due to a bomb scare.
Other schools evacuated due to threats were Highlands Primary School in Hull, East Yorkshire, and Boxgrove Primary School in Guildford, Surrey.
Meanwhile in Devon and Cornwall, three schools in Exeter, Plymouth and Falmouth also received claims that suspicious devices were in place.
Parents of children at St Sidwell's Church of England School in Exeter were messaged just after 12pm to inform them of the action.
St Sidwell's acting headmaster Mr Tom Page said in an email to parents: 'We received an electronic phone call at approximately 8.50am saying that a suspicious device had been placed on the school premises.
'We therefore put our emergency evacuation procedure into place. The children were promptly evacuated to the Methodist Church Hall on Sidwell Street.
"The police were on the school site within minutes and began their search of the building.
'There have been three recent hoax calls to schools in Devon of exactly the same nature and after a thorough and comprehensive search of the building the police informed me that it was completely safe for the children and staff to return to school.
'The children have been informed of the reason for the evacuation."
The other schools affected were St Mary Catholic Primary School in Falmouth and Ford Primary School in Plymouth, but neither were evacuated. However, police were in attendance and liaising with staff.
A Devon and Cornwall Police spokesman said: 'Whilst we are currently of the opinion that this call is without substance, as a precaution, police officers attended each of the school in question.
'This is being treated as a hoax call and will be offences under the Malicious Communications Act. We take this extremely seriously, and condemn whoever is responsible.
'Malicious threats such as these divert police resources and cause disruption and alarm to the public and are completely irresponsible.
'Members of the public are encouraged to be vigilant and report anything suspicious to police.'
Meanwhile three schools in Hampshire were also targeted, which all took the decision to evacuate the pupils and staff before a search was carried out.
The trio of Hampshire schools were Oakfield Primary School in Totton, Castle Primary School in Portchester and Castle Hill Primary School in Basingstoke.
Elsewhere at Paddox Primary School in Rugby, Warwickshire, a threat was reported at 9.45am, with sniffer dogs and specialist officers sent to search the site.
Parents began rushing to pick their children up from their evacuation point at the nearby Ashlawn School after reports of the threat were posted on Facebook groups.
Councillor Yousef Dahmash, a Paddox Primary parent, said: 'There was a threat made to the school. It appears that it was a bomb threat.

'We don't know where it came from at the moment. Police were on site this morning and they are still there now.

'At first, lots of parents were really worried about their children, but word got round quite quickly that they were all safe.

'When I went to collect my daughter at around 10.45, most of the children were quietly sat in the large hall at Ashlawn. The teachers seemed well drilled and did a very good job.'

A Warwickshire Police spokesman said: 'We received a call at 9:45am about a threat to a primary school on Fareham Avenue.

'The school was evacuated and trained officers with search dogs entered the school. So far, nothing has been found.'

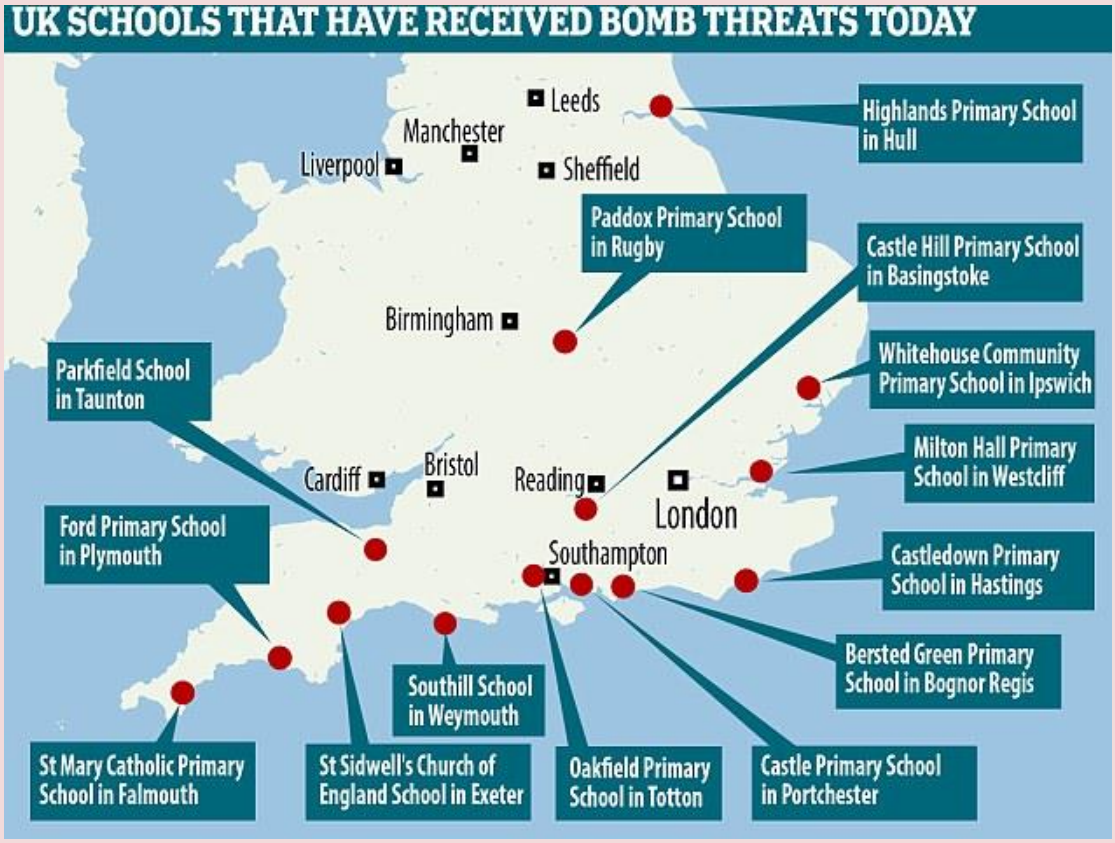
Meanwhile staff and pupils two primary schools in Sussex were evacuated after reports that bombs had been left on the premises.

Calls with threats were made shortly after 9am to Bersted Green Primary School in Bognor Regis and Castledown Primary School in Hastings.

Pupils and staff at both schools were evacuated and the buildings and grounds were searched by police officers.

Superintendent Carwyn Hughes, of Sussex Police, told the Brighton Argus: 'The calls were received by the schools just minutes apart.

'They show similarities to a number of calls that were received at other schools in the UK. The calls



remain under investigation as malicious hoaxes.'

Which UK schools have received threats today?

- St Sidwell's Church of England School in Exeter, Devon [evacuated]
- Whitehouse Community Primary School in Ipswich, Suffolk [evacuated]
- Castle Hill Primary School in Basingstoke, Hampshire [evacuated]
- Paddox Primary School in Rugby , Warwickshire [evacuated]
- Oakfield Primary School in Totton, Hampshire [evacuated]
- Bersted Green Primary School in Bognor Regis, Sussex [evacuated]
- Castle Primary School in Portchester, Hampshire [evacuated]
- Castledown Primary School in Priory Road, Hastings, Sussex [evacuated]

- Milton Hall Primary School in Westcliff, Essex [evacuated]
- Parkfield School in Taunton, Somerset [evacuated]
- Southill School in Weymouth, Dorset [evacuated]
- Highlands Primary School in Hull, East Yorkshire [evacuated]
- Boxgrove Primary School in Guildford, Surrey [evacuated]
- St Mary Catholic Primary School in Falmouth, Cornwall [not evacuated]
- Ford Primary School in Plymouth , Devon [not evacuated]

How hoax calls led to dozens of evacuations of UK schools last year

The hoax calls and follow a similar pattern to incidents last year when dozens of UK schools faced a series of bomb threats just as the GCSE exam season started.

Over a period last May, 27 schools shut on a Monday due to bogus calls, before 16 more closed the following day and then another ten on the Wednesday.

It was feared last year that a campaign led on social media to close down schools was sparking copycat calls by people making bomb threats.

A Russian Twitter group known as 'Evacuators 2K16' appeared to have claimed responsibility for hoaxes, telling pupils to contact them to 'get out of school'.

There were also reports of similar incidents in France, the US, Australia and Japan.

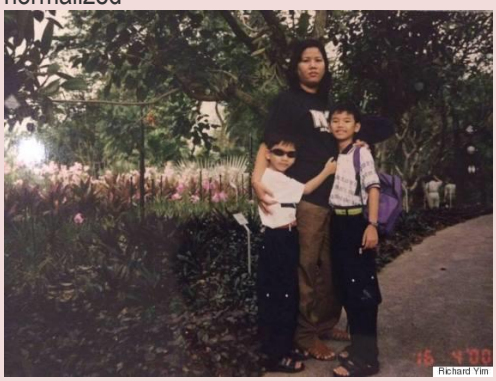
EDITOR'S COMMENT: Just keep in mind that the evacuation process following a bomb hoax might result in high numbers of people in a given area and this is quite attractive for a real detonation causing high scores of victims. Just like secondary IEDs aiming at first responders,

Canadian Engineer Designs A Machine To Rid The World Of Landmines

Source: http://www.huffingtonpost.ca/2017/03/09/canadian-invention-landmines_n_15268472.html

Mar 14 – An object the size of a tuna can had a long and menacing hold over Richard Yim's childhood in Cambodia.

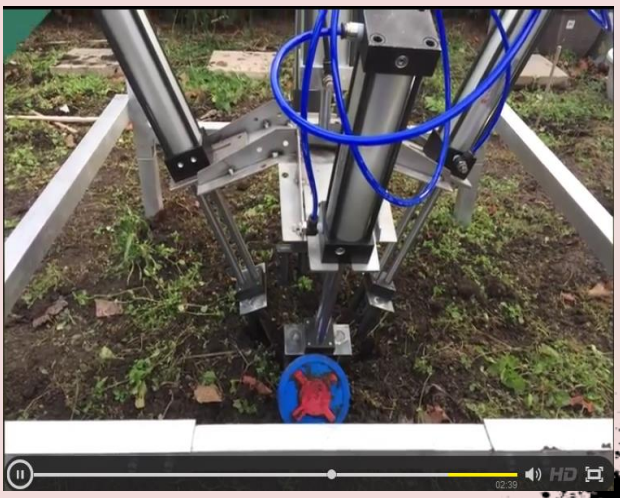
That was the average size of unexploded landmines that dotted parts of the country. Learning which streets and swaths of land to avoid is a childhood rite to many Cambodians — their ominous presence, normalized



Richard Yim poses with his mom and older brother in a family photo. (Photo: Richard Yim)

So when Yim moved to Canada at the age of 13, one of the very first things he noticed about everyday Canadian life was the freedom to safely go wherever he wanted.

"It's very different when you suddenly are actually able to walk where you want. It's such a strange feeling in a way," he told The Huffington Post Canada.



According to the Cambodian Red Cross, children account for 50 percent of landmine casualties in the country.

A decade after leaving Cambodia, Yim is utilizing his childhood experience by starting a Canadian company — named The

Landmine Boys — to take on the 110 million landmines still buried around the world.
The University of Waterloo graduate is drawing attention for his invention, which could put the dangerous work people undertake defusing landmines in the past.

Watch Yim explain how his machine works in the video above.

Colombia Aims to Rid Country of Landmines by 2021

Source: http://www.voanews.com/a/colombia-aims-rid-country-landmines-by-year-twenty-twenty-one/3724700.html

Mar 14 – **Colombia, one of the most mined countries in the world, aims to remove all landmines and other explosives by 2021** after the government and FARC rebels signed a peace deal last year, a top government official has said.
Colombia's left-wing guerrilla group, the Revolutionary Armed Forces of Colombia (FARC), planted thousands of landmines across swaths of the country during its five-decade war against the government.
"Forty percent of the areas that were covered in landmines for the past 25 years are now being cleared to reach the goal of having a Colombia free of anti-personnel mines by 2021," Rafael Pardo, the government's post-conflict commissioner, told local media Monday.
After Afghanistan, Colombia has the second-highest number of landmine casualties, with more than 11,500 people killed or injured by landmines since 1990, government figures show.
The FARC rebels planted homemade mines in mostly rural areas, using empty glass bottles of rum, coffee and tuna cans, and plastic tubes filled with sulfuric acid.
In 2015, the government and FARC rebels agreed to work together to remove landmines during peace talks in Cuba.
Under the December peace accord, around 6,300 FARC fighters have so far moved to designated areas across Colombia where they will hand in their weapons over the next six months.
The government hopes that nearly 1,000 former FARC combatants will work to identify and clear mines, Pardo said.
With the FARC moving away from their former strongholds, it is now safer for government military demining teams, along with local and international demining groups, to work in new areas.
Colombia's president, Juan Manuel Santos, has said clearing landmines is a key challenge facing the nation as it emerges from decades of war and is crucial for rural development.
Experts say Colombia's mountainous and jungle terrain make mine clearance difficult, and it will take Colombia at least a decade to rid the country of all its landmines.
International donors, including the United States and Norway, have so far contributed nearly $112 million for landmine clearance in Colombia.

How landmines and booby traps are piling fresh terror on war-weary Iraqis

Source: http://www.euronews.com/2017/03/01/how-landmines-and-booby-traps-are-piling-fresh-terror-on-war-weary-iraqis

Mar 14 – Already scarred by the horrors of war and ISIL occupation, villagers returning home in Iraq are facing a fresh terror.
They have found communities covered in a swathe of landmines and their homes riddled with booby traps.
The number of landmines around Mosul is unprecedented and their viciousness unimaginable, says the Mines Advisory Group (MAG).
The charity says it has cleared more than 8,000 devices since last summer, including 1,000 landmines and booby traps in one village alone, Tullaban.
"The grief and fear in communities after what they've been through, like losing family members in the

fighting, is just horrendous," said Sean Sutton, who spent three months working with MAG experts near Mosul at the end of 2016. "Then to flee and come back and just when you think it's sorted, you get this."

Sutton, communications manager for MAG, told Euronews the devices were improvised but made on an industrial scale.

He said there were 'barrier' minefields between or around villages, some up to 20 kilometres long.

Even if civilians escape these, some are being blown up by booby traps in their homes.

"We've found them inside chicken coops, in freezers, in cupboards and there was one reportedly set off by a TV remote control, but we don't know whether this was when they stood on something else as they were turning on the television," said Sutton. "Not every house is set up like this but it's a lottery for people going back."

MAG says civilian deaths from landmines are escalating but precise figures are difficult.

Authorities are not differentiating between those killed by improvised explosive devices or during the conflict.

"There was one family that I met in a village [Wardak] near Mosul and I came across this guy and his daughter who were putting sheep in a pen," Sutton recalled. "It was quite picturesque, so I took some photos.

"Six weeks later I went back and I found out the guy's 14-year-old son had died. He'd been playing and dancing to music on his phone and went to check on the sheep, in the same place he'd been going to repeatedly, and there was an explosion.

"His father ran barefoot over to where it happened and his son's legs had been blown off and his body burnt to a toast.

"That was really hard. The whole family was there and it was just awful. He said he had other sons who were fighting in the war against ISIL. He told me he expected them to die but he never expected his younger son to, because he was still a child."

MAG is calling for more funding to tackle the problem. It says an extra £8 million (9.3 million euros) would allow it to double the number of mine-clearing experts in Iraq.

Nina Seecharan, MAG's Iraq director, said: "We have been working around the clock to clear landmines in Mosul and make villages, schools and homes safe to go back to, but more support is needed if we are to prevent further civilian casualties.

"We are outraged by the escalating loss of civilian life. Our thoughts are with the families of the innocent men, women and children killed by landmines in recent months. The indiscriminate nature of these weapons means they should have no place in modern warfare."

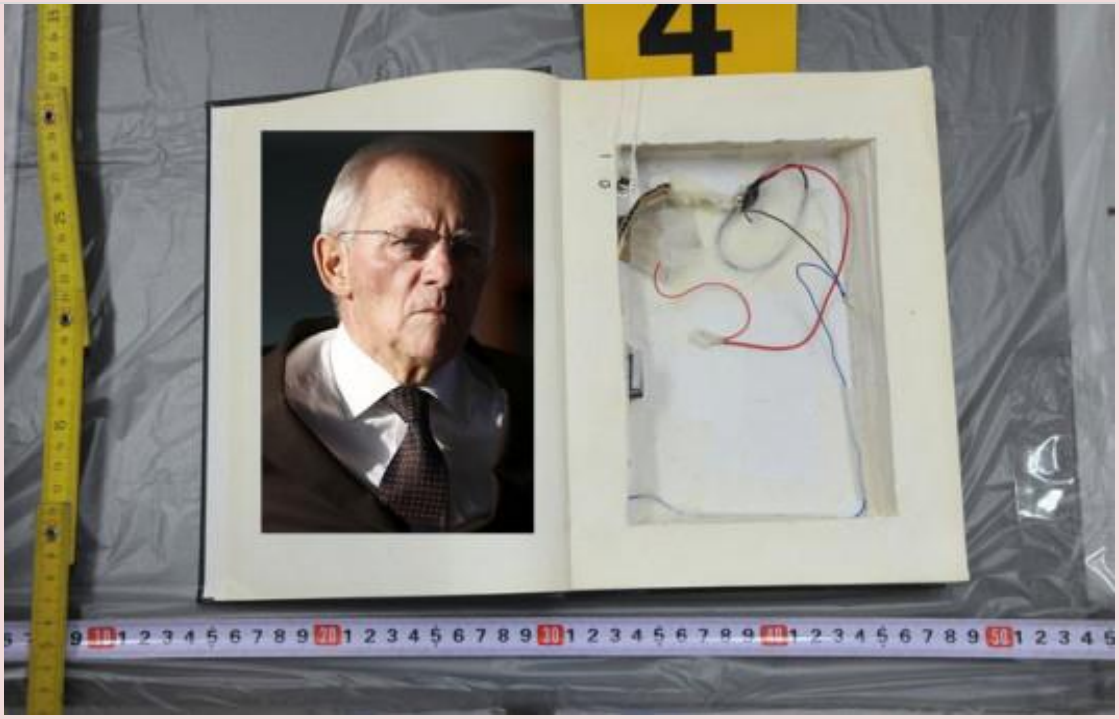
Parcel bomb was sent to Schaeuble from Greece

Mar 16 – Greek authorities indicated late Wednesday night that they had not received an appeal for information from German authorities following reports in the German media that a package with explosives sent to Finance Minister Wolfgang Schaeuble had been mailed from Greece.

The name and address of a New Democracy Party MP (Adonis Georgiadis – photo right) was written on the envelope bearing Greek stamps.

According to reports by Deutsche Presse-Agentur and Maerkische Allgemeine, a "functioning explosive device" was found in a package sent to the ministry in Berlin on Wednesday morning.

The device was successfully defused, the reports said.



A second parcel bomb sent to the offices of the International Monetary Fund (IMF) in Paris wounded one woman. Again it was sent from Greece and the sender cited on the package was New Democracy spokesman Vasilis Kikilias, Alternate Citizens Protection Minister Nikos Toskas said on Thursday, speaking at the evening newscast of ANT1 TV channel. He said the intended recipient was the Director of the IMF Europe Office, Jeffrey Franks. Toskas said Kikilias was briefed about these developments, adding that the senders address was an old one used by ND's spokesman. When asked about why the use of the names and addresses of politicians on the bomb parcels, the minister said the perpetrators possibly see it as a way to "offend the political system."

A militant Greek group has claimed responsibility for Wednesday's parcel bomb mailed to the German finance ministry in Berlin, claiming the failed attack was part of a campaign they dubbed 'Nemesis Project.'

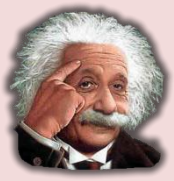
"We still have the rage. We sent the package to Germany's finance minister as part of the second act of Nemesis Plan," **Conspiracy of Fire Cells** said in a statement posted on a radical anti-establishment website. *"Nothing is over, everything continues."*

The group, designated a terrorist organization by the US Department of State, said the failed attack was part of an ongoing operation they call the 'Nemesis Project'.

Last November the group described the project as *"an international proposal to create a list with the names of people in authority so that we can attack them where they feel safe, on the sidelines… at their own houses."*

The group became prominent in Greece at the beginning of the country's economic crisis and has previously claimed responsibility for a wave if parcel bombs sent to foreign embassies in 2010. In 2011, six members of the group were sentenced to between 11 and 37 years in prison.

Investigators told BFMTV the **device was a "large black cylinder, about 30cm long", with the blast so large the room's ceiling was hit by shrapnel.** Police authorities in Paris said the explosive substance was not a bomb but rather a homemade "big firecracker".



Outrage as police kill runaway sniffer dog at Auckland Airport

Source: http://www.telegraph.co.uk/news/2017/03/17/outrage-police-kill-runaway-sniffer-dog-auckland-airport/

Mar 17 – New Zealand police have sparked outrage by shooting dead a runaway sniffer dog at Auckland Airport.

Police decided to take action after the 10-month-old bearded-collie and German shorthaired pointer cross called Grizz prevented planes from taking off.

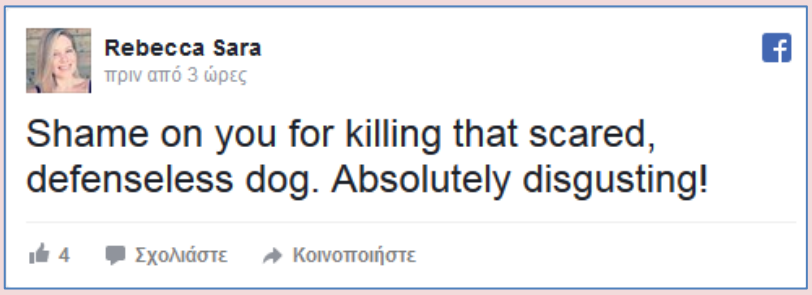
Sixteen domestic and international flights were delayed for safety reasons at the nation's busiest airport while the dog was on the loose for three hours, a spokeswoman for Auckland Airport, Lisa Mulitalo, told Reuters.

"The dog was clearly distressed and wouldn't let anyone near it so the decision was made to shoot the dog," she said.

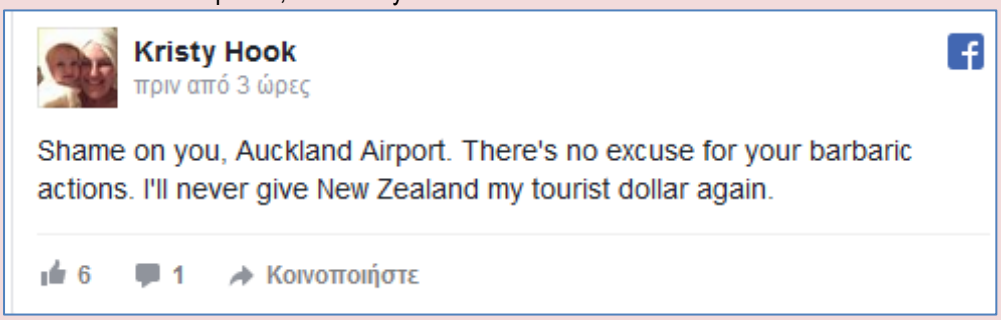
Grizz was reportedly not on the tarmac but on the outer perimeter of the airfield.

A police marksman killed the dog, which was in training to detect explosives, said Mike Richards, a spokesman for New Zealand's Aviation Security Service.

"Of course it was dark for most of the time it was on the run, they tried everything they could, but just couldn't lure the dog back, I think it was just freaked out," he said.



"The handler and Avsec (Aviation Security Services) are naturally upset but do understand there were no other options, in the very difficult circumstances."



National animal rights organisation Safe declared the shooting of Grizz as "needless", the New Zealand Herald reported.

"A tranquilliser gun should have been used after efforts to catch the dog failed. If such a gun was not available - which it should - then they could have borrowed one from Auckland Zoo or elsewhere," spokesman Hans Kriek said.

"We hope that lessons will be learned from this and that better systems will be put in place to avoid such unnecessary killing in the future."

Hilary Barry, a host on TVNZ's Breakfast programme, also asked why a tranquiliser gun wasn't used.

"One of them got spooked at Auckland airport and went a bit cray-cray and was running around on the tarmac. So? It's only Auckland airport. Sixteen flights were delayed. So?" she said.
"So they shot it! They shot it dead. They've got to have tranquiliser guns, surely. They shot the dog dead. I don't care if your plane was delayed, they don't need to shoot the dog."
The airport's Facebook page was also flooded with posts criticising the decision to shoot the animal.
The dog's handler was identified as Noel Thorburn. His son, Nicky, said on Facebook that his father was "very upset" by the decision but understood that it was a "last resort".
"I'm reading disgusting comments ... people need to understand how traumatising and upsetting this was for him," he said.

Perhaps one day...

GREYSCAN – Inorganic explosivee detector

A world-first in the detection of inorganic explosives

Source: http://www.greyinnovation.com/greyscan-explosive-detector/

The GreyScan technology is focused on identifying trace amounts of inorganic explosives commonly found in homemade explosives. The capillary electrophoresis process used in GreyScan detects trace levels of inorganic explosives within 60 seconds. The accurate, consistent and rapid identification of these explosives is a first for any explosive trace detection system worldwide.
The GreyScan technology was developed by the Australian Centre for Research on Separation Science (ACROSS) based at the University of Tasmania. Grey Innovation was the industry partner in the initial development of the proof-of-concept demonstrator. This demonstrator system underwent extensive bench and field

testing and proved to consistently and accurately detect inorganics from common background ions, from a solid surface in 60 seconds.
Samples for analysis by the system are collected from a target surface using a swab. The swab is placed into the introduction port, from which the device then extracts the sample. The extracted fluid is then analysed for target inorganic explosive anions utilising capillary electrophoresis.
In 2014, the University of Tasmania (UTAS) licensed its novel explosive detection technology to Grey Innovation. Grey Innovation is advancing the further development and commercialisation of the next generation of this explosive detection technology through GreyScan Pty Ltd.
GreyScan units will be trialled in a real threat environment where the ability to detect trace levels of inorganic explosives in less than a minute could prove life-saving.

EXPRAY Explosives Detection Identification Field Test Kit

Source: http://www.meditests.com/exexdetfielt.html

Product description:

- For both law enforcement and investigative personnel, Expray is a proven tool for increasing the accuracy, efficiency and number of interdictions. For forensic and environmental laboratories, it has proven to reduce the number of samples submitted for testing, saving both time and money.
- Expray is a unique, aerosol-based field test kit for the detection and identification of Group A explosives (e.g. TNT, TNB, etc.), Group B explosives (e.g. Semtex H, RDX, C4, etc.) and compounds containing inorganic nitrates that are used in improvised explosives (e.g. ANFO).
- Expray is commonly used as a pre-blast, analytical tool, post-blast investigative tool, screen against potential terrorist elements and as a technical evaluation test in soil remediation on hazardous material "clean-up" sites.
- When used as a post-blast investigative tool, the product is field proven to speed up crucial investigations.
- The level of sensitivity (20 nanograms) surpasses that of other currently available products. The testing process is fast and efficient. No glass ampoules, spatulas or waiting period required. Results appear in seconds. No additional tools or equipment required. The identification/detection process requires no special training and testing can be performed "on the spot".

Expray is sold in a kit configuration, which provides all three aerosol sprays, collection papers, and an RDX-impregnated verification pad (verification pad is useful for ensuring that the spray can still contains active reagents and for demonstrating how a positive reaction will appear) in a convenient plastic carry case. Expray kits are also available in mini-size (50 tests).

Medimpex United is proud to say that Expray provides a low "per test" cost and poses no risk to you or the environment.

"E": Expray-1 for Group A Expray-1 is used to search for GROUP A type explosives which include TNT, Tetryl, TNB, DNT, picric acid and its salts. To use, wipe suspected surface with special collector test paper. Spray with Expray-1. If a dark brown-violet color appears, this indicates the presence of TNT; An orange color indicates the presence of Tetryl and other GROUP A explosives.

"X": Expray-2 for Group B Expray-2 is used to search for GROUP B type explosives which include Dynamite, Nitroglycerine, RDX, PETN, SEMTEX, Nitrocellulose and smokeless

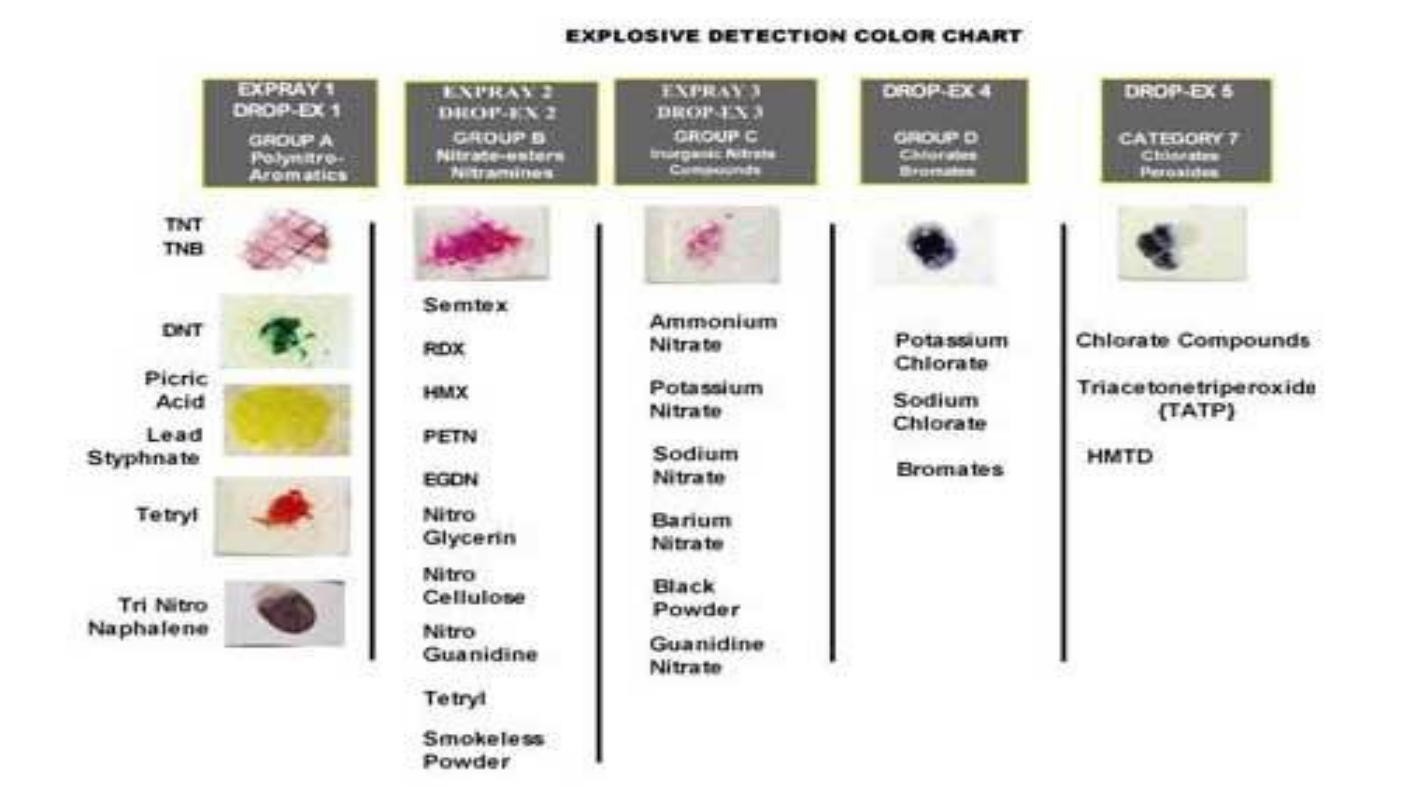
powder. If after spraying Expray-1 there is no color change, spray Expray-2. The almost immediate appearance of a pink color change indicates the presence of GROUP B explosives. Most plastic types of explosives belong to this group, including C-4 and Semtex.

"I": Expray-3 for Nitrates Expray-3 is used to search for nitrate-based explosives which includes ANFO (ammonium nitrate-fuel oil), commercial and improvised explosives based on inorganic nitrates, black powder, flash powder, gun powder, potassium chlorate and nitrate, sulfur (powder), and ammonium nitrate (both fertilizer and aluminum). If there is still no reaction after using the Expray cans 1 and 2, but presence of explosives is still suspected, spray the same paper with Expray-3. A pink reaction indicates the presence of nitrates, which could be part of an improvised explosive.

Test Instructions* (Expray is a chemically cumulative testing procedure):

- First wipe the surface with the collection paper (Model #0530). Spray the collection paper with Expray #1 and observe for a dark violet to brown color reaction indicating the presence of Group A explosives.
- Next, spray the same collection paper with Expray #2 and observe for a pink color reaction indicating the presence of Group B explosives.
- Finally, spray the same collection paper with Expray #3 and observe for a crimson pink color reaction indicating the presence of nitrate compounds. It is recommended that all three Expray cans be sprayed during a testing process even if a positive reaction is observed in either step #1 or #2.

* Even if the environmental surface or package being tested is light in color, the collection paper should still be used.



Read Results:

Additional Information:

The kits detect 99% of the explosives on the FBI Threat List and provide "on-the-spot" results by producing a unique color when they come into contact with specific explosive substances.

Commonly used by armed forces in Iraq and Afghanistan, Expray helps detect a wide spectrum of explosives and HME precursors quickly and effectively.

On-site Rapid Detection of Trace Non-volatile Inorganic Explosives by Stand-alone Ion Mobility Spectrometry via Acid-enhanced Evaporization

By Liying Peng, Lei Hua, Weiguo Wang, Qinghua Zhou and Haiyang Li

Scientific Reports ***4****, Article number: 6631 (2014)*
Source: http://www.nature.com/articles/srep06631

New techniques for the field detection of inorganic improvised explosive devices (IEDs) are urgently developed. Although ion mobility spectrometry (IMS) has been proved to be the most effective method for screening organic explosives, it still faces a major challenge to detect inorganic explosives owing to their low volatilities. Herein, we proposed a strategy for detecting trace inorganic explosives by thermal desorption ion mobility spectrometry (TD-IMS) with sample-to-sample analysis time less than 5 s based on in-situ acidification on the sampling swabs. The responses for typical oxidizers in inorganic explosives, such as KNO_3, $KClO_3$ and $KClO_4$ were at least enhanced by a factor of 3000 and their limits of detection were found to be subnanogram. The common organic explosives and their mixtures with inorganic oxidizers were detected, indicating that the acidification process did not affect the detection of organic explosives. Moreover, the typical inorganic explosives such as black powders, firecrackers and match head could be sensitively detected as well. These results demonstrated that this method could be easily employed in the current deployed IMS for on-site sensitive detection of either inorganic explosives or organic ones.

Introduction

The instrumental methods such as X-rays, neutron analysis, nuclear quadrupole resonance, and colorimetric detection are always adopted for the bulk detection of **organic** and **inorganic explosives**, while the thermal desorption ion mobility spectrometry (TD-IMS) is proven to be a practical technique for trace detection (from ng to pg) of organic explosives such as 2,4,6-trinitrotoluene (TNT) and cyclo-1,3,5-trimethylene-2,4,6-trinitramine (RDX) *et al*. IMS is a gas-phase ion separation and detection technique in a uniform electric field based on the mobility difference of gaseous ions. More than 20,000 stand-alone IMS have been deployed at airports and subway stations worldwide for security applications, due to the advantages of fast speed, low cost, analytical flexibility, portability and commercial availability. However, it still remains a great challenge for TD-IMS to detect trace inorganic explosives except for ammonium nitrate-fuel oil (ANFO) and sulphur (S) in black powder, owing to their ultra-low vapour pressure even at the typical maximum desorber temperature (≤280°C).

Inorganic explosives generally consist of an inorganic oxidizer such as potassium nitrate (KNO_3), potassium chlorate ($KClO_3$), or potassium perchlorate ($KClO_4$) and a fuel such as carbon source, sulphur (S), sugar or powdered metals. Inorganic explosives are extensively used in terrorist attacks owing to the readily available, low cost and legally purchased components. Ion chromatography (IC), capillary electrophoresis (CE), electrospray ionization mass spectrometry (ESI-MS) and electrospray ionization ion mobility spectrometry (ESI-IMS) have been performed to identify their characteristic ions, such as nitrate (NO_3^-), chlorate (ClO_3^-), sulphate (SO_4^{2-}) and perchlorate (ClO_4^-) etc. contained within inorganic explosives. However, the field-deployment of these techniques is hampered by the tedious and time-consuming procedures for handling the aqueous samples. Additionally, the relatively long analysis time (>5 minutes) of IC and CE, and the relatively large bulk, high expensive cost of mass spectrometer make them not suitable for on-site screening as well.

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

Bullet, Blast Protective Tech Integrated into Public Space Seating

Source: http://www.hstoday.us/single-article/bullet-blast-protective-tech-integrated-into-public-space-seating/0616237f04c1bd60865f701ecbfab29a.html

A new line of bullet- and blast-resistant furniture designed to shield travelers in the event of an act of violence in public spaces was announced by Arconas, a designer and manufacturer of furniture for airports and public spaces, which has teamed with Amulet Ballistic to seamlessly integrate Amulet's bullet-absorbing technology into airport seating.

The "invisible" barrier technology is integrated during the manufacturing process and designed to protect people from gunfire or explosive devices without affecting the design, appearance or comfort of the airport seating.

"Unfortunately, acts of violence in the public space have become an all too common occurrence around the globe," said Jeffrey Isquith, president and CEO of Arizona-based Amulet Ballistic Barriers. "Our number one goal is to save lives, and this technology adds a critical layer of protection for the public. Amulet is a 21st Century solution to saving lives and reducing injuries to innocent people."

"I am also very proud of the exceptional level of collaboration demonstrated between the US-based Amulet technology team and our Canadian alliance partner Arconas. The desire to protect life in the public space is truly universal," Isquith said.

"As the leading designer and manufacturer of furniture for airports and public spaces, Arconas is constantly striving to develop design innovations that are human-focused and meet changing market demands," said Dan Nussbaum, Arconas president. "There is demand for this technology, not only in airports, but also in public spaces throughout the world."

New Bomb Disposal Robot to Neutralize Car Bombs

Source: http://i-hls.com/2017/01/new-bomb-disposal-robot-neutralize-car-bombs/

A new bomb disposal and tactical robot was launched recently. The **Avenger Remotely Operated Vehicle (ROV)** robot has been engineered to provide police and military response teams with enhanced capabilities to manage ongoing and emerging threats posed by terrorists, particularly in urban environments where car bombs (Vehicle-Borne Improvised Explosive Devices, VBIEDS) are of concern.

The robot was launched at the 2017 SHOT (Shooting, Hunting, Outdoor Trade) Show. Designed and manufactured by ICP NewTech, the robot is a mid-sized ROV with most of the operational capabilities typically found only in much larger and more expensive robots, according to safariland.com.

The Avenger's highly dextrous arm and claw can easily reach inside, above and below cars, pick-up trucks and delivery vans, to remotely investigate suspicious devices, such as Improvised Explosive Devices (IED).

The system includes an on-board computer that fuses data from multiple Chemical, Biological, Radiological, Nuclear & Explosive (CBRNE) sensors and cameras, and relays it to a command post. This integrated sensor suite provides a mission-critical tool for managing CBRNE and Hazmat threats, such as a terrorist's 'dirty bomb', and mitigating risks to the surrounding public. The numerous sensor ports are compatible with many specialized sensors that bomb squads already have, so they can make use of their existing equipment and attach new tools in the future.

In announcing this new urban response tool, The Safariland Group President Scott O'Brien said "the safety of first responders, elite military EOD teams and local citizens is of utmost importance to Safariland and this new system will prove to be an integral part of securing densely populated areas across the United States and the international community."

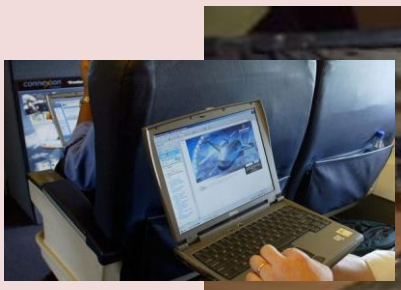
Eamon Jackson, CEO of ICP NewTech, commented, "We listened very carefully to the needs of end users and recognized the operational challenges they're facing now and in the foreseeable future. It became clear that response teams needed a robotic platform that could be easily transported through congested urban centers, which meant keeping the robot at a smaller scale. We then applied our engineering expertise to develop a system that could attack a range of VBIED-type threats, overcome obstacles, and give users the freedom to deploy and leverage many of their existing sensors and EOD tools."

The Safariland Group is a leading global provider of a broad range of safety and survivability products designed for the public safety, military, professional and outdoor markets.

What prompted the US and UK electronics bans?

Source: http://gantdaily.com/2017/03/22/what-prompted-the-us-and-uk-electronics-bans/

Mar 22 – **The US and British electronics bans announced Tuesday on flights from certain airports in the Middle East and Africa seem to have come out of the blue, with no specific event prompting the sudden change.**



So what's behind these coordinated bans?

One factor, a US official told CNN, was recent intelligence that the terrorist group al Qaeda in the Arabian Peninsula (AQAP) was perfecting techniques for hiding explosives in batteries and battery compartments of laptops and other commercial electronic devices. The intelligence was obtained in recent weeks and months, according to the official.

More generally, US officials have said intelligence shows that terrorist groups are still looking to target commercial flights by smuggling explosive devices in various items.

One US official said that some information from a recent US Special Forces raid on an AQAP compound in Yemen in January contributed to the ongoing concern.

A US official tells CNN they are seeing a growing capability to target aviation from al Qaeda affiliates in Yemen, Syria, Somalia, as well as ISIS. It's not fully clear to what extent

these groups are sharing specific information but "there is a growing pool of intelligence all pointing to threats to aviation" the official said.
ISIS is believed to be not as advanced in perfecting techniques for hiding explosives in electronics as AQAP, the official added.
If that were to change it could significantly increase the threat because of ISIS's still significant resources, global reach and remaining large cohort of Western recruits.
While the CIA believes AQAP and ISIS sometimes tactically cooperate in Yemen, the senior leaderships of the two groups are at loggerheads, making technology transfers between them unlikely.

Drumbeat of al Qaeda plots

AQAP has for years been working to perfect techniques to get bombs on planes.
Between 2009 and 2012, AQAP master bombmaker Ibrahim al Asiri orchestrated three terrorist plots to bring down American aviation.
In 2009, al Asiri fitted out a Nigerian AQAP recruit with an explosive underwear device containing PETN, a white powdery explosive that basic X-ray systems have difficulty detecting.
But the attempted attack failed to bring down the passenger jet, landing in Detroit on Christmas Day. Al Asiri used the same explosive compound concealed in printer cartridges in a plot to blow up cargo jets headed to the United States just before the 2010 mid-term elections.
And according to Western counter-terrorism officials, he used ETN, a closely related chemical compound, in a third plot targeting US aviation with a more advanced form of the underwear device. The plot was thwarted by a Saudi-British spy in 2012, who was recruited for the suicide attack and who retrieved the device.
The same year, Western intelligence agencies learned that AQAP was pioneering techniques to surgically implant devices inside potential bombers, according to British intelligence documents cited by the New York Times.
"(The Transportation Security Administration) took this threat seriously, especially because in 2009 al-Asiri had implanted a bomb in the rectum of his brother in an attack against then-Saudi Arabian counterterrorism chief Prince Muhammad bin Nayef," according to research published by the aviation security experts Robert Liscouski and William McGann in CTC Sentinel, the flagship publication of the Combating Terrorism Center at West Point.
They pointed out that in 2014 it emerged that al-Asiri and his team of bombmakers had "continued to do research and development on explosive devices, including shoe bombs." In the summer of 2015, al Asiri declared hitting the United States remained a priority.
In an interview with CTC Sentinel last September then CIA director John Brennan stated al Asiri was still at large and had become "very sophisticated in terms of his concealment capabilities."
In early to mid 2014, US intelligence agencies learned that the so-called Khorasan group — a network of al Qaeda veteran operatives in Syria — was developing plans to conceal bombs in personal electronics and smuggle them onto Western passenger aircraft.
This led to the Transportation Security Administration requiring tighter security measures at certain overseas airports with flights to the United States. As part of these measures, spot checks were introduced to make sure appliances taken on board could power up safely. That same year, US intelligence agencies came to the belief that AQAP was transferring bomb-making know-how to the Khorasan Group.
In the past couple of years most of AQAP's energies appear to have been focused on taking advantage of the turmoil in Yemen to build up its position rather than plotting international terrorism. This expansion strategy has provided the group with more resources than ever before, including up to $100 million seized from the al-Mukalla branch of the Yemeni central bank, creating concern the group could be providing extra funding to its bombmakers.
One former senior Western counter-terrorism official told CNN there is worry the recent escalation in US counter-terrorism operations in Yemen, including January's Navy Seal raid, might lead to the group retaliating.

Exploding Laptops

The February 2016 a bomb attack on a Somali airliner leaving Mogadishu made clear terrorist groups' continued determination to bring down passenger jets.

The al Qaeda affiliated Somali terrorist group al Shabaab smuggled a laptop bomb onto a plane by recruiting two airport workers who handed the device to one of the group's operatives. The device was "sophisticated" and passed through an X-ray machine at the airport, a source close to the investigation told CNN.
The suicide bomber was blown out of the aircraft when the laptop bomb detonated and the plane was able to make an emergency landing. Only the fact that the aircraft had not reached cruising altitude prevented a disaster.

Questions unanswered
It is still not fully clear why the new restrictions are being implemented now, given the Somali attack was more than a year ago and the longstanding intelligence indicating al Qaeda groups have been working to conceal explosives in electronics for years.
Moreover, explosive detection experts believe it is much less likely that a laptop bomb would get through screening at international aviation hubs, like Dubai and Abu Dhabi, which operate state of the art detection systems and layered security.
Writing in CTC Sentinel, Liscouski and McGann said that some media reports had falsely created the impression that al Qaeda was developing undetectable explosive devices. They stressed that the latest explosive trace detection technology when used in combination with the latest X-ray technologies were excellent at detecting the types of explosives being developed by AQAP, even if these explosives were concealed in the electronics of a laptop. Such systems are now in place at major modern airports like Dubai and Abu Dhabi.
Another aspect that is puzzling counterterrorism analysts is why the ban on laptops applies only to cabin luggage when the same explosive detection technology is used for both hand and checked baggage.
This might suggest Western intelligence is concerned about a threat stream involving manually detonated devices, like in the Christmas 2009 underwear bombing attempt.
Aviation security experts tell CNN there is particular concern over carry-on explosives because suicide bombers have sought to locate themselves to do maximum damage to the fuselage, increasing the chances of a catastrophe.
In the attempt to blow up the Somali airliner, the bomber knew precisely were to sit to maximize damage, a source close to the investigation told CNN. When it comes to hold luggage, terrorists have no control over the placement of their baggage creating the possibility a bomb hidden inside would be some distance from the fuselage and be insulated by other luggage, the aviation security sources told CNN.
Another reason why terrorists might want to bring explosive devices into the cabin is that their plans might require them to assemble them mid flight from multiple components possibly carried by multiple passengers. A former senior US official told CNN this has also been a longstanding concern of US security agencies.
Timer triggered devices are however well within the skill set of a group like AQAP.
US officials believe a timer was used to trigger the bomb which brought down a Russian passenger jet leaving Sharm el Sheikh, Egypt in October 2015. Western intelligence services believe ISIS's Sinai affiliate carried out that attack by recruiting an airport insider who placed the device inside the aircraft.

The Silicon Valley Community Foundation Must Stop Funding Islamist Hate Groups

By Gregg Roman, Director MEForum
Source: http://www.meforum.org/6558/the-silicon-valley-community-foundation-must-stop

Mar 01 – The Middle East Forum asks the public to sign a petition urging the Silicon Valley Community Foundation (SVCF) to stop all funding of extremist groups, including the Council on American-Islamic Relations (CAIR) and Islamic Relief.

The Forum's Islamist Watch project has uncovered eight donations from SVCF to these groups totaling $330,524. CAIR received five donations totaling $132,933, while Islamic Relief received three donations totaling $197,591.
CAIR and Islamic Relief regularly give platforms to speakers who incite hatred against women, Jews, Christians, and the LGBTQ community.
CAIR was named as an unindicted co-conspirator during the 2008 Holy Land Foundation terrorism financing trial. Since then, the Justice Department has banned outreach with CAIR. In 2014, the United Arab Emirates, a devout Muslim country, designated CAIR a terrorist organization. The Anti-Defamation League accuses CAIR of promoting anti-Jewish sentiment.
Islamic Relief is one of the largest Islamic charities in America and the Western world, reporting a U.S. income of about $110 million in 2014. However, it is a designated terrorist entity both in Israel and the UAE. Banks such as UBS and HSBC have closed Islamic Relief bank accounts over concerns about terrorism financing.
Click here to read the details of Islamic Relief and CAIR's promotion of hate preachers, as well as to sign the petition. Click here to send an email to the SVCF.
"The SVCF is the country's leading community foundation, with more than $8 billion in assets," said Forum director Gregg Roman. "It enjoys close partnerships with dozens of prominent tech companies. We call on the SVCF to stop funding organizations that promote extremism. When the SVCF funds Islamist groups, it is betraying those moderate Muslims working to free their faith from the grip of extremists, who have learned to shroud their work under the guise of charitable endeavor."

New malware attack shutters London hospital

Source: https://www.scmagazineuk.com/new-malware-attack-shutters-london-hospital/article/641717/

Mar 03 – A previously unseen malware is being blamed for an attack on a London hospital that forced the facility to shut down a segment of its systems for a few days as a precautionary measure.
Barts Health NHS Trust, a conglomerate of five hospitals in London employing a staff of 15,000, was hit in January by the malware attack, which managed to circumvent the facility's anti-virus software, according to a report on ZDNet.

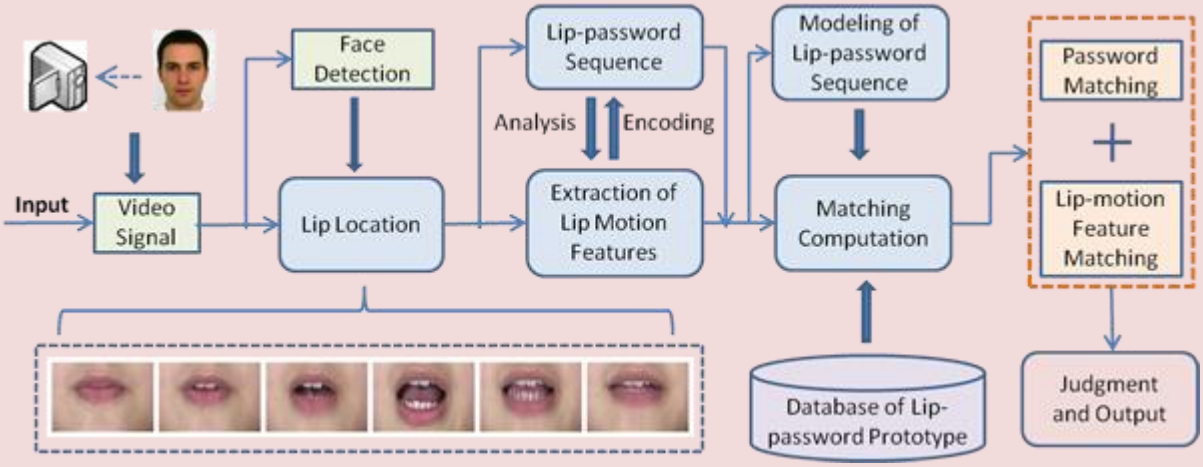
Although administrators at Barts Health said patient data was not accessed, the facility's pathology system was offline for a few days.
While previous reports said it was unclear how the Trojan had gotten into the hospital's network, an update from 1 March board minutes revealed that four of the hospital group's five facilities were affected. While the

hospital's AV software was up to date, the incident involved "a new virus not seen previously".
The investigation continues.
Tony Rowan, chief security consultant at SentinelOne told *SC Media UK*: "Truly "new" malware is relatively rare but, on a daily basis, we see hundreds of thousands of modified or obfuscated malware samples. The clear objective of this process is to bypass the legacy AV tools that are primarily based on detecting known-bad malware based on their signatures. Yet again, we see from this incident at Barts that the signature based approach is very limited and needs replacing with methods capable of detecting the attributes and behaviours of malware, rather than depending entirely on "knowing" the sample from other affected sites."

"Lip password" uses a person's lip motions to create a password

Source: http://www.homelandsecuritynewswire.com/dr20170314-lip-password-uses-a-person-s-lip-motions-to-create-a-password

Mar 14 – The use of biometric data such as fingerprints to unlock mobile devices and verify identity at immigration and customs counters are used around the world. Despite its wide application, one cannot change the scan of their fingerprint. Once the scan is stolen or hacked, the owner cannot change his/her fingerprints and has to look for another identity security system. HKBU researcher has invented a new technology called "lip motion password" (lip password) which utilizes a person's lip motions to create a password. This system verifies a person's identity by simultaneously matching the password content with the underlying behavioral characteristics of lip movement. Nobody can mimic a user's lip movement when uttering the password which can be changed at any time. This novel technology, the first in the world and has been granted a US patent in 2015, is expected to be used in financial transaction authentication.



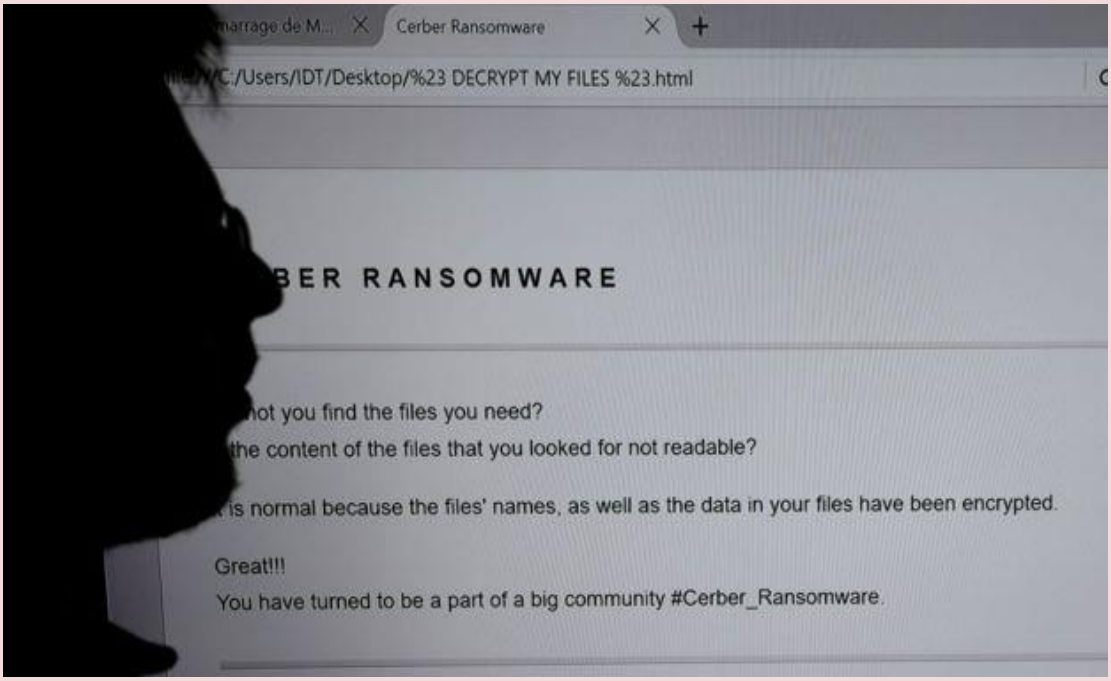
HKBU says that HKBU's Department of Computer Science Professor Cheung Yiu-ming in charge of the research said the new technique has a number of advantages over conventional security access control methods: 1) The dynamic characteristics of lip motions are resistant to mimicry, so a lip password can be used singly for speaker verification, as it is able to detect and reject a wrong password uttered by the user or the correct password spoken by an imposter; 2) Verification based on a combination of lip motions and password content ensures that access control is doubly secure; 3) Compared with traditional voice-based authentication, the acquisition and analysis of lip movements is less susceptible to background noise and distance, moreover, it can even be used by a speech-impaired person; 4) A user can reset the lip password in a timely manner to strengthen security; 5) There is no language boundary, in other words, a person from any country can use this lip password verification system.
Professor Cheung said: "The same password spoken by two persons is different and a learning system can distinguish them." The study adopted a computational learning model which extracts the visual features of lip shape, texture and movement to characterize lip

sequence. Samples of lip sequence are collected and analyzed to train the models and determine the threshold of accepting and rejecting a spoken password.
The potential application of this new patented technology includes, but is not limited to, financial transaction authentication including electronic payment using mobile devices, transactions at ATM machines, and credit card user passwords. It can also be applied to enhance the security access control system currently used in entrances of companies or private premises.
In addition, lip password can be used together with other biometrics to enhance the security level of systems. For instance, lip password can be combined with face recognition, whereby the problem of spoofing face recognition with 3D masks in personal identity verification would be solved.

Cyber security: Experts warn on rise of hacker ransoms

Source: http://www.bbc.com/news/uk-39260174

Mar 15 – **Smartphones, watches, televisions and fitness trackers could be used to hold people to ransom over personal data, cyber security experts have warned.**



Ransomware, which makes devices unusable until their owners pay to unlock them, has become increasingly prevalent in the past year, they say.
Devices holding photos, emails and fitness information could be targeted.
The risk to business is "significant and growing", the National Crime Agency and National Cyber Security Centre say.
The joint report from the NCA and the NCSC says cyber crime is becoming more aggressive.
More devices connecting to the internet meant opportunities for criminals, the report said.
Any devices containing personal data such as photos, that people consider sufficiently valuable to pay for, are likely to be targeted by criminals.
Such devices often have limited security built in.
In their report, aimed at businesses, the agencies say: "This data may not be inherently valuable, and might not be sold on criminal forums but the device and data will be sufficiently valuable to the victim that they will be willing to pay for it.
"Ransomware on connected watches, fitness trackers and TVs will present a challenge to manufacturers, and it is not yet known whether customer support will extend to assisting with unlocking devices and providing advice on whether to pay a ransom."
The report also raises concerns about the ability of the most sophisticated criminal gangs to use the same high-tech tools as

states to target financial institutions.
Others, it adds, can download more basic software to carry out attacks on smaller businesses and the general public which require very little technical ability.

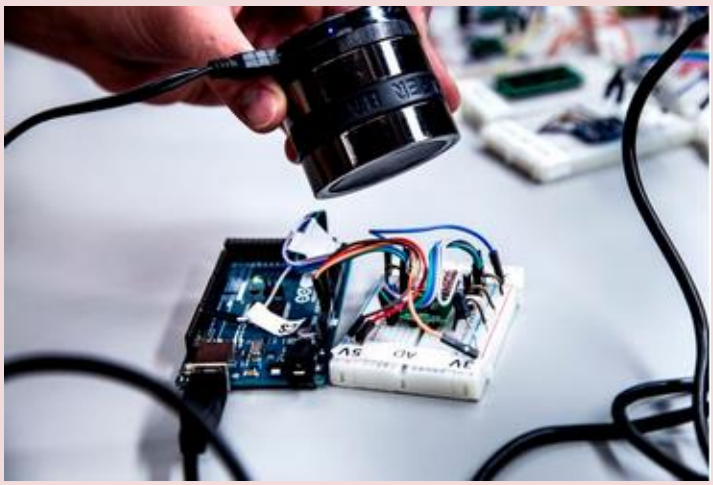
What is the scale of the problem?
As many as 21 billion devices used by businesses and consumers around the world are forecast to be connected to the internet by 2020.
Ciaran Martin, chief executive of the NCSC, said cyber attacks would continue to evolve and the public and private sectors must continue to work at pace to reduce the threat to critical services and deter would-be attackers.
The report also says there is no clear understanding of the true scale and cost of current cyber attacks to the UK, as they believe they are under-reported.
In three months after the NCSC was created, there were 188 "high-level" attacks as well as "countless" lower-level incidents, it says.
Donald Toon, director for economic and cyber crime at the NCA, told the BBC devices that helped businesses control operations remotely had an online capability built into them.
"They're mass-produced and the security may not be particularly good," he said. "Businesses often don't change the basic security software that's in there, or change the passwords."

The report will be published on Tuesday as the NCSC hosts a major conference, CyberUK, in Liverpool.

These researchers can hack your phone with sound waves

By Laura Hautala
Source: https://www.cnet.com/news/hack-fitbit-samsung-sound-waves-researchers/

Mar 14 – **Did you hear that? Your phone could be hacked with sound waves.**
Researchers at the University of Michigan released a paper Tuesday (PDF) explaining how audio tones can send false readings to devices through the devices' accelerometers. Accelerometers are those sensors in phones, fitness trackers, and tons of other tech toys that tell our devices where they are in space. Any device with an accelerometer could potentially be vulnerable to this kind of hacking attack.



University of Michigan researcher Timothy Trippel said our devices rely on their sensors just like we rely on our ears, eyes and noses. Sending confusing information to those sensors can wreak havoc.

A University of Michigan researcher points a speaker at an accelerometer, which can send false readings to a phone, fitness tracker or other device.

"If autonomous systems can't trust their senses, then the security and reliability of those systems will fail," Trippel said in a statement.
Sound wave attacks aren't new -- researchers at the Korea Advanced Institute of Science and Technology have crashed quadcopter drones with a similar approach, for example (here's a video). But they show how hard it is to totally secure an internet-connected device, whether it's your toy drone, your fitness tracker, or your pacemaker.
The results of the hacks the Michigan researchers demonstrated are minor. They caused a Samsung Galaxy S5 to spell out the word "WALNUT" in a graph of the accelerometer's readings (which the user wouldn't likely see), and they tricked a Fitbit fitness tracker into recording steps that no one was taking.
But the fact is, something as simple as sound waves can make your devices do something you didn't ask them to do. You probably don't like the sound of that.

Accelerometers are vulnerable to the attack because they vibrate. The attack works by hitting the accelerometer with a sound wave that matches the frequency of that vibration. A hacker could use the attack to destroy the accelerometer, but the University of Michigan researchers decided to do one better -- they made phones and Fitbits behave strangely.

They can do this because accelerometers send signals to the devices they live inside, telling them to record information or take action.

Samsung didn't immediately respond to a request for comment. Fitbit said in an emailed statement that the attack doesn't put user information at risk.

"What is being described is simply a way to game the system," the statement reads. "We continue to explore solutions that help mitigate the potential for this type of behavior."

The researchers suggest some low-frills ways to protect accelerometers from Sonic the Hacker, including putting some sound-dampening foam around the sensors.

Laura Hautala *writes about cybersecurity and privacy. She joined CNET News from the San Francisco Daily Journal, where she covered securities fraud, corporate misdeeds, shrinking unions and people who sue their bosses. She's also written for the Los Angeles Times, Politico and the East Bay Express, among others. Laura is a native of Tacoma, Wash. and holds degrees from Saint Mary's College of California and UC Berkeley's Graduate School of Journalism. She's based in San Francisco.*

U.K. industry warned that cybercriminals are imitating nation state attacks

Source: http://www.homelandsecuritynewswire.com/dr20170315-u-k-industry-warned-that-cybercriminals-are-imitating-nation-state-attacks

Mar 15 – **The annual assessment of the biggest cyberthreats to U.K. businesses has been published the other day, after being produced jointly for the first time by the National Crime Agency (NCA), National Cyber Security Center (NCSC). and industry partners from multiple sectors.**

The assessment — the most detailed of its kind to date — emphasizes the need for increased collaboration among industry, government, and law enforcement in the face of a growing and fast-changing threat.

The NCA notes that the report discusses the trend of criminals imitating the way suspected nation state actors attack organizations such as financial institutions, and the risk posed by the ever-increasing number of connected devices, many of which are not always made secure by manufacturers or users.

It also highlights increased levels of aggressive and confrontational cybercrime, particularly through Distributed Denial of Service (DDoS) attacks combined with extortion, and ransomware, which encrypts victim computers and demands a ransom in return for restoring control to the user.

Particularly through the contribution of the private sectors companies forming the Strategic Cyber Industry Group, the report notes the cyber security challenges faced by businesses, and urges them to report all cybercrime to ensure the United Kingdom has an accurate intelligence picture.

The assessment additionally highlights the resources available to companies of all sizes, particularly the large firms which often present the most attractive targets for attackers.

The report was presented at the NCSC's Cyber U.K. Conference in Liverpool, yesterday (14 March).

Donald Toon, Director for economic and cybercrime at the National Crime Agency, said:

"We have worked with the NCSC and valued private sector partners to produce this assessment, setting out an up to date picture of threats to business including ransomware, DDoS and evolving financial Trojans. These threats demonstrate the need for a collaborative response across industry, law enforcement and government, with the ultimate aim of protecting customers and the U.K. economy.

"Businesses reporting cybercrime is essential if we are to fully understand the threat, and take the most effective action against it. And while 100 percent protection doesn't exist, making cyber security an

organizational priority and ensuring up to date processes and technology can protect against the vast majority of attacks.

"The NCA and its partners continue to have significant success against cybercrime, through identifying and arresting criminals at home and abroad, working to deter young people from becoming involved in criminality, and disrupting the ways in which criminals make and launder their money."

Ciaran Martin, CEO of the National Cyber Security Center, said:

"The National Cyber Security Centre exists to benefit the whole country, so we are delighted to be here in Liverpool - the UK's first 'Smart City' — to share knowledge and expertise with many of our essential partners.

"As the national technical authority for cyber security in the United Kingdom, the NCSC agenda is unashamedly ambitious; we want to be a world leader in cyber security.

"Cyberattacks will continue to evolve, which is why the country must work together at pace to deliver hard outcomes and ground-breaking innovation to reduce the cyber threat to critical services and deter would-be attackers.

"No single organization can defend against the threat on its own and it is vital that we work together to understand the challenges we face. We can only properly protect U.K. cyberspace by working with others with the rest of government, with law enforcement, the Armed Forces, our international allies and, crucially, with business and wider society."

Don Smith, technology director, SecureWorks and Strategic Cyber Industry Group representative, said:

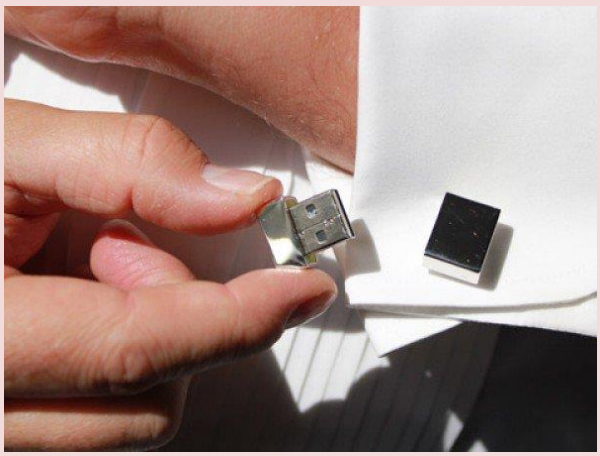
"The development of technology throughout history has given smart criminals new ways to get what they want: email spawned the development of phishing and spam; online banking led to the creation of viruses that target bank accounts; and the Internet of Things will doubtless bring opportunities for new methods of attack. Many businesses face understandable difficulty in reporting cybercrime incidents, but knowing that revealing such information might prevent further harm to their business is essential. This assessment proves that collaboration is key to protecting our assets and targeting cyber criminals."

Cyber-jihadi who stored his secrets on dozens of James Bond-style USB cufflinks faces jail after admitting being an ISIS terrorist

Source: http://www.dailymail.co.uk/news/article-4331030/Extremist-terror-files-USB-disguised-cufflinks.html

Mar 20 – **An extremist who stored his secrets on USB sticks disguised as cufflinks is facing jail after admitting being an ISIS terrorist.**

Samata Ullah, from Cardiff, admitted membership of ISIS and confessed to being involved in terrorist training and preparation of terrorist acts.



Then 34-year-old was a key member of a group calling itself the 'Cyber Caliphate Army' and gave other members of ISIS advice on how to communicate using sophisticated encryption techniques.

When his home was raided last October, Ullah was found with 30 metal cufflinks from a batch he had bought on a Chinese website, using the name Cardiff Trader.

One of them was loaded with an open-source computer operating system known as Linux, which is popular with computer programmers.

Police also discovered that Ullah had a PDF version of a 500-page book titled 'Guided Missile Fundamentals' and another called 'Advances in Missile Guidance, Control, and Estimation.'

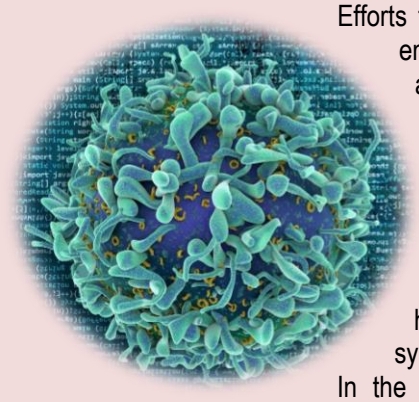
Ullah, a British national of Bangladeshi origin, had recently resigned from his job as an insurance worker.
He had also been making instructional videos in which he wore gloves and used a voice modification system to hide his Welsh accent.
At an Old Bailey hearing, Ullah pleaded guilty to five terror offences including possession of an article for terrorist purposes on or before September 22 last year.
It can be disclosed that Samata Ullah, 34, from Cardiff, South Wales, was the subject of an international manhunt by British and American security services.
Ullah had a PDF version of a 500-page book titled 'Guided Missile Fundamentals' and another called 'Advances in Missile Guidance, Control, and Estimation.'
The first was a manual used by the US to train rocket engineers until the 1970s and the second explained the mathematical algorithms behind missile guidance systems used to tack and intercept a moving target.
In one message, Ullah wrote: 'Ask the brothers in Turkey and Dawlah [Islamic State] whether the book would be useful for them. I have bought a copy and I want to scan all 500 pages and send it to them so that they can start learning the basics of rocket design.
'It can also be translated into Arabic to form the basis of our future weapons programs.'
In another message, he wrote: 'We should also [try] recruiting people from Turkish and Pakistani defence companies as Turkey and Pakistan already have the technology needed to destory or jam drones and planes - but that takes stealth as you don't want to approach them saying, 'hi, we are ISIS, do you want to work for us?"

What Biosecurity and Cybersecurity Research Have in Common

By Kendall Hoyt

Source:http://www.slate.com/articles/technology/future_tense/2017/03/what_biosecurity_and_cybersecurity_research_have_in_common.html

Mar 17 – Biosecurity and cybersecurity research share an unusual predicament: Efforts to predict and defend against emerging threats often expose and create vulnerabilities. For example, scientists must first learn how to isolate and grow a pathogen before they can develop a new vaccine. Similarly, researchers must first learn how to break into a computer system in order to defend it.



In the wrong hands, both types of knowledge can be used to develop a weapon instead of a vaccine or a patch. The genetic tools and exploit software that enable these activities are becoming easier to use and to acquire, prompting security experts to ask one question with growing urgency: How can we protect against misuse without limiting discovery and innovation?
Both fields have grappled with this dual-use dilemma independently for decades. In 2005, when scientists reconstructed the 1918 flu virus that killed 50 million people worldwide, did they advance the science of prevention, or did they introduce new risks? When scientists test computer systems for vulnerabilities, do they promote legitimate software development, debugging, and security auditing? Or do they enable malicious computation as well?
Government efforts to control this type of "dual-use knowledge" date back to the Cold War (and earlier) with mixed results. By working together, cybersecurity and biosecurity experts have an opportunity to identify new approaches and to avoid repeating past mistakes.
Government regulators do not want to squelch innovation, but they work with blunt instruments. To date, they have focused on the tangible products of sensitive research such as pathogens, publications, and malicious code. Regulations that rely on static lists struggle to keep pace with fields as fast-moving as bio- and cybersecurity. Worse, they can damage research productivity without offering meaningful security.
For example, in 1997, "select agent" regulations—so called because they focus on creating restrictions around particular pathogens, like anthrax and plague—were put in place after a white supremacist

fraudulently obtained vials of Y. pestis (the bacterium that causes plague) from the American Type Culture Collection. It certainly may seem like a reasonable policy. But many scientists soon stopped working with these pathogens after concluding that the professional risks and regulatory burdens were too cumbersome. As a result, legitimate research suffered.

Meanwhile, a determined bioterrorist can still steal pathogens from labs, isolate them from nature, or synthesize them. Select-agent regulations provide a basis for prosecution if pathogens are obtained illegally, but, as the anthrax letter attacks demonstrated, it is all too easy to evade detection. These kinds of dragnet regulations are unlikely to catch a skilled opponent but certain to hinder legitimate research.

Intellectual property and cybersecurity legislation—namely the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act—has similarly stifled legitimate scientific and commercial activities and delayed defensive applications. In one well-known example, fear of prosecution under DMCA deterred a Princeton graduate student from reporting a problem that he discovered: Unbeknownst to users, Sony BMG music CDs were installing spyware on their laptops. Several weeks elapsed before another researcher (who did not know about the potential legal repercussions under DMCA) reported this problem. Meanwhile, hundreds of thousands of computers continued to run Sony's spyware along with a rootkit that made these systems more vulnerable to other viruses.

International agreements stumble over this duality as well. The Wassenaar Arrangement restricts "intrusion software" exports, which U.S. regulators have defined as software modifications that permit "externally provided instructions" to run. The idea is to prevent companies from exporting surveillance software to authoritarian regimes that could use these tools to abridge civil liberties and abuse human rights. But such a broad definition also prevents the export of legitimate software products that can enhance security, such as debuggers and performance-testing tools.

More recently, biosecurity experts have begun to scrutinize not just pathogens and publications but also the activities and techniques that create them, identifying seven research categories that demand closer scrutiny. These include a subset of experiments that increase pathogens' stability, transmissibility, or host range (the animals that could harbor the disease). This type of research gained notoriety in 2011 when two labs engineered a highly pathogenic form of bird flu to transmit more easily between mammals. These efforts, while still a work in progress, signal a way for regulators to begin to focus less on pathogens and code and more on the risks and intent of research projects themselves.

For all of their similarities, key differences between biosecurity and cybersecurity risks and timelines will dictate varied regulatory strategies. For example, zero-day exploits—that is, holes in a system unknown to the software creator—can be patched in a matter of months, whereas new drugs and vaccines can take decades to develop. Digital vulnerabilities have a shorter half-life than biological threats. Measures to promote disclosures and crowd-sourced problem-solving will therefore have a larger immediate impact on cybersecurity.

On the other hand, reporting "vulnerabilities" in the bio realm poses a greater security risk when countermeasures are not and may never be available. Unless drug and vaccine development times improve dramatically (i.e., from decades to weeks), the rationale for restricting sensitive research is somewhat stronger because the risk can outweigh the benefit.

Moreover, some restrictions are more feasible in the life sciences. Researchers require expensive labs with institutional overhead, federal grants, and a publication stream. As a result, governments, research organizations, and publishers have many opportunities to intervene. For example, after scientists announced the results of the 2011 bird flu experiments, the White House and the National Institutes of Health placed a stop order on existing research until the costs and benefits of these experiments could be more fully evaluated. It is hard to imagine how one might implement a similar measure in the hacker community.

Still, both fields face the same basic problem: There are no true "choke points" in either field. The U.S. government is not the only

source of research funds and, thanks in large part to the internet itself, it is increasingly difficult to restrict sensitive information. As the funding, tools, and skills for security research become globally distributed, dual-use dilemmas will become more pronounced, and the regulatory challenges facing both fields will share more similarities than differences.

Looking ahead, biosecurity and cybersecurity regulations will need to adopt a more liberal governance regime that places less emphasis on static lists of controlled items. This choice acknowledges and even embraces the limits of "hard" rules, such as select agent rules and export control lists. To be sure, regulators should erect high walls around a few narrowly-defined, high-risk activities, such as research that enhances the pathogenicity of viruses. But these boundaries should be drawn with precision and restraint. Otherwise, regulators must prioritize measures that maintain vibrant research communities. These include actions to promote information-sharing and establish responsible norms. These methods must be developed with the scientists themselves and tailored to specific technologies and research methods.

Traditional policy tools—legislation, treaties, federal and international security standards—continue to provide opportunities for softer rule-making and norm development. Increasingly, however, new information-sharing platforms can facilitate concrete agreements that build the norms, standards, trust, and transparency necessary for security research to flourish. Examples include the Global Initiative on Sharing All Influenza Data, which hosts a database to promote genetic data-sharing for flu viruses around the world, and sector-specific Information Sharing and Analysis Organizations, which seek to provide timely information to mitigate cyber vulnerabilities.

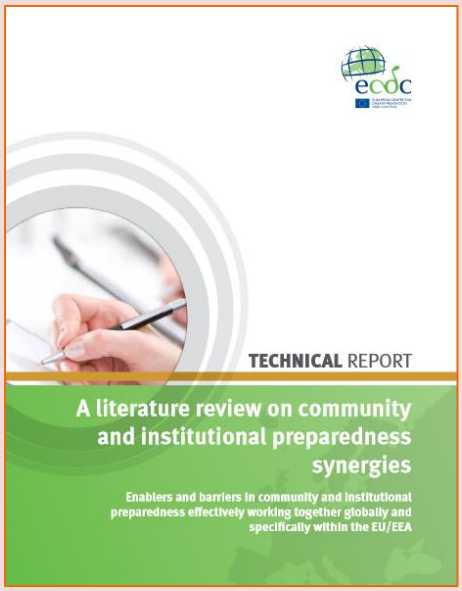
Regulators must work with biosecurity and cybersecurity experts to preserve productive research environments so that they may defend us in return. Our interconnected world of humans and computers provides fertile ground for viruses of both sorts. As these connections grow in density, viruses become even harder to contain. Research communities that can rapidly detect and respond to these emerging threats will be our greatest defense in the future.

Kendall Hoyt *is an assistant professor at the Geisel School of Medicine at Dartmouth and a Cybersecurity Fellow at New America.*

Devastating literature review on community and institutional preparedness synergies

Source:http://ecdc.europa.eu/en/publications/_layouts/forms/Publication_DispForm.aspx?List=4f55ad51-4aed-4d32-b960-af70113dbb90&ID=1645

Feb 23 – The importance of involving communities in all the phases of emergency preparedness is highlighted in the new ECDC literature review on 'Community and institutional preparedness synergies'. This report focuses on the factors that can enable or hinder the work of communities and institutions together to improve emergency preparedness. Recent public health emergencies, most notably Ebola, have shown the potential of community engagement as a resource that can either help or hinder institutional responses to emergencies. It also demonstrated that public health emergencies cannot be handled effectively without taking into consideration the perspectives of the involved communities.



The ECDC report highlights that public health emergency preparedness often focuses on institutional capabilities alone, including provision of material and financial resources, technical expertise and political influence, while overlooking community capabilities. However, the success of institutional preparedness plans depends upon acceptance by the public to ensure that the execution of plans is complete and successful at community-level.

The report identifies a series of factors that can act as enablers and barriers of community and institutional synergies in emergency preparedness. It concludes with a series of key messages on effective practices to facilitate community engagement. For instance, in emergency preparedness, there is often a one-way communication system, from institutions to communities; communication should be two-way, with institutions listening to and acknowledging the needs and capacities of communities. The report also suggests that further research is needed in community and institution synergies in emergency preparedness focused on the 'response' and 'recovery' phases, as well as on the synergies in different areas of the world.

Recovery lessons from Hurricane Sandy to help improve resilience, disaster preparedness

Source: http://www.homelandsecuritynewswire.com/dr20170227-recovery-lessons-from-hurricane-sandy-to-help-improve-resilience-disaster-preparedness

Feb 27 – Purdue University will lead research to determine why some communities recover from natural disasters more quickly than others, an effort aimed at addressing the nation's critical need for more resilient infrastructure and to enhance preparedness.

The research team will apply advanced simulations and game-theory algorithms, access millions of social media posts and survey data collected along the New Jersey shore, which was devastated by Hurricane Sandy in 2012.

Purdue notes that the project, funded with a $2.5 million, four-year grant from the National Science Foundation, will focus on six communities.

"Why do some communities recover faster than others, and why do some neighborhoods never recover?" said Satish Ukkusuri, the project's principal investigator and a professor in Purdue's Lyles School of Civil Engineering.

"What are the underlying factors and mechanisms that

lead to this recovery? We need to understand this from an integrative, interdisciplinary and data-driven perspective and provide tools for emergency preparedness agencies so that both rural and city governments can be more prepared when disasters happen."

He is working with co-principal investigators Shreyas Sundaram, an assistant professor in Purdue's School of Electrical and Computer Engineering, and Seungyoon Lee, an associate professor in Purdue's Brian Lamb School of Communication. Also a member of the team is Laura Siebeneck, an associate professor in the University of North Texas Department of Emergency Management and Disaster Science.

"It's a very interdisciplinary team that involves social science, civil engineering, computer engineering and disaster management," Ukkusuri said. "We chose Sandy because it is the most recent large-scale disaster that has happened in the nation that involved a complex, diverse community. Sandy is not too old, so the data are fresh, and yet it is old enough that we can talk about recovery."

▶ **A YouTube video about the project is available at** https://youtu.be/5FgY16WvU6E.

The team will investigate recovery over a time scale ranging from the storm's immediate aftermath to the present day.

"So, it's from 2012 until 2016, and we might even look into the longer term because recovery time could take almost 10 or 20 years," he said.

From the social science perspective, the team will collect various kinds of data through surveys of residents in communities on the New Jersey shore.

"We will ask questions related to the recovery efforts, and we also want to understand how their social networks, their family structures, their community structures impede or contribute toward the recovery of these communities," he said.

The project will serve as part of the NSF's multiyear initiative on modeling resilience in interdependent systems and is funded by a program known as CRISP: Critical Resilient Interdependent Infrastructure Systems and Processes. Researchers will probe how to more efficiently allocate resources, better prepare, and reduce the time and cost of recovery when a community is struck by a disaster.

"We have the social side, which is how people interact with other people, and then we have the physical side, which is all these

infrastructure networks, the power grid, the communication systems and so forth," Sundaram said. "And you have interdependencies between the two sides. You have to understand both in order to really get a clear picture."

Modeling approaches will be harnessed for improved knowledge of both social factors such as how residents' involvement in the community affects their willingness to return to the neighborhood, and physical factors such as road and infrastructure repairs that enhance recovery.

Officials across the nation will be able to use the simulations in what-if scenarios.

"So you can change the initial conditions and then see what kinds of recovery outcomes you are going to get," Sundaram said. "And you can change community structures, people's objectives, what we call utility functions, and see how that would result in different kinds of recovery outcomes in the end."

Ultimately, Ukkusuri said, his team's goal is to allow governmental and emergency agencies to take actions that will accelerate system recovery and enhance the resilience of communities.

"The scientific tools will be broadly applicable to various types of disasters and communities," he said.

The project also will provide opportunities for students to work with a multi-disciplinary research team, preparing them for complex, systems-related challenges.

Serious security vulnerabilities found in home, business, industrial robots

Source: http://www.homelandsecuritynewswire.com/dr20170306-serious-security-vulnerabilities-found-in-home-business-industrial-robots

May 06 – Seattle, Washington-based IOActive, Inc. last week released a new paper identifying numerous vulnerabilities found in multiple home, business, and industrial robots available on the market today. The vulnerabilities identified in the systems evaluated included many graded as high or critical risk, leaving the robots susceptible to cyberattack. Attackers could employ the problems found maliciously to spy via the robot's microphone and camera, leak personal or business data, and in some cases, cause serious physical harm or damage to people and property in the vicinity of a hacked robot.

The research paper, Hacking Robots Before Skynet, is authored by IOActive's Chief Technology Officer, Cesar Cerrudo, and Senior Security Consultant, Lucas Apa.

"There's no doubt that robots and the application of Artificial Intelligence have become the new norm and the way of the future," said Cerrudo. "Robots will soon be everywhere - from toys to personal assistants to manufacturing workers - the list is endless. Given this proliferation, focusing on cybersecurity is vital in ensuring these robots are safe and don't present serious cyber or physical threats to the people and organizations they're intended to serve."

IOActive says that during the past six months, company's researchers tested mobile applications, robot operating systems, firmware images, and other software in order to identify the flaws in several robots from vendors, including: SoftBank Robotics, UBTECH Robotics, ROBOTIS, Universal Robots, Rethink Robotics, and Asratec Corp.

"In this research, we focused on home, business, and industrial robots, in addition to robot control software used by several robot vendors," said Apa. "Given the huge attack surface, we found nearly 50 cybersecurity vulnerabilities in our initial research alone, ranging from insecure communications and authentication issues, to weak cryptography, memory corruption, and privacy problems, just to name a few."

According to Cerrudo and Apa, once a vulnerability has been exploited, a hacker could potentially gain control of the robot for cyber espionage, turn a robot into an insider threat, use a robot to expose private information, or cause a robot to perform unwanted actions when interacting with people, business operations, or other robots. In the most extreme cases, robots could be used to cause serious physical damage and harm to people and property.

The report also outlines basic security precautions that should be taken by robotic vendors to improve the security of robots,

including implementing Secure Software Development Life Cycle (SSDLC), encryption, security audits, and more.

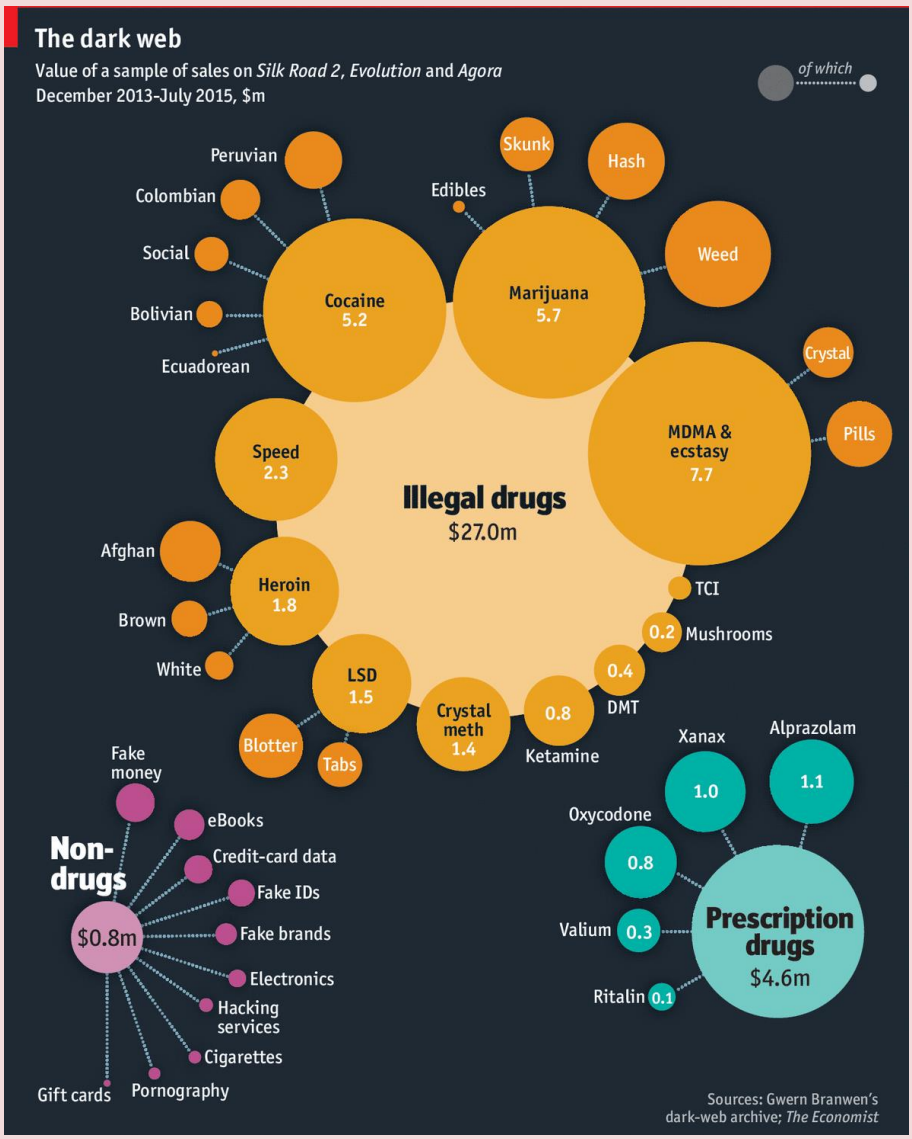
"We have already begun to see incidents involving malfunctioning robots doing serious damage to their surroundings, from simple property damage to loss of human life, and the situation will only worsen as the industry evolves and robot adoption continues to grow," continued Cerrudo. "Vendors need to start focusing more on security when speeding the latest innovative robot technologies to market or the issue of malfunctioning robots will certainly be exasperated when malicious actors begin exploiting common security vulnerabilities to add intent to malfunction."

IOActive notes that all vendors included in the paper were alerted of the various specific vulnerabilities identified within their products many weeks ago, in the course of responsible disclosure. Specific technical details of the vulnerabilities identified will be released at the conclusion of the disclosure process when vendors have had adequate time to address the findings.

— Read more in Cesar Cerrudo and Lucas Apa, Hacking Robots before Skynet (IOActive, 2017).

The dark web: What it is and how it works

By Daniel Prince (Associate Director Security Lancaster, Lancaster University, UK)
Source: https://www.weforum.org/agenda/2016/10/the-dark-web-what-it-is-and-how-it-works/



October 2016 – We often hear about the dark web being linked to terrorist plots, drug deals, knife sales and child pornography, but beyond this it can be hard to fully understand how the dark web works and what it looks like.

So just for a minute imagine that the whole internet is a forest – a vast expanse of luscious green as far as the eye can see. And in the forest are well worn paths – to get from A to B. Think of these paths as popular search engines – like Google – allowing you as the user the option to essentially see the wood from the trees and be connected. But away from these paths – and away from Google – the trees of the forest mask your vision.

Off the paths it is almost impossible to find anything – unless you know what you're looking for – so it feels a bit like a treasure hunt. Because really the only way to find anything in this vast forest is to be told where to look. This is how the dark web works – and it is essentially the name given to all the hidden places on the internet.

Just like the forest, the dark web hides things well – it hides actions

and it hides identities. The dark web also prevents people from knowing who you are, what you are doing and where you are doing it. It is not surprising, then, that the dark web is often used for illegal activity and that it is hard to police.

Technical challenges

Dark web technologies are robustly built without central points of weakness, making it hard for authorities to infiltrate. Another issue for law enforcement is that – like most things – the dark web and its technologies can also be used for both good and evil.

So in the same way criminals use it to hide what they are up to, it can also help groups fight oppression or individuals to whistle blow and exchange information completely anonymously. In fact, Tor – "free software and an open network that helps you defend against traffic analysis" and a critical part of the so-called dark web – has been funded by a range of Western governments, including the US.

A service like Tor, is global, in no one physical location, and is operated by no one commercial entity – which is typical of these technologies.

Theoretically, the only way to intercept communications sent via something like Tor is to install a

"backdoor" in the application everyone uses. A backdoor is meant to provide a secret way to bypass an application's protection systems – in a similar way to how people hide backdoor keys in flower pots in the garden in case they get locked out of their house.

However, the use of a "backdoor" could also allow any governments – even oppressive ones – to intercept communications. Indeed, cyber breaches have shown us that any backdoor or weakness can be found and exploited by hackers in order to steel people's information, pictures and data.

Exploiting the darkness

Of course, none of this is new – criminals have always found ways to communicate with each other "under the radar". Mobile phones have been used by criminal gangs to organise themselves for a long time, and as a society we are comfortable with laws enabling police to tap telephones and catch criminals.

Unfortunately, infiltrating the dark web is not quite as easy as tapping the local telephone exchange or phone network. Because the dark web is quite unlike the telephone system –

which has fixed exchanges and is operated by a small set of companies, making interception easier.
Even if tapping the dark web was a straightforward exercise, morally it is still fraught with questions. In the UK, the Draft Investigatory Powers Bill, dubbed the snoopers' charter, sets out the powers and governance for Law Enforcement over communications systems. However, the discussion of the bill has been impacted by the Snowden revelations which have demonstrated that society is not comfortable with mass, unwarranted surveillance.
This public distrust has led to many technology companies pushing back when it comes to accessing users' devices. We have seen Microsoft take on the US government over access to email and Apple against the FBI when petitioned to unlock an iPhone of a known terrorist.
And yet some of these same communications companies have been harvesting user data for their own internal processes. Famously, Facebook enabled encryption on WhatsApp, protecting the communications from prying eyes, but could still look at data in the app itself.
For now, though, it is clear that we still have a long way to go until society, government, law enforcement and the courts settle on what is appropriate use of surveillance both on and offline. And until then we will have to live with the fact that the one person's freedom fighting dark web is another's criminal paradise.

▶ ▶ Watch a related video in the source's URL.

More effective response to unpredictable disasters

Source: http://www.homelandsecuritynewswire.com/dr20170313-more-effective-response-to-unpredictable-disasters

Utøya memorial

Mar 13 – **When the unthinkable happens and the unpredictable takes over, crises cannot be handled by the book. What should the police have actually done during the 2011 attack on the Norwegian island of Utøya?**
22 July 2011: A terrorist attack in the government quarter has crippled Oslo, and reports of shooting on the island of Utøya are coming in. Desperate youths have already started swimming, and many of them are picked up by individuals in small boats.

The first police patrol arrives at the Utvika ferry dock opposite the island forty-four minutes after the perpetrator landed on the island.

The patrol has been ordered to observe, and decides to wait for the emergency squad that they believe to be heading in by helicopter. But Police officers only arrive on Utøya thirty-three minutes later. At least twenty people are killed during the last quarter hour of the massacre on the island. All told, the attack by Anders Behring Breivik on Utøya and the government quarter killed seventy-seven people, and was the deadliest attack on Norwegian soil since the Second World War.

Should police have violated the order?

Police received sharp criticism in the 22 July Commission report, which came out a year after the terrorist attacks. According to the Commission, the police officers who first arrived at Utvika should have immediately acted on their own, despite the fact that they had been ordered to observe what was happening.

"Police were strongly criticized in the report, but according to their existing procedures they actually did everything correctly," says NTNU associate professor Endre Sjøvold at the Department of Industrial Economics and Technology Management.

"In retrospect," he says, "we can see that maybe the police should allow their operational units greater autonomy in complex situations like this."

SINTEF says that Sjøvold has researched team dynamics and group processes for several decades, and over the past three years he has led the Innovative Teams project, which deals with managing operational situations where uncertainty predominates, and where the consequences could be great if something fails. He stresses that he has not studied the police conduct in the 2011 Norway attacks, but those attacks are good examples of issues that the project concerns itself with.

One of the results of the project is Norway's — and Europe's — first ICT-based educational program for operational leadership that incorporates the automated collection of interaction data. The program is geared to businesses where crises could have enormous social consequences – such as the Armed Forces and oil and power companies. The initiative's continuing education and training offerings at the Norwegian University of Science and Technology (NTNU) are being established in collaboration with the Norwegian Agency for Digital Learning in Higher Education (Norgesuniversitetet), starting in 2017.

Unusual crises require different practices

Sjøvold's research shows that traditional emergency work emphasizes fixed procedures and strong leadership, as is typically exemplified by the police force. People who do not

know each other can form an effective crisis team since they know what to do and have their regular roles. The team leader has final authority.
"This may involve breaking certain procedures, if they hinder solving the task at hand."
This kind of emergency team can be trained, enabling each employee to know exactly what he or she will do when a situation arises. Team members follow orders and concentrate on their specific task, which reduces stress.
This approach works in most emergency situations – but not when the unthinkable happens, as in the 2011 Norway attacks when chaos and unpredictability reigned and everything was turned upside down. This is when the rigidity of traditional crisis management needs to be set aside.
But how do you get police patrols to break an order or change a procedure and do something completely different than the team leader has instructed them to do?
"After 22 July, the police were criticized and the hospital received kudos," Sjøvold said. "But the police had faced a new and quite foreign situation, whereas the hospital was operating under more familiar conditions. Although the scale [of events] was bigger for the hospital, too, procedures were the same. Seen this way, I would say police were criticized a bit unfairly."

Flexible protocols needed
He points out that as the international security paradigm has evolved in recent years, so have the views on what constitutes effective operational leadership. Traditional practices have focused on safety procedures and regulations on the one hand and teamwork and communication on the other. Despite disagreement about what is most important, it has become evident that neither rules nor communication training alone are sufficient, according to Sjøvold.
Evaluations of past events indicate that the scale of the disasters could have been reduced if the ability to make decisions locally had been greater.
Sjøvold adds that the increased use of advanced technology and virtual communication reinforces the need for more integrated training and flexible protocols. Offshore oil installations and structures that are managed through computer systems by land-based personnel are one example where this is needed.

Local decision making can help limit the scale of disasters
Evaluations of past events show that the scale of many disasters could have been reduced if local decision-making power had been greater — that is, if the part of the team that was closest to the situation had been involved in a different way. For a response to be effective, team members and leaders need to be able to read the situation correctly and act in accordance with the intent of the assignment.
According to Sjøvold, this may involve violating existing procedures, if they are a hindrance to solving the mission. "If we believe that only one type of team dynamics works in all situations, we'll end up with teams that aren't able to solve the most critical tasks," he says.

Uncertainty in oil disaster

Gulf of Mexico, 20 April 2010: Everything was working as expected on Deepwater Horizon, the drilling rig that had recently been heralded for its security systems.
Suddenly an oil and gas blowout caused a huge explosion and fire on the rig, killing 11 workers. Two days later, the rig sank and triggered the largest oil spill in American history.
The subsequent investigation revealed considerable uncertainty around crew authority and roles, although these were clearly defined in the written procedures.
— One of the two rig officers was in the shower when the accident occurred, which delayed the emergency response efforts for several minutes. The procedures required that both officers take the decision on what should be done.
— When a young bridge officer on board signaled MAYDAY because she noticed that this had not been done, she was reprimanded by the captain.

— An emergency system to shut off the well was only triggered twelve minutes after the accident. The operation was delayed by a rule that said the highest-ranking officer present had to give the permission. On that day that officer was an onshore office employee who happened to be on a rare visit to the rig.

Mobilize the whole team

Kenneth Stålsett wrote his doctoral dissertation on teams and team dynamics in changing and uncertain settings, as part of NTNU's Innovative Teams project. His doctoral work included a study on the oil industry, where he looked at switching between routine and crisis operations. Stålsett has also conducted several studies on interactions, group dynamics and leadership in the Royal Norwegian Naval Academy operations.

Paradoxically, authoritarian leadership with centralized decision making is considered "military," even though the Norwegian Armed Forces introduced decentralized leadership in the early 1990s. So the military's approach, which bases leadership on operational context, is not anything new.

Stålsett points out that several other industries, like the oil industry, also practice this form of leadership to some degree, but they tend to revert to a "command and control" management style when a crisis situation arises.

"For example," he says, "we find that when the alarm goes off on an oil platform, employees are put under extreme mental and physical stress and instinctively follow what they're trained to do. In that case, it's drill and practice that prevails, and that in turn makes it difficult to adapt to new and changing situations."

Stålsett stresses that training in breaking out of routines is also needed for these kinds of operations.

"That's when something you've never trained for actually happens, and you have to mobilize the power of all the team members, not just the strong leader. You can't see the leader as an isolated entity. To have a good leader, all the team players need to assist and take on their share of leadership. This is exactly what the special forces and the Naval Academy do so well," he says.

Must challenge leadership

A good emergency response team, therefore, has to be able to change group dynamics when the situation demands it. A team that is just drilled in routines won't develop this capability.

"Most of the time we're used to being in groups with strong leaders, so this isn't necessarily easy to unlearn. In some cases it isn't the group leader who has the most influence. Influence sometimes coincides with social patterns rather than a formal title," Stålsett adds.

So how does one train for this more distributive leadership approach? It requires a team that works together, dares to ask questions and gives constructive criticism, according to Stålsett. This does not just apply to the oil industry and the military.

Imagine a regular meeting room where a project group or staff members are sitting. It is usually the ones who talk the loudest that get their way.

"Expertise is highly valued and as a rule one is expected to go along with the expert in a field. Experts tend to be right, but we can arrive at a better solution when we manage to add nuances. And experts aren't always right either, so we have to be able to challenge each other in an objective manner. Innovative solutions emerge when different areas of knowledge are brought together and combined," says Stålsett.

Creating a University Disaster Medical Response Team

By Ruben D. Almaguer

Source: https://www.domesticpreparedness.com/healthcare/creating-a-university-disaster-medical-response-team/

Mar 15 – As one of the top 10 disaster-prone states in the nation, Florida continues to strengthen its ability to prepare for and respond to any disaster requiring specialized emergency surgical or critical care medicine. With shrinking budgets and increased demand, building effective and rapid disaster medical response capabilities requires more than just collaboration among governments, healthcare providers, hospitals, and the private sector.

Building effective and rapid disaster medical response capabilities requires getting creative and exploring new organizations and resources such as universities. Most major universities are already integral parts of their communities, yet they still have untapped existing medical capability and resources that could enhance local and state response capabilities.

In 2015, Florida International University (FIU), located in Miami, reached into its own backyard and began a dialogue with the Florida Advanced Surgical Transport (FAST) Team to determine how the existing FAST Team could leverage the resources of FIU's Herbert Wertheim College of Medicine and Department of Emergency Management. Early in the process, both parties recognized that collaboration between FIU and the FAST Team could address many of the challenges and needs that the state of Florida and the FAST Team were struggling to handle. Currently, the FIU-FAST Team is in place and working through administrative and logistical challenges, adding new team members, purchasing and storing additional equipment, and securing a larger and more centralized warehouse facility in Miami-Dade County.

FIU-FAST Team members group photo, after conducting an austere environment exercise in the Everglades National Park, Miami, Florida (Source: Thomas Congdon, 10 December 2016).

Status of Florida's Medical Response Teams

Through the Florida Department of Health (DOH), the state maintains seven regional State Medical Response Teams (SMRTs) and one FAST Team. As the lead agency for public health and medical, DOH can activate SMRTs during a gubernatorial declared state of emergency when the ability to manage medical surge exceeds local resources and state assistance is required. The SMRTs and FAST Team are comprised of volunteer medical and public health professionals and support personnel. Although both receive funding through the DOH, the FAST Team is distinctly different from a SMRT as it is the only civilian critical care and surgical medical team certified and capable of transporting vehicles, equipment, supplies, and patients on military aircraft. On short notice, the FAST Team can immediately transport by ground or on military aircraft – such as a C5, C17, or C130 – via the 315th Airlift Wing, at the request of and supported by Homestead Air Reserve Base in Florida to the area of need.

FIU-FAST Team members inside their critical care tent, simulating patient packaging of a critical patient for helicopter transport in Miami, Florida (Source: FIU Media Relations, 29 April 2016).

Decision to Create a University-Based Disaster Medical Response Team

Over the years, Florida SMRTs and the FAST Team have faced the same perennial challenges as many federal, state, and local disaster response teams. Common questions include:

- How do you recruit, retain, and train volunteer medical professionals and support staff?
- How do you procure, maintain, and store nonmedical support equipment, a medical cache, and pharmaceuticals with limited funding?
- What is the latest research on emerging diseases or new public health threats?
- What are new technologies that can be used to teach and train medical professional?

The simple answer to all of these is, "Look in your own backyard."

Many major colleges and universities have a variety of medical professionals on staff. In addition to the obvious medical schools, there are opportunities and resources within other programs such as nursing or public health. Obviously, the primary focus of the academic faculty is to educate students, among their other administrative duties. However, it has been FIU's experience that, when asked and supported by their supervisors and deans, staff are more than willing to volunteer to be members of the FIU-FAST Team.

A large part of FIU's success in recruiting medical staff is owed to the leadership of Dr. John A. Rock, founding dean of the Herbert Wertheim College of Medicine and senior vice president of medical affairs. He immediately recognized the benefits of creating a university disaster medical response team and worked closely with the University's Department of Emergency Management to make it happen. Dr. Robert Levine, FIU college chair, professor of emergency medicine, and FIU-FAST team member, was tasked to identify and recruit existing FIU physicians in needed specialties (pediatrics, emergency medicine, anesthesiology, trauma surgery, and orthopedics) to voluntarily serve on the FIU-FAST Team. Ten additional FIU physicians quickly volunteered to be part of the team.

Maintaining a disaster medical response team in a deployable-ready status requires funding to purchase and store a significant amount of equipment and supplies. Limited funding also makes it difficult, if not impossible, to hire staff to perform the many administrative functions required to support a team such as maintaining personnel records, licenses, and certifications, property accountability, procurement contracts, vehicle maintenance, training records, etc. Limited funding also limits the ability to conduct trainings and exercises, a critical part of a team's development and its readiness level. Training provides new members and existing

members the chance to work together and understand each other's medical strengths and weaknesses, which strengthens the team's capabilities and effectiveness as a whole. The opportunity to practice with critical medical equipment, with each other, in an austere environment is invaluable.

FIU immediately tackled these fiscal challenges. Again, through the leadership of Dean John A. Rock, the Herbert Wertheim College of Medicine entered into a funding partnership with a multitude of private companies to assist in financially supporting the FIU-FAST Team. Supporters included Baptist Hospital, Florida Blue, Leon Medical Center, Nicklaus Children's Hospital, and The Batchelor Foundation for now. These partnerships quickly provided financial commitments to support needed operating expenses, including upgrading and purchasing equipment and medical supplies, acquiring a communications system, establishing a portable base of operations, and improving ground transportation.

This ability to recruit and utilize physicians and other medical professionals from within the university and from area hospitals has already paid dividends. Following Hurricane Matthew, the Florida Department of Health requested two members of the team to deploy to Daytona Beach to support Halifax Health Medical Center. In February 2017, the FIU-FAST Team deployed with the U.S. Southern Command and the U.S. Navy as part of a medical humanitarian mission known as Continuing Promise 2017. The FIU-FAST Team sent six physicians, one nurse, and one paramedic on a 12-day medical mission to Puerto Barrios, Guatemala. FIU-FAST served alongside a team of 169 Army, Navy, Air Force, and Marine Corps service members providing veterinary and medical services to local communities in Guatemala. Throughout the 12 days, the FIU-FAST Team saw over 1,500 patients and assisted in distributing much-needed medical supplies provided by the U.S. military to local hospitals.

The Next Step

There are clear, discernable advantages for local, state, and even federal medical disaster teams to collaborate with major colleges and universities. Like FIU, many of these institutions possess the credibility, organizational structure, and fiscal resources that can serve as a force multiplier in creating or collaborating with disaster medical teams. The experiences, good will, and community engagement that a team can bring to a university are equally vast.

The creation of the FIU-FAST Team illustrates the benefits of working with both government and private sector partners to find innovative solutions to long-standing problems. One final unintended consequence and benefit has been that the FIU-FAST Team has already inspired many medical and nursing students. Upon completing their education at FIU, they have been challenged to find similar disaster medical response teams around the country and the world to volunteer and give back to their communities during disasters, when their profession is most in need. With all the growing pains and a learning curve, and challenges still to be faced, the FIU-FAST Team has so far demonstrated that this university-based model is worth considering in other states.

▶ **For more information about FIU-FAST, visit** https://fast.fiu.edu/

Ruben D. Almaguer *currently serves as the assistant vice president of disaster management and emergency operations and serves as the executive director for the Academy for International Disaster Preparedness. He also oversees the Florida Advance Surgical Transport Team, in coordination with the Herbert Wertheim College of Medicine. Formerly, he served in Monroe County Fire Rescue Department, Florida, as the chief of emergency medical services. He served as the interim director and deputy director for the Florida Division of Emergency Management. Prior to this, he worked for Miami-Dade Fire Rescue Department as a division chief and led many Florida Task Force One (FL-FT1) Office of U.S. Foreign Disaster Assistance (OFDA) and Federal Emergency Management Agency (FEMA) Urban Search & Rescue Teams to over 27 natural and manmade disasters, including: earthquakes in Venezuela, Colombia, Taiwan, and Turkey; hurricanes and floods throughout Central America, Africa, and the Caribbean, including hurricane Katrina; as well as responses to the Oklahoma City Bombing and the terrorist attacks of 9/11 at the Pentagon in Washington, DC. He received masters in homeland security and defense from the Naval Postgraduate School and in public administration from Florida International University. He also graduated from Harvard University's John F. Kennedy School of Government's Senior Executives in State and Local Government and is a Certified Emergency Manager (CEM®).*

Calculating climate change losses in major European coastal cities

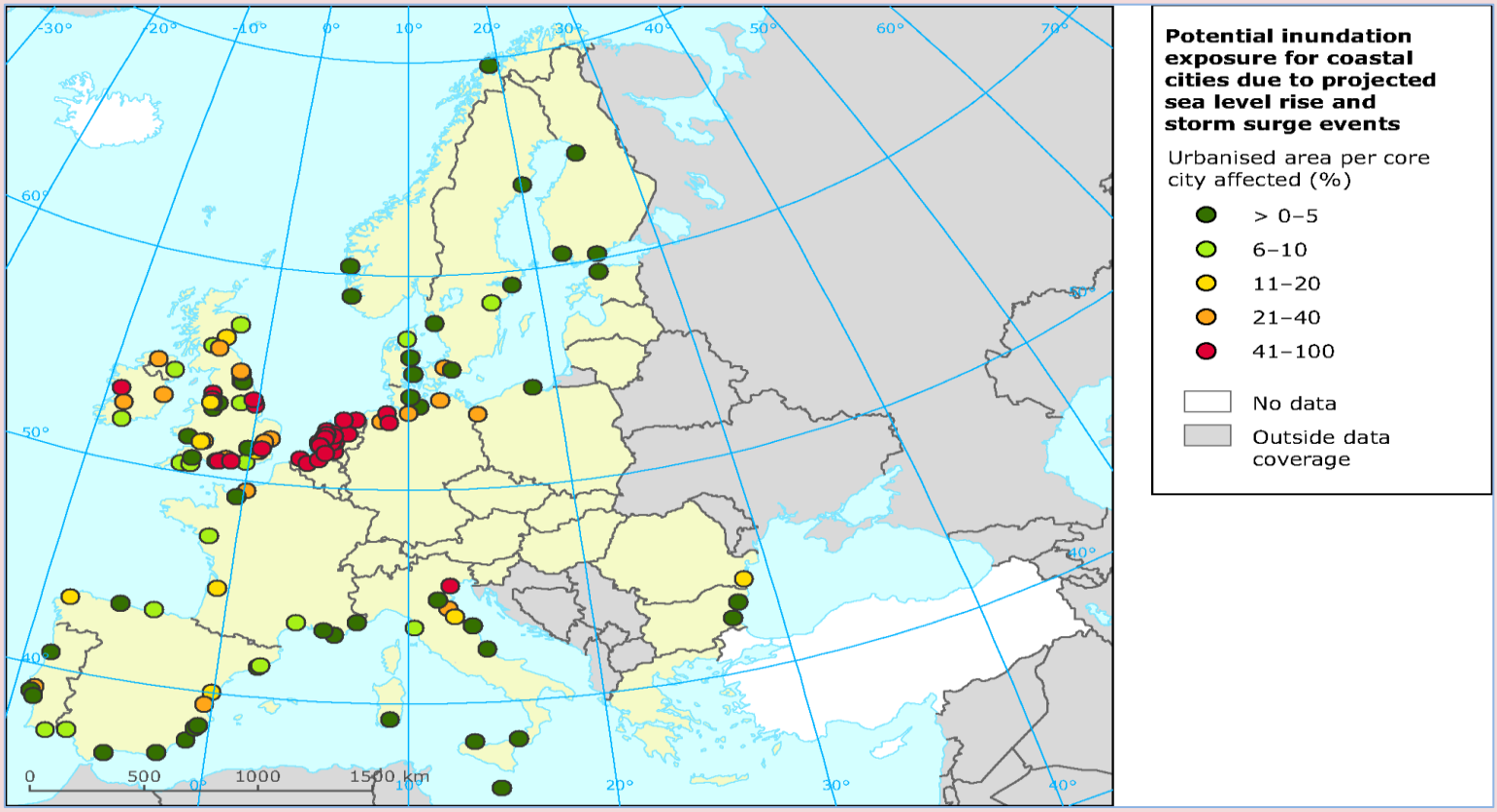
Source: http://www.homelandsecuritynewswire.com/dr20170302-calculating-climate-change-losses-in-major-european-coastal-cities

Mar 02 – **A new study that assesses potential future climate damage to major European coastal cities has found that, if, as currently, global carbon emissions continue to track the Intergovernmental Panel on Climate Change's worst emission scenario (RCP8.5), overall annual economic losses may range from $1.2 billion in 2030 to more than $40 billion by 2100.**

Frontiers notes that the paper, "Climate Risk Assessment under Uncertainty: An Application to Main European Coastal Cities," published in the journal *Frontiers in Marine Science*, focused on nineteen major European coastal cities including Istanbul, Rotterdam, Barcelona, Hamburg, London, Dublin, Marseille, St Petersburg, and Copenhagen.

For the first time, the report's authors adapted into their modelling methods for dealing with uncertainty well known in other fields of economics, such as financial economics. They successfully applied them to so called 'tail events' and their possible impacts in the chosen cities. The study's results show that despite their low probability of occurrence the huge scale of damage that tail events may cause means that they should be carefully considered in coastal vulnerability analysis.

In 2030, just thirteen years away, under a worst-case emission scenario, Rotterdam tops the economic impact table with expected annual losses of almost $240-million, closely followed by Istanbul, St Petersburg and Lisbon. By 2100 the expected annual losses in Istanbul could reach almost $10-billion, Odessa in the Ukraine could lose $6.5-billion annually, and Rotterdam $5.5-billion. Glasgow and Dublin could both suffer economic losses of around $1.5-billion in annual economic losses by 2100.



About two thirds of our planet's mega-cities—cities with populations of more than 5 million

people—are located in low-lying coastal areas so protecting these areas from rising sea levels is critical to saving lives and property. Being so vulnerable to the impacts of climate change, coastal cities also have a major role in adapting to them.

The report urges local, regional, and national policy-makers not to settle for traditional approaches to calculating climate impacts but instead seek to introduce risk assessments under uncertainty into their decision-making processes. The author's say that in line with the level of risk in each coastal city and the risk aversion of decision-makers, adaptation measures will need to be implemented in the near future in order to avoid critical damage and major losses.

— Read more in Luis M. Abadie et al., "Climate Risk Assessment under Uncertainty: An Application to Main European Coastal Cities," Frontiers in Marine Science *(16 December 2016).*