January 2015

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

10 years

Charlie Hebdo

www.cbrne-terrorism-newsletter.com

Strategic Frames Analysis of NATO Ballistic Missile Defense and Changes in Public Opinion

Source: http://www.stratcomcoe.org/~/media/SCCE/BALISTISKO_RAKESU_PETIJUMS.ashx

STRATEGIC FRAMES ANALYSIS OF NATO BALLISTIC MISSILE DEFENSE AND CHANGES IN PUBLIC OPINION

Steven R. Corman
Kristin P. Fleischer
R. Bennett Furlow
Hasan Davulcu
Matthew Wiedeman

This project was designed as a capabilities demonstration for the Latvia Ministry of Defence, NATO Strategic Communications Centre of Excellence (NATO STRATCOM COE). The project developed a media analysis methodology based on strategic framing, a well- known function of media and strategic communication that attempts to influence the perception of facts and situations by encouraging certain interpretations and discouraging others using words, phrases, metaphors and images highlight desired aspects of a perceived reality. The goals were to demonstrate that framing is relevant to understanding and improving strategic communication capabilities of NATO member and partner countries, to do this in the context of a topic important to NATO, and to show the potential relevance of these methods to operational capabilities.

The project studied NATO Ballistic Missile Defense, as discussed in texts from NATO, the governments of nine member/partner countries, and major print media outlets from these same countries. Initial analysis of a sample of these texts revealed ten frames: General threat, specific threat, collective security, deterrence systems, domestic benefit, progress/effectiveness, political tensions, threat to Russia, Russian roadblocks, and Russia partnership. Each frame could be either affirmed or negated in a particular framing instance.

These frames were reliably coded and analyzed in 795 texts from the above sources. The analysis shows, first, that with respect to NATO/government sources, NATO framing is very disciplined, consistently invoking general threat, specific threat, collective security, deterrence systems, progress/effectiveness, and Russia partnership in the affirmative, and negation of threat to Russia. Government framing is remarkably similar to NATO framing. Second, media framing is significantly different from that by NATO and government sources. In almost all cases, media are significantly less likely to invoke the frames favored by NATO and government, and significantly more likely to use frames less emphasized by them. This indicates that Russian strategic communication is driving media coverage, likely because of the media's interest in reporting and promoting controversy. Third, framing appears to differ based on both individual countries' political and economic concerns, as well as the general political climate. Finally, there are strong correlations between some of the frames studied and public opinion in the United States and Poland. This suggests that framing analysis could serve as a useful measure of effectiveness for NATO strategic communication.

The project also established the practicality of adding a strategic framing capability to the NATO STRATCOM COE. First, it showed that data from the project could be effectively incorporated into a decision-making environment based on ASU Decision Theater visualization technology. Second it demonstrated that automation of strategic frames coding using machine classifiers is feasible. The combination of these can provide real-time, on-demand analysis and monitoring of strategic framing on topics of interest to NATO.

Based on results of this project we make three recommendations: (1) The NATO STRATCOM COE should develop an in-house capability to do strategic frames analysis, (2) it should develop training for NATO personnel on framing, and (3) it should develop the equipment and capabilities to visualize data.

▶ **Read the full text at source's URL.**

Drone spotted over Belgium nuclear plant

Source: http://zeenews.india.com/news/world/drone-spotted-over-belgium-nuclear-plant_1518054.html

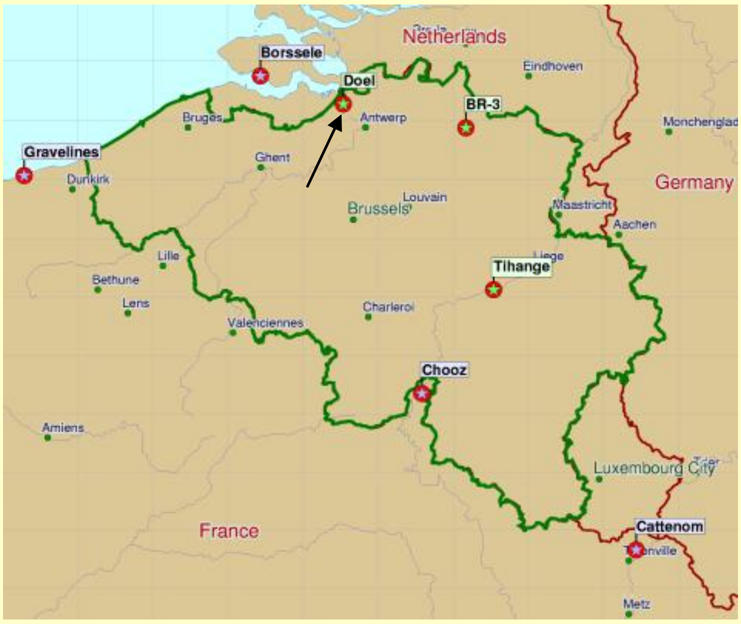
Dec 21, 2014 – **An unexplained drone was spotted flying over a Belgium nuclear facility,** local authorities have said, a day after one of the plant's reactors came back on line after a four-month closure caused by sabotage.

The mystery appearance by an unmanned aircraft, on which Belgian authorities refused to provide much detail, resembles a spate of similar drone sightings over nuclear plants in neighbouring France this autumn.

Around 20 unidentified drones have been spotted over nuclear plants since October throughout France.

"We can confirm that the East Flanders prosecutor's office has opened an investigation into a drone flight over the Doel nuclear plant," a spokesman for the investigation told Belga news agency.

"We will not provide further information for the time being," the spokesman added, hours after the plant's operator, GDF-Suez unit Electrabel, first disclosed the incident, which took place early yesterday.



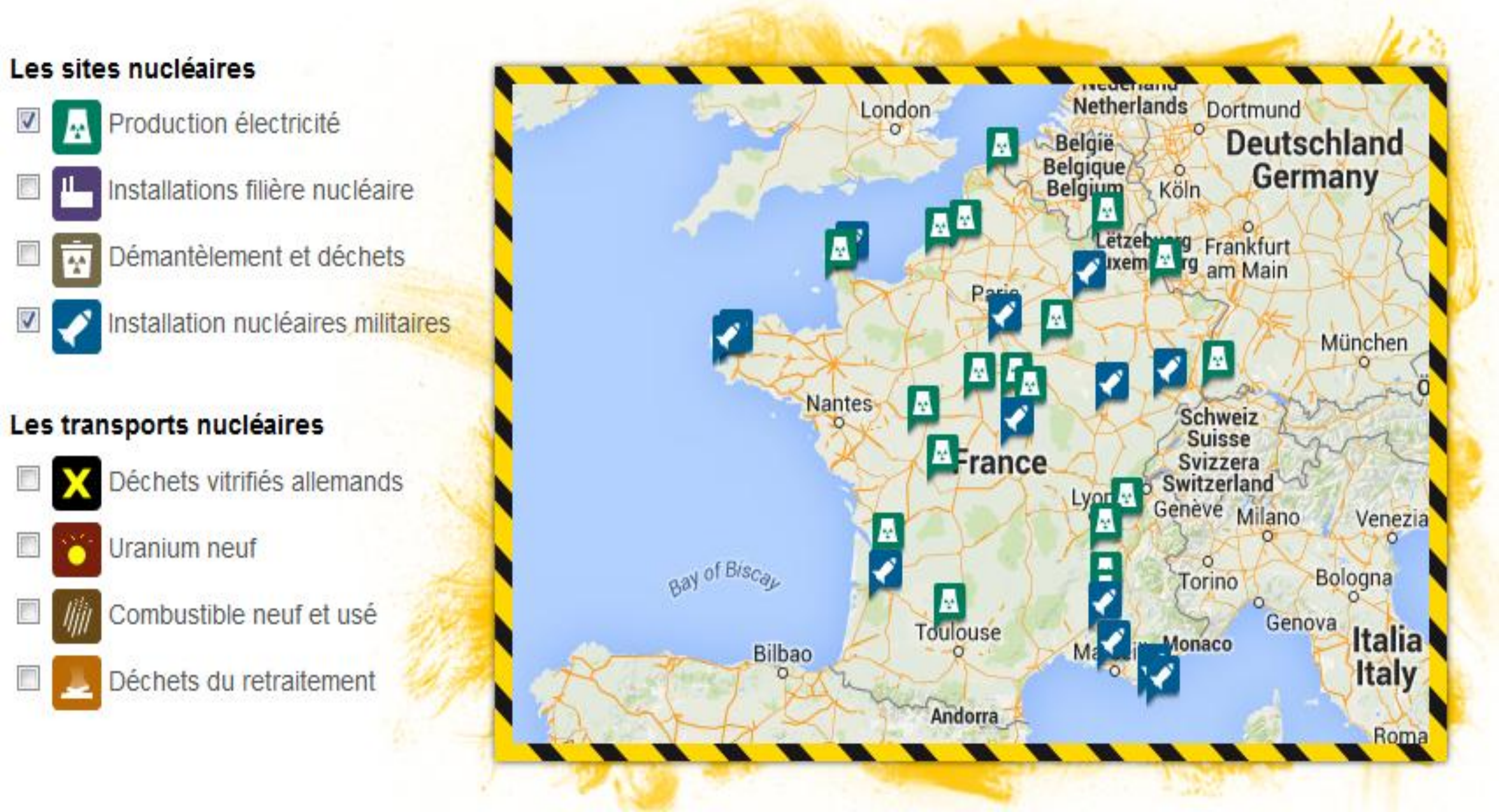
The imposing Doel nuclear site sits on a riverbank near the North Sea about 25 kilometres north of Antwerp. It holds four of Belgium's seven reactors.

One of those reactors, Doel 4, was shut urgently in August after a leak, caused by tampering, gushed out 65,000 litres of oil lubricant.

A steam turbine weighing 1,700 tonnes was severely damaged by the loss of lubricant, requiring a 30-million-euro (USD 37-million) repair job that was carried out in Germany.

Belgian prosecutors have refused to confirm the sabotage as an act of terrorism, without excluding it either.

Two other Belgian reactors still remain shut, both due to cracks in their reactor containment vessels.


Les sites nucléaires

☑ Production électricité

□ Installations filière nucléaire

□ Démantèlement et déchets

☑ Installation nucléaires militaires

Les transports nucléaires

□ Déchets vitrifiés allemands

□ Uranium neuf

□ Combustible neuf et usé

□ Déchets du retraitement

To face a potential shortfall in power, Belgium's government on Thursday said plans to close the Doel site's two oldest reactors, both nearly four decades old, would be suspended.

The Doel 1 and 2 reactors were due to be the first to be shut as part of Belgium's planned phase out of nuclear power by 2025, but the government said it would seek to keep them operating.

Nuclear plants account for 55 per cent of Belgium's power generation, and the loss of over half of the country's nuclear power has caused concerns of a shortage or even a blackout.
Regulators have put in place special measures to help meet Belgium's needs this winter.

EDITOR'S COMMENT: First France, now Belgium! Also over Hellenic Ministry of Defense (5 flights; one during the night [2014]). Simple curiosity? Testing responses and counter measures (by both sides of the moon)? Testing drones' capabilities? Connected incidents or just coincidences? Part of a massive terrorist plan – recon phase? Then another question: can these drones really harm a nuclear plant? Surely not! BUT the impact would be tremendous not to mention the cost of follow-up hardening that follows all revealed plots – both in paper and in reality. And a more generic question: "Are UAVs the next tool for bombing incidents in urban environment?" Here the answer is not "surely not"…

Micro Nukes: New warfare in Terrorism

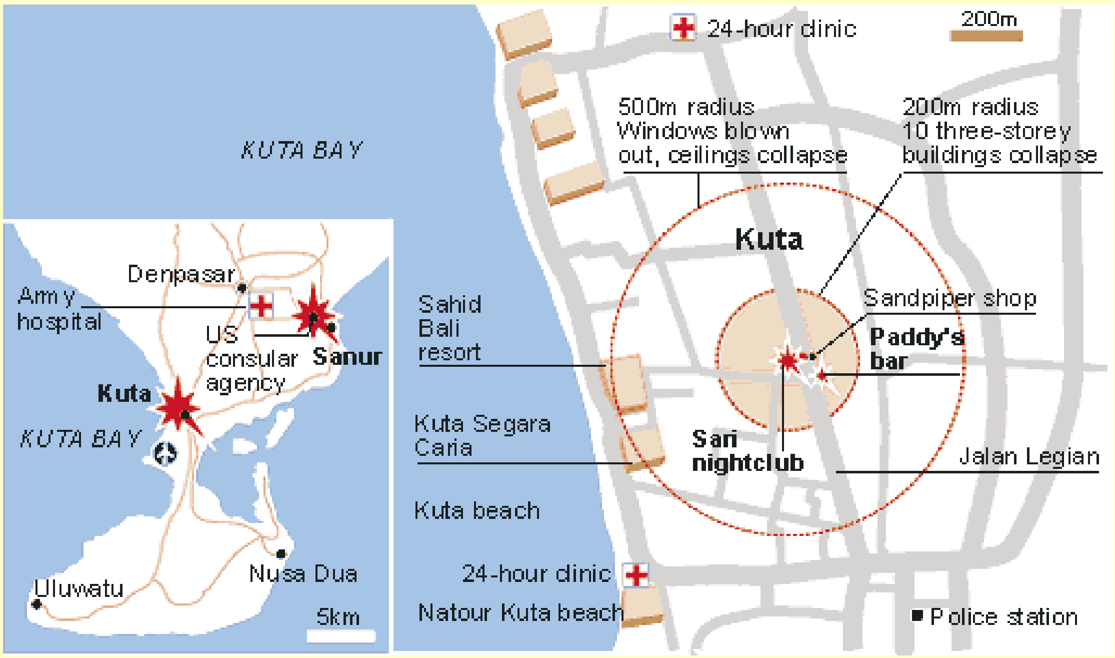
Source: http://www.newdelhitimes.com/micro-nukes-new-warfare-in-terrorism123/

Micro nuclear bombs or Micro nukes as the name suggests are mini versions of a larger technology that can physically wipe out cities or even countries. **These nukes are also known as the 1/10th version of a nuclear weapon, but are known to be quite effective.** Mini or Micro nukes have been present for a long time, this tactical nuclear weapon is portable enough to be carried in a suitcase or a backpack, till now only the United States and the then Soviet Union/ Russia are known to have the technology that could manufacture micro nuclear weapons. Though neither country has ever made public the existence of such weapons. Countries such as China, Israel are reported to be producing Micro Nukes. Any form of nuclear weaponry in itself is worrisome to put it lightly, weapons being in the wrong hands is even worse. New reports say that now militant groups and terrorists have started to get their hands on these new weapons of mass destruction that now come in a smaller size.

9/11 and others

Scientists and reporters have been going back and forth on the theory that for two enormous towers to be pulverized there may have been nuclear forces at play. In a recent investigation done by several international inter-governmental organizations**, traces of nuclear material were found in the 9/11 airline bombing** and at several locations in the Middle East. In 2002, in **Bali, Indonesia when 188 club goers were killed in a blast (photo next page) that had reports of survivors having their skin fall off.** The attacks were linked to Al Qaeda as the traces of the same were found in the US embassy bombing in Libya which killed the

US ambassador. If certain intelligence reports are to be believed then **Micro Nukes have been used more than 50 times** but have never been exposed due to fear of a mass hysteria. From the Bali bombing to the Oklahoma City bombing, micro nukes are being suspected as the weapon of choice.



ISIS and Al Qaeda

The terrorist organisations mainly ISIS and Al-Qaeda have found the source of these weapons and have been openly using these since couple of years. Since the knowledge of using these Micro Nukes is limited even within the terrorist community, the demand for the handlers is high and limited. It is believed that several terrorist cells have Micro Nukes in possession but are not aware of how to use them or operate them. Most recently the United Nations released information that according to an ISIS militant, the Islamic State has developed a nuclear weapon from radioactive material stolen from an Iraqi university (Mosul).

Governments are collaborating to take hold of the situation, for example the United States and Russia agreed to exchange intelligence information on the quantity, types, and locations of Syrian chemical weapons and to develop procedures for the destruction of Syria's chemical weapons stockpile. Similarly, with the help of intelligence agencies and inter agency cooperation, the government is using methods of finding and eliminating these cache of new weapons. The extent of the availability of Micro Nukes is unknown and is certainly a cause for worry.

▶ **Read the related postings below** – quite interesting apart the conspiracy theories mentioned:
http://www.cuttingedge.org/news/n1715.cfm
http://911research.wtc7.net/wtc/analysis/theories/nuclear.html
http://themillenniumreport.com/2014/09/busting-911-myths-nanothermite-big-nukes-and-dews/

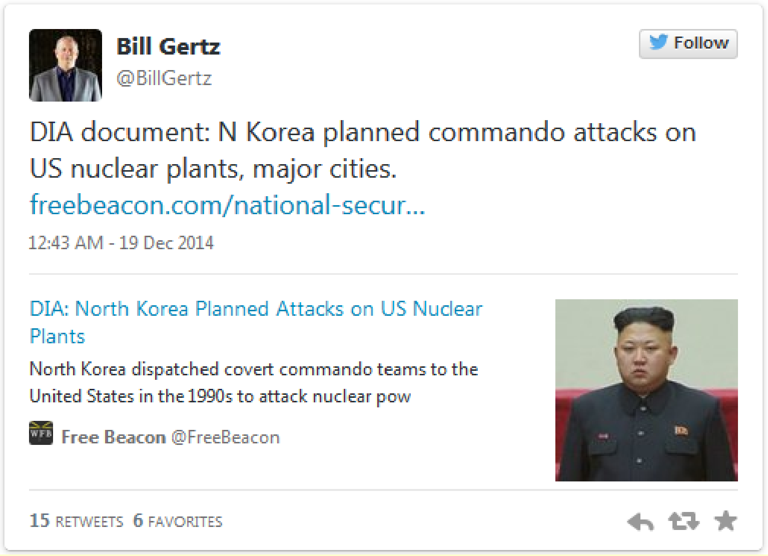
North Korea Allegedly Planned Attacks On U.S. Nuclear Plants

Source: http://www.inquisitr.com/1692452/north-korea-allegedly-planned-attacks-on-u-s-nuclear-plants/#xioFcjB76hXILDqG.99

North Korea allegedly planned to attack U.S. nuclear power plants in the 1990s, according to a recent article and declassified intelligence report, but whether that is true remains unclear.

Bill Gertz of the *Washington Free Beacon* reported on December 18 that North Korea had inserted teams into the U.S. in order to attack nuclear power plants and other targets.

"The document states that the North Korean Ministry of People's Armed Forces, the ministry in charge of the military, 'established five liaison offices in the early 1990s, to train and infiltrate operatives into the United States to attack nuclear power plants and major cities in case of hostilities.'"



Bill Gertz
@BillGertz

Follow

DIA document: N Korea planned commando attacks on US nuclear plants, major cities. freebeacon.com/national-secur...

12:43 AM - 19 Dec 2014

DIA: North Korea Planned Attacks on US Nuclear Plants

North Korea dispatched covert commando teams to the United States in the 1990s to attack nuclear pow

Free Beacon @FreeBeacon

15 RETWEETS 6 FAVORITES

The article is based on a declassified Defense Intelligence Agency report obtained by The DMZ War website through a Freedom of Information Act request. The declassified document is a raw intelligence report, and the significance of that is partially explained in the *Free Beacon* article.

"The heavily redacted report is what is known as a raw intelligence report, consisting of information possibly provided to the United States by a defector or agent, or possibly obtained from electronic surveillance."

However, a raw intelligence report also means that intelligence analysts have not had the chance to verify its accuracy based on information from other sources. The raw intelligence report says as much in one of the first lines of the unredacted portions. "Warning: (U) This is an information report, not finally evaluated intelligence."

Additional information in both the *Free Beacon* article and on The DMZ War website indicate the U.S. might not have received further intelligence to verify that North Korean operatives were on U.S. soil and planning attacks on nuclear sites or other targets. The DMZ War website reports the FBI could not locate any information on this upon request.

"Despite the reports mentioned above, and other Pentagon analysis on the Reconnaissance Bureau, the FBI has repeatedly rejected DMZ War Freedom of Information Act requests for its information on the Reconnaissance Bureau and related organizations. Not because all such reports remain classified, but – remarkably — because the Bureau claims it can't find any reports on North Korea's main intelligence and terrorism group."

The Free Beacon acknowledges these sentences in its article.

Yet none of this means the DIA raw intelligence report is wrong. The *Free Beacon* article quoted multiple people, who indicate that the U.S. may have underestimated North Korean capabilities. The article also reported that the North Koreans have previously conducted multiple significant operations in other parts of the world, even as it later stated that "intelligence activities" in the U.S. have been "limited."

The raw DIA intelligence report and *Free Beacon* article on alleged North Korean activities in the U.S. underscore how difficult it can be for U.S. officials to assess threats. They often can be accused of failure regardless of how they act. A recent press release from Senator Carl Levin accused the George W. Bush administration of misinterpreting intelligence used in the lead-up to the Iraq War. Senator Levin claims that other intelligence disproved intelligence the Bush administration supposedly relied on as accurate. Meanwhile, a recent article from *NBC News* reported on accusations that a U.S. intelligence official failed to share intelligence that might have helped prevent the September 11, 2001 attacks on the U.S. The *NBC News* article reported that this "was considered by the 9/11 Commission as a key intelligence failure."

The Inquisitr previously reported on how the U.S. has identified North Korea as being responsible for the cyberattacks on Sony.

The Russian and Iranian Missile Threats: Implications for NATO Missile Defense

Memorandum No. 143 Tel Aviv: Institute for National Security Studies, November 2014

By Azriel Bermant

Source: http://www.inss.org.il/index.aspx?id=4538&articleid=8425

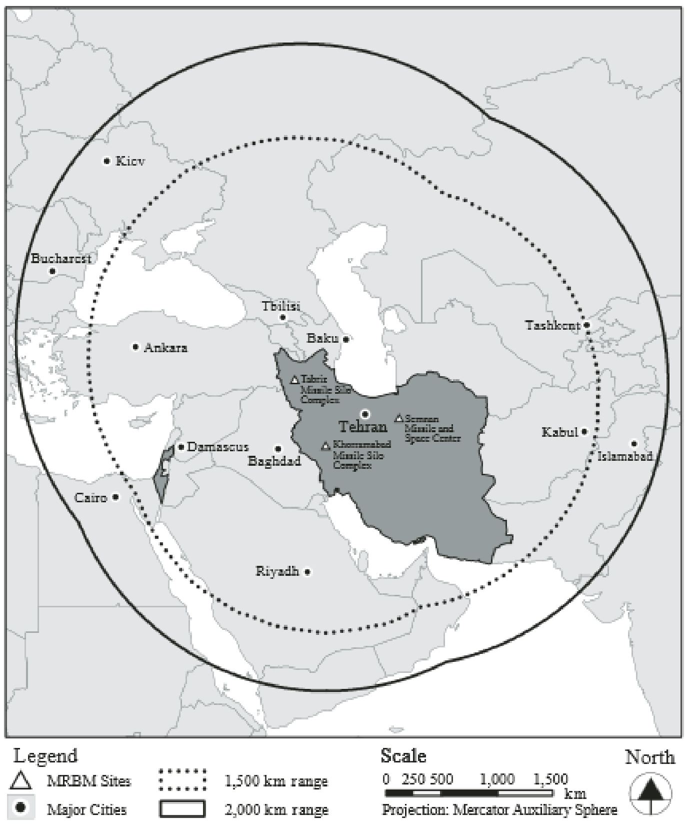
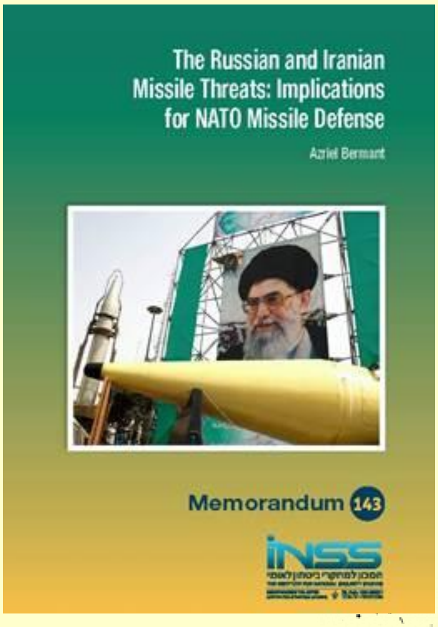


Figure 2: MRBM Sites and Ranges

As tensions rise over Ukraine, NATO is making preparations for the deployments of a ballistic missile defense (BMD) system in Romania in 2015 and in Poland in 2018. The United States and NATO claim that the missile defense shield is not directed at Russia, but is designed to deal with the dual threat of ballistic missiles and weapons of mass destruction emanating from the Middle East. Russia, on the other hand, has consistently maintained that the anti-missile shield is directed at its own strategic nuclear forces, as NATO's planned deployments in Eastern Europe reinforce the Kremlin's resentment over what it perceives as Western penetration into its "near abroad." The monograph provides an in-depth exploration of the ongoing controversy over the NATO BMD system in Europe and argues that the very high cost of maintaining the system is justified in terms of its ability to mitigate damage, provide greater flexibility for national leaders, strengthen the morale of vulnerable populations, and devalue the threats posed by revisionist states.

***Azriel Bermant**, a research fellow at the Institute for National Security Studies, specializes in US Arms Control Policy, US Policy in the Middle East, NATO missile defense policy, and nuclear weapons proliferation. He is also an expert on Israel's relations with Europe. Dr Bermant was awarded his PhD from University College London. The title of his doctoral thesis was: "A Triumph of Pragmatism over Principle: Margaret Thatcher and the Arab-Israel Conflict." Between 1998 and 2006, he worked as a writer, editor, and translator for the Israel Ministry of Foreign Affairs in Jerusalem.*


The Russian and Iranian Missile Threats: Implications for NATO Missile Defense

Azriel Bermant

Memorandum 143

INSS

▶ **You can read the full report at:**
http://www.inss.org.il/uploadImages/systemFiles/memo143i.pdf

If South Korea's nuclear plant staff are vulnerable, then so are the reactors

By Alan Woodward

Source: http://www.homelandsecuritynewswire.com/dr20141224-if-south-korea-s-nuclear-plant-staff-are-vulnerable-then-so-are-the-reactors

Does it matter that a South Korean nuclear plant was hacked and plans of the complex stolen? As it is South Korea that's the subject of this latest attack, everyone tends to assume it must have had something to do with North Korea. With a target as sensitive as a nuclear power plant, not unreasonably people are asking if safety could be compromised by a cyberattack. **Could hackers cause the next Chernobyl or Three Mile Island?** This points to an important and infrequently discussed problem, the vulnerability of critical national infrastructure. Cyber-attacks like these are a great way of levelling the playing field: why invest in massively expensive nuclear weapons program if you can simply shut down your enemies' power, gas, water, and transportation systems? Increasingly more and more infrastructure is connected to the Internet, with all the security risks that entails.

Claude Shannon, who many consider the father of modern information theory, wrote a paper in 1949 in which he pointed out that security should never be based upon your enemy's ignorance of how your system is built. This is known today as the mantra: "There is no security through obscurity." Does it matter, then, that a South Korean nuclear plant was hacked and plans of the complex stolen? That rather depends on what happens next.

As it is South Korea that's the subject of this latest attack everyone tends to assume it must have had something to do with North Korea. With a target as sensitive as a nuclear power plant, not unreasonably people are asking if safety could be compromised by a cyber attack. Could hackers cause the next Chernobyl or Three Mile Island? The South Korean authorities have sought to reassure the public, making it clear that no "core systems" — those computers that control the reactor and safety systems — were compromised.

If it was North Korea — and there is no evidence it was — then one might imagine it was actually the technical details and blueprints of a modern nuclear reactor that was the intended target. But sadly there is secondary security implication: the plans reveal the role of the human operators in running the reactor, and when it comes to hacking into critical infrastructure it is people that are the weakest link.

Weakest link in the chain

For example, when Iran's nuclear reprocessing plant at Natanz was hacked with the infamous Stuxnet virus, it should not have been possible as the computers affected were not connected to the outside world. There was a very distinct "air gap" maintained between the reactor computer controllers and any other network. But that air gap was relatively easy to bridge, by leaving USB sticks where curious people would find them, plug them in, and transfer the virus to the systems.

Imagine that — now you know which computers operate a nuclear power plant, and who uses them, which departments they work in, and at what times. Suddenly it's possible to design a very targeted attack on the operators themselves, aimed at fooling them into breaching their own security. Information about people and processes that operate a technology is as valuable to a hacker as knowledge of the technology itself. Not only did Stuxnet damage equipment, it caused the computers to falsely report that all was well to the operators. It doesn't take much imagination to see how the same could happen to a nuclear power plant — with devastating consequences.

And so although it's great to hear that the plant operators are running safety drills, I really hope they make sure that their security drills include the vital triad of people, processes, and technology.

The "soft target" of civilian infrastructure

This again points to an important and infrequently discussed problem, the vulnerability of critical national infrastructure. Cyber-attacks like these are a great way of levelling the playing field: why invest in massively expensive nuclear weapons program if you can simply shut down your enemies' power, gas, water, and transportation systems? Increasingly more and more infrastructure is connected to the Internet, with all the security risks that entails.

And many of these systems — hardware and software — are old, updated far less frequently than a desktop computer at home or at work. Computer security flaws that may have ceased to be a problem in data centers or on desktops years ago might still affect an embedded system running a gas pump, sluice gate or electricity sub-station somewhere.

The U.K. government at least has been on the case for some time, having established the Center for the Protection of National Infrastructure (CPNI) to focus on infrastructure resilience to cyber-attacks. Bringing together various government agencies and businesses, it has made significant progress in at least establishing what might be vulnerable, which is the first step in knowing where to focus your efforts.

There is no room for complacency, however, as every day more systems become Internet-connected, and more security vulnerabilities are discovered. **This trend of attaching everything and anything to the Internet — such as with the growing Internet of Things, but not limited to that — is embraced even more enthusiastically in Europe and the United States.** Take a look at search engines like Shodan or Thingful which show locations of online devices, and see just how widespread the Internet of Things has already become.

This problem will not go away. It is a fact now and will only grow in the future. Security is possible only by including people and processes as well as technology. And anyone who relies solely on security through obscurity is doomed to fail.

***Alan Woodward** is Visiting Professor at University of Surrey.*

One million curies of radioactive material safely recovered

Source: http://www.homelandsecuritynewswire.com/dr20141224-one-million-curies-of-radioactive-material-safely-recovered

Dec 24, 2014 – Los Alamos National Laboratory (LANL) expertise helped the Department of Energy's (DOE) National Nuclear Security Administration (NNSA) Defense Nuclear Nonproliferation (DNN) Radiological Material Removal Program's Off-Site Source Recovery Project (OSRP) recover more than one million curies of radioactive sources since 1999. LANL says that the accomplishment represents a major milestone in protecting our nation and the world from material that could be used in "dirty bombs" by terrorists.

"Taking disused, unwanted and, in limited cases, abandoned nuclear materials out of harm's reach supports the Laboratory's mission of reducing global nuclear danger," said Terry Wallace, Principal Associate Director for Global Security at Los Alamos. "This milestone represents tremendous progress in removing a potentially deadly hazard from all corners of the globe. Los Alamos helped usher in the nuclear age, so it's quite appropriate that this Laboratory continues to use its nuclear expertise to assist the DOE in stewardship of nuclear materials."

Off-Site Source Recovery Project personnel recovered several high-activity sealed radioactive sources from a Maryland facility in November, which pushed the total recovered radioactivity above one million Curies. Los Alamos National Laboratory supports OSRP with instrumentation, expertise, and personnel. **With the Maryland recovery, OSRP has recovered and secured more than 38,000 sealed radioactive sources from more than 1,100 different locations, including all fifty states within the United States.**

The particular source that achieved the 1-million-curie milestone was a small stainless steel capsule, about the size of a pencil (photo), containing 100 curies of the radioactive isotope cobalt-60. This source was part of a larger 9,000-curie shipment that was characterized and verified before loading into specially shielded containers for safe transport to a secure location.

A Curie is a unit of radioactivity named after scientists Marie and Pierre Curie, who discovered, among other things, the element radium. One Curie is roughly equivalent to the amount of radioactivity in one gram of the radium-226 isotope.

NNSA's DNN Radiological Removal Program and OSRP mission includes removal and disposal of excess, unwanted, abandoned, or orphan radioactive sealed sources that pose a potential risk to national security, public health, and safety. These sources include radiological materials from universities, and medical and research facilities worldwide that could potentially be utilized in a dirty bomb — an ad-hoc weapon created by rogue states or individuals to instill fear and disrupt activity in large population areas.

DOE initiated OSRP in 1999. Originally it was an environmental management project to recover and dispose of excess and unwanted sealed radioactive sources. In 2003, the project was transferred to NNSA DNN in a shift towards more aggressive recovery of unwanted radioactive sealed sources for national security purposes. Sealed source recovery and disposal efforts result in permanent threat reduction, as this material is eliminated and no longer has potential to be used by terrorists.

Vast secret Nazi 'terror weapons' site uncovered in Austria

Source: http://www.theaustralian.com.au/news/world/vast-secret-nazi-terror-weapons-site-uncovered-in-austria/story-fnb64oi6-1227168312942?utm_content=SocialFlow&utm_campaign=EditorialSF&utm_source=TheAustralian&utm_medium=Twitter

A secret underground complex built by the Nazis towards the end of World War II that may have been used for the development of weapons of mass destruction, including a nuclear bomb, has been uncovered in Austria.

The vast facility was discovered last week near the town of St Georgen an der Gusen.

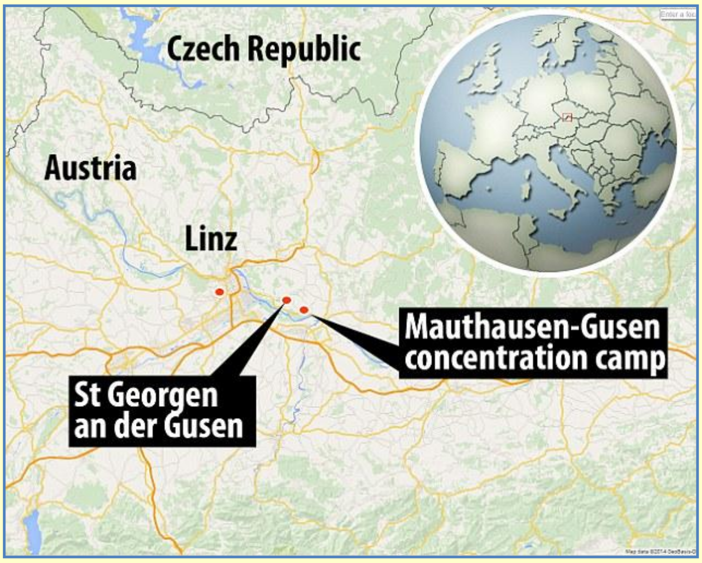
It is believed to be connected to the nearby B8 Bergkristall underground factory that produced the Messerschmitt Me-262; the first operational jet-powered fighter that posed a brief threat to allied air forces in the war's closing stages.

Although the Bergkristall factory was examined after the war, the Nazis went to much greater lengths to conceal the newly discovered bunkers apparently used for weapons research. Declassified intelligence documents as well as testimony from witnesses helped excavators identify the concealed entrance.

Heavy equipment was deployed to cut away thick layers of soil as well as large granite plates with which the Nazis in 1945 had sealed the entrance shaft once used by large transport trucks.

Ground-penetrating radar confirmed historic accounts that the underground maze covers an area of up to 30ha; researchers found helmets and other Nazi items scattered by the entrance.

"This was a gigantic industrial complex and most likely the biggest secret weapons production facility of the Third Reich,” said Andreas Sulzer, an Austrian documentary film-maker who is in charge of the excavations.



The facility, like the Bergkristall factory, relied on slave labour from the nearby **Mauthausen-Gusen concentration camp** (photo right). Up to 320,000 inmates are said to have died because of the brutal conditions in the subterranean labyrinth.

Sulzer, whose work is funded by broadcasters including ZDF, the German state television network, found a reference to the bunkers in the diaries of an Austrian physicist who was called up to work for the Nazis.

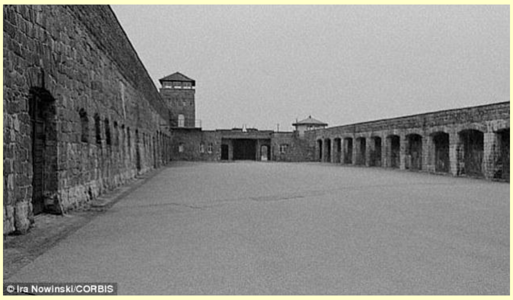
The film-maker assembled a team of historians and found further evidence of scientists working on the secret project, which was managed by SS General Hans Kammler.

Kammler was in charge of Hitler’s missile programs, including the V-2 rocket used against London in the latter stages of the war.

He was known as a brilliant but ruthless commander, who had signed off the blueprints for the gas chambers and crematoria at the Auschwitz concentration camp complex in southern Poland. Rumours persist that he was captured by the Americans and given a new identity after the war.

Previous research had found increased levels of radiation around the St Georgen site, apparently giving credibility to longstanding claims that Nazi scientists experimented with nuclear weapons in the area, which was under the exclusive command of the SS.

“The SS leadership ... aspired to create a combination of missiles and weapons of mass destruction. They wanted to equip the A4 (a variant of the V-2) missile, or more advanced rockets, with poison gas, radioactive material or nuclear warheads,” said Rainer Karlsch, a historian who worked with Sulzer.


© Ira Nowinski/CORBIS

A key lead obtained by Sulzer was the testimony of John Richardson, whose father Donald was a top operative of the Office of Strategic Services, forerunner of the CIA.

Donald Richardson reported directly to supreme allied commander General Dwight D. Eisenhower and one of his tasks was to ensure that Kammler and other leading Nazi scientists did not fall into the hands of the Russians.

The OSS reported in February 1944 that a huge complex was operated near St Georgen. Aerial footage from RAF planes obtained by Sulzer shows the outline of a concrete structure with large entrances.

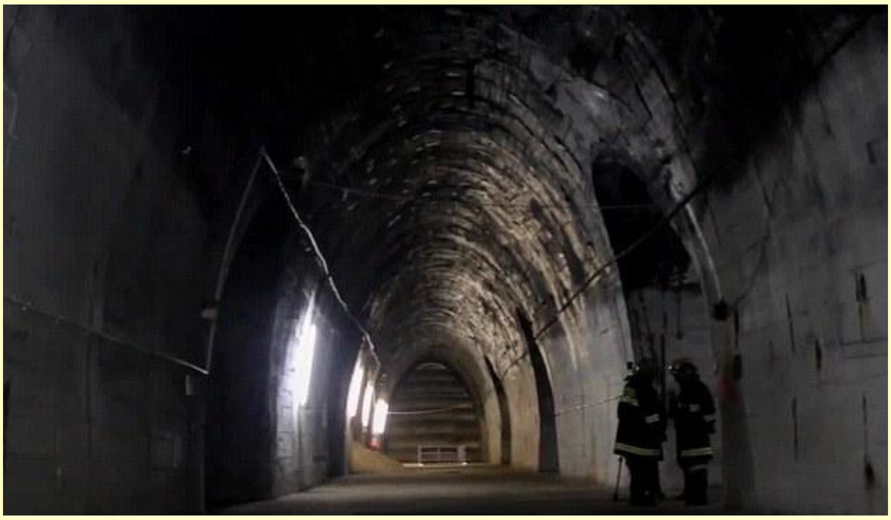
Such was the importance of the underground facilities that Heinrich Himmler, head of the SS and one of Hitler's key aides, visited to oversee them.

Kammler was officially said to have committed suicide after the war. But according to John Richardson, supported by declassified documents from the Counter Intelligence Corps (CIC), he was interrogated by Richardson's father and then taken to the US as part of Operation Paperclip, which gathered Nazi scientists who could contribute to US weapons programs.

Kammler is believed to have lived on the St Georgen site towards the end of the war; his last known headquarters was in an area that the US army took over in May 1945.

The Americans discovered the Bergkristall facility but had to relinquish it to the Russians two months later under an agreement to divide Austria into allied military zones.

The Russian army plundered the factory, removed all the technology and then destroyed and filled in the bunkers. The second part of the site, which Sulzer has discovered, seems to have remained unnoticed by both the Americans and the Russians.



Sulzer's excavation was stopped last Wednesday by local authorities, who demanded a permit for research on historic sites. But he is confident that digging can resume next month. "Prisoners from concentration camps across Europe were handpicked for their special skills — physicists, chemists or other experts — to work on this monstrous project and we owe it to the victims to finally open the site and reveal the truth," said Sulzer.

These Locations Are The 9 Most Radioactive Sites In The World

Source: http://www.viralnova.com/most-radioactive-places/

You definitely want to skip these places when planning your next vacation. Even if someone you know is beaming about the trip they took to one of these areas, it's *probably* from the radiation.

That's right. These are the most radioactive places on the planet. Enjoy your all-expenses-paid virtual voyage to them via the pictures below. You might not get the tan you've been meaning to work on, but at least you won't have to pack.

1. Sellafield, United Kingdom

This is another plutonium production plant gone awry. Sellafield, located in western England, leaks 8 million liters of contaminated waste into the sea on a daily basis. This makes the Irish Sea one of the most polluted bodies of water in the world.

2. Mediterranean Sea

For decades, the Italian mafia was accused of dumping hazardous waste into the Mediterranean Sea. Over 40 ships carrying loads of radioactive materials have gone missing since 1994, so you can expect to see a disastrous fallout sooner rather than later.

3. Somalian Coast

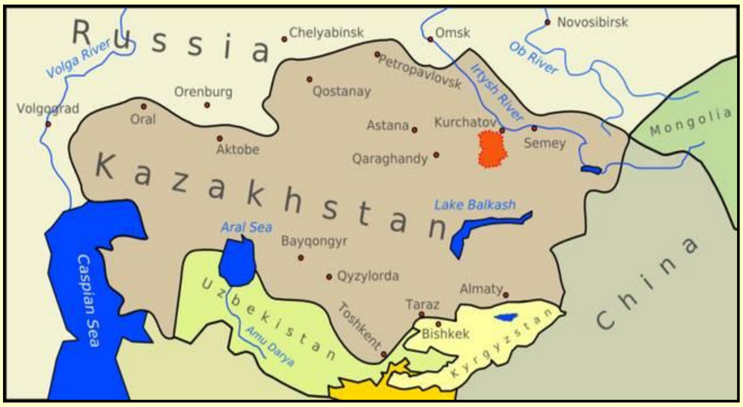
The Italian mafia is rumored to be using this coast as their dumping grounds, too. The lack of government regulations certainly doesn't help the people of Somalia. When a tsunami hit the area in 2004, discarded oil barrels dating back from the '90s were washing up on the shore.

4. Siberian Chemical Combine, Russia

Despite looking like a winter wonderland, this place is actually a nuclear hell. With over four decades of radioactive waste (about 125,000 tons) uncovered and easily spreadable by wind and weather, it seems like it's only going to get worse.

5. Semipalatinsk Test Site, Kazakhstan

This facility holds the record for the largest concentration of nuclear explosions in the world. That's 456 tests over 40 years from 1949 to 1989. To make matters worse, the site is surrounded by 700,000 people. It is estimated that nearly a third of those people have suffered health complications as a result of the radiation.



6. Mayak, Russia

Long before Chernobyl, Mayak was home to a disastrous nuclear explosion of its own. When all was said and done, the explosion released over 100 tons of radioactive waste. To make things worse, the disaster was kept a secret by the government until the 1980s. That's over 20 years of people living their daily lives in a totally toxic environment. Those poor souls!

7. Hanford Site, United States of America

Located in Washington, the Hanford Site was where plutonium was manufactured for the country's atomic bomb project and the Cold War. Most of the weaponry was not used, but the production alone did plenty of damage to its surrounding area. Leaks have contaminated the groundwater below it and, even though the site was decommissioned, it still holds much of the incredibly dangerous materials it was used to make.

8. Chernobyl, Ukraine

This is the place most people think of when they hear the phrase "nuclear disaster." The radiation released from the accident at the plant was over 100 times more than that of both bombs dropped on Japan. Over 6 million people were exposed to the radiation, and the death toll from the incident ranges from 4,000 to 93,000.

9. Fukushima, Japan

A 2011 earthquake resulted in what was the worst nuclear disaster since Chernobyl. Three of the plant's six reactors melted down, and much of the radiation leaked into the surrounding sea. Radioactive material linked to the disaster was found over 200 miles away from the plant.

DRDO develops mobile lab to screen troops in nuclear scenario

Source: http://www.tribuneindia.com/news/nation/drdo-develops-mobile-lab-to-screen-troops-in-nuclear-scenario/26753.html

With threat perception of terrorists using weapons of mass destruction increasing, the Defence Research and Development Organisation (DRDO - India) has developed a mobile truck mounted laboratory to screen troops in the field from the after effects of radiation and initiate remedial measures.

The chamber, termed as Mobile Whole Body Counter (MWBC) will do away with the necessity and the logistic impediment of evacuating soldiers from operational areas to rear echelons.

According to a bulletin issued by DRDO's Institute of Nuclear Medicine and Allied Sciences (INMAS), in case of radiological and nuclear accidents, some radio-nuclides are released, which contaminate the environment for extended periods of time due to their long life. Stating that terrorists are fast graduating towards chemical, biological radiological and nuclear (CBRN) terrorism and since Indian forces are constantly engaged in anti-terrorist and internal security duties in Jammu and Kashmir, the North-East and Maoist affected areas, the bulletin claims that the chances of use of radiation dispersal devices (RDD) by terrorists on Army installations are high.

Consequently, in order to keep soldiers fighting fit in the event of use of RDDs by terrorist outfits, each soldier suspected of being affected by radiation will be required to screen for radioactive contamination. This would help mitigate any panic in the unit concerned as well monitor therapeutic response.

Polonium found in nuclear-reactors; difficult to get, very lethal

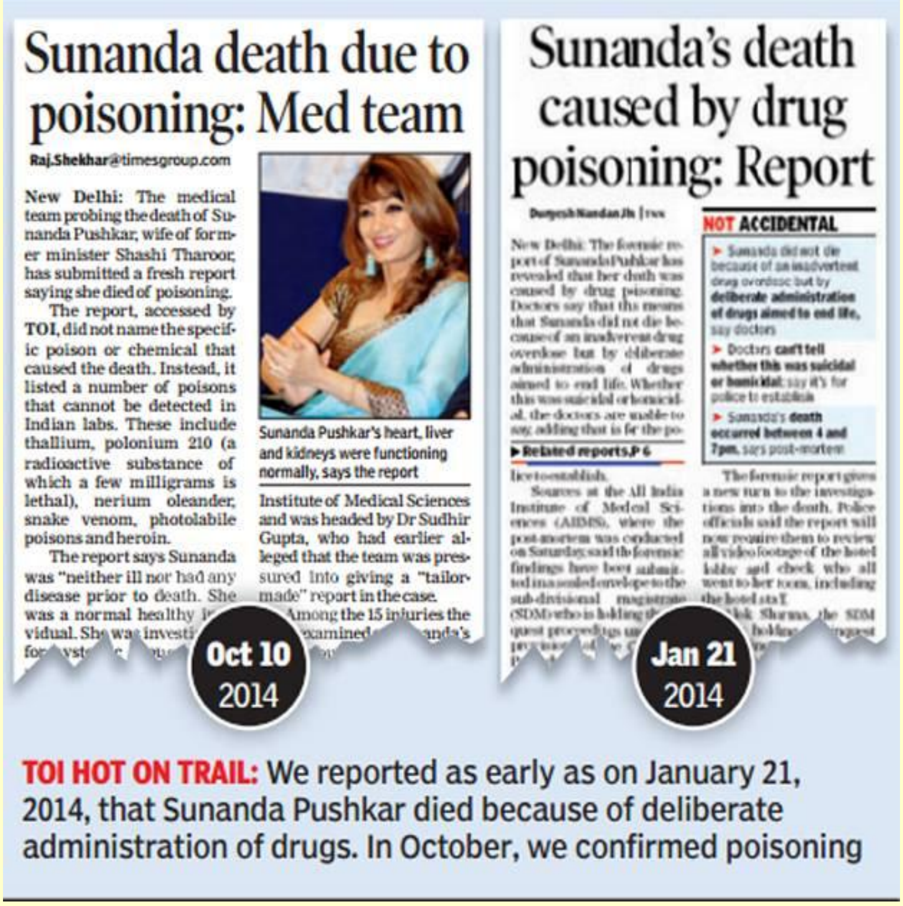
Source: http://timesofindia.indiatimes.com/city/delhi/Polonium-found-in-nuclear-reactors-difficult-to-get-very-lethal/articleshow/45784870.cms

Jan 07 – **One of the poisons experts suspect may have caused Sunanda's death is polonium-210, a toxin thousands of times more deadly than cyanide. How was such a rare and difficult-to-procure substance used?** Although discovered in 1898 by Marie Curie, it was not known much outside the nuclear power and arms industry. But this obscurity was destroyed when two famous cases of polonium poisoning rocked the world. One was that of Yasser Arafat, the legendary Palestinian leader who died in 2004. Investigations by Swiss scientists showed in 2013 that the cause of death was probably polonium poisoning.

Then in 2006, a Russian spy, Alexander Litvinenko, who had fallen foul of Russian authorities and fled to London, was murdered after he drank tea laced with polonium. The case caused an international sensation and led to diplomatic tension.

This radioactive element is produced as a by-product in nuclear fission reactions (in reactors) and occurs in very minute quantities in nature, including in tobacco. It is estimated by the US Nuclear Regulatory Commission that only about 100 grams is produced in a year in the world's nuclear reactors. It is very tightly regulated and experts believe that it will be virtually impossible for a lay person to either make it or acquire it.

Polonium is 250,000 times more deadly for humans than hydrogen cyanide. It's mode of action is not chemical interaction but rather the fact that it emits a steady stream of alpha particles, that is, doubly charged particles that destroy organs and tissue.



Sunanda death due to poisoning: Med team

Raj.Shekhar@timesgroup.com

New Delhi: The medical team probing the death of Sunanda Pushkar, wife of former minister Shashi Tharoor, has submitted a fresh report saying she died of poisoning.

The report, accessed by TOI, did not name the specific poison or chemical that caused the death. Instead, it listed a number of poisons that cannot be detected in Indian labs. These include thallium, polonium 210 (a radioactive substance of which a few milligrams is lethal), nerium oleander, snake venom, photolabile poisons and heroin.

The report says Sunanda was "neither ill nor had any disease prior to death. She was a normal healthy in[illegible]vidual. She was investi

Sunanda Pushkar's heart, liver and kidneys were functioning normally, says the report

Institute of Medical Sciences and was headed by Dr Sudhir Gupta, who had earlier alleged that the team was pressured into giving a "tailor-made" report in the case.

Among the 15 injuries the [illegible] examined [illegible]anda's

Oct 10 2014

Sunanda's death caused by drug poisoning: Report

Durgesh Nandan Jha | TNN

New Delhi: The forensic report of Sunanda Pushkar has revealed that her death was caused by drug poisoning. Doctors say that this means that Sunanda did not die because of an inadvertent drug overdose but by deliberate administration of drugs aimed to end life. Whether this was suicidal or homicidal, the doctors are unable to say, adding that is for the police to establish.

▶ Related reports, P 6

Sources at the All India Institute of Medical Sciences (AIIMS), where the post-mortem was conducted on Saturday, said the forensic findings have been submitted in a sealed envelope to the sub-divisional magistrate (SDM) who is holding the inquest proceedings un[illegible]

The forensic report gives a new turn to the investigations into the death. Police officials said the report will now require them to review all video footage of the hotel lobby and check who all went to her room, including the hotel staff.

Alok Sharma, the SDM [illegible] holding [illegible] inquest

NOT ACCIDENTAL

- Sunanda did not die because of an inadvertent drug overdose but by **deliberate administration of drugs aimed to end life,** say doctors
- Doctors **can't tell whether this was suicidal or homicidal;** say it's for police to establish
- Sunanda's **death occurred between 4 and 7pm,** says post-mortem

Jan 21 2014

TOI HOT ON TRAIL: We reported as early as on January 21, 2014, that Sunanda Pushkar died because of deliberate administration of drugs. In October, we confirmed poisoning

WHAT IS IT

Po 84 Polonium

Polonium, a rare and highly radioactive element, was discovered by Marie and Pierre Curie in 1898. If ingested, a minuscule amount can prove lethal. Experts say once it enters bloodstream, polonium's deadly effects are nearly impossible to stop

WELL-KNOWN CASES

YASSER ARAFAT | Traces of polonium were detected in clothes and personal belongings of the late Palestinian leader in July 2012. He died on 11 November 2004 of uncertain causes. However, it was not confirmed whether Arafat's death was caused by radiation

ALEXANDER LITVINENKO | The Russian dissident died in London in 2006. He is said to be first confirmed victim of lethal polonium-210-induced acute radiation syndrome

It doesn't have the capacity to cross the outer layer of human skin. But if inhaled or ingested or absorbed, it will generate the lethal alpha radiation inside the body, progressively destroying everything. If taken in, polonium can exist in human bodies for 30 to 50 days. All this while, it will keep burning up organs, tissues, vessels and so on, causing a rapid and painful decline to death.

Since cases of polonium poisoning are rare, not much is known about treatment although some successful experiments have been done with mice.

The worrying part is that this poison can't be procured so easily. Experts and veteran cops say this leads to the question about the stature of the person behind the murder of if there was an agency - maybe a foreign hand - involved.

Eventually, the case may have to be transferred to the special cell or crime branch because it would require a higher level of skill set and infrastructure to carry out the probe.

The cops will begin by serving notice to all the witnesses under section 160 CrPC to join investigations and will question them "differently" and not merely record statements.

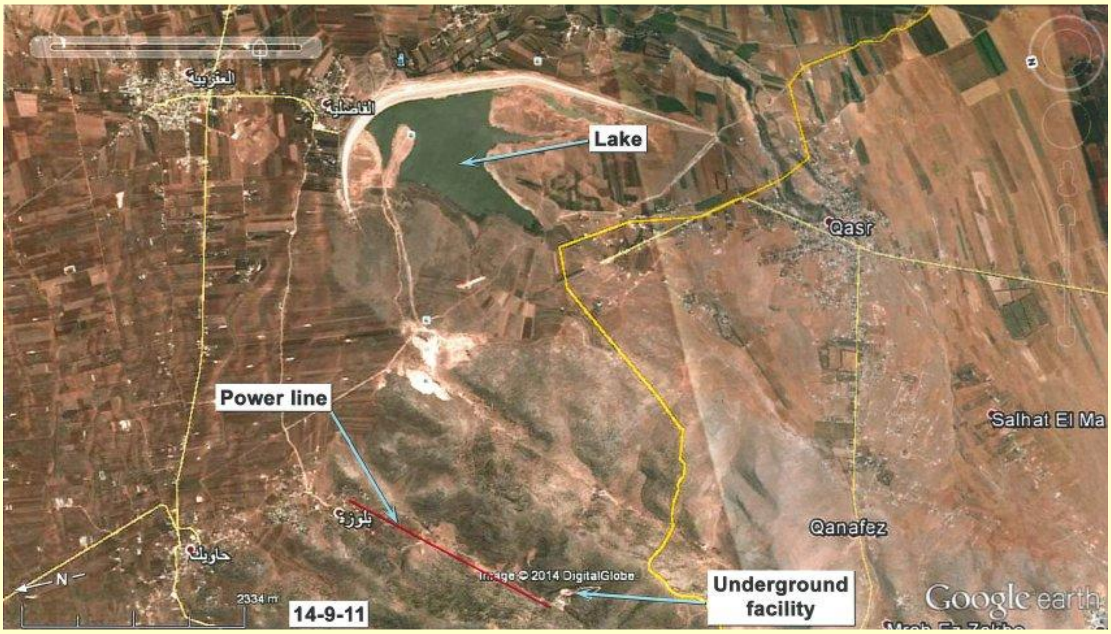
The cops will have to analyze the call details of Sunanda Pushkar's number ending with 007 along with the details of Shashi Tharoor, his secretary and others present in the room.

The cops will now also need to obtain the dump data - all mobile numbers present in an area - of the cell ID around Leela hotel and analyze each of the numbers which can run into few thousands, an officer said.

The cops will now re-analyze the CCTV footages and also question the hotel staff presents on that day. The cops said they were verifying reports about some of the hotel staff having quit. The cops still haven't confirmed if they have got anything out of the list of passengers who travelled in and out of Delhi on and around January 17. The destinations states being Pakistan and Dubai, sources said.

Great news: Bashar al-Assad still developing nuclear weapons

Source: http://hotair.com/archives/2015/01/12/great-news-bashar-al-assad-still-developing-nuclear-weapons/



This satellite image shows the Qusayr site's link to the power grid, one of many details of the site which have intelligence officials worried that it could be a facility for the construction of a nuclear weapon.

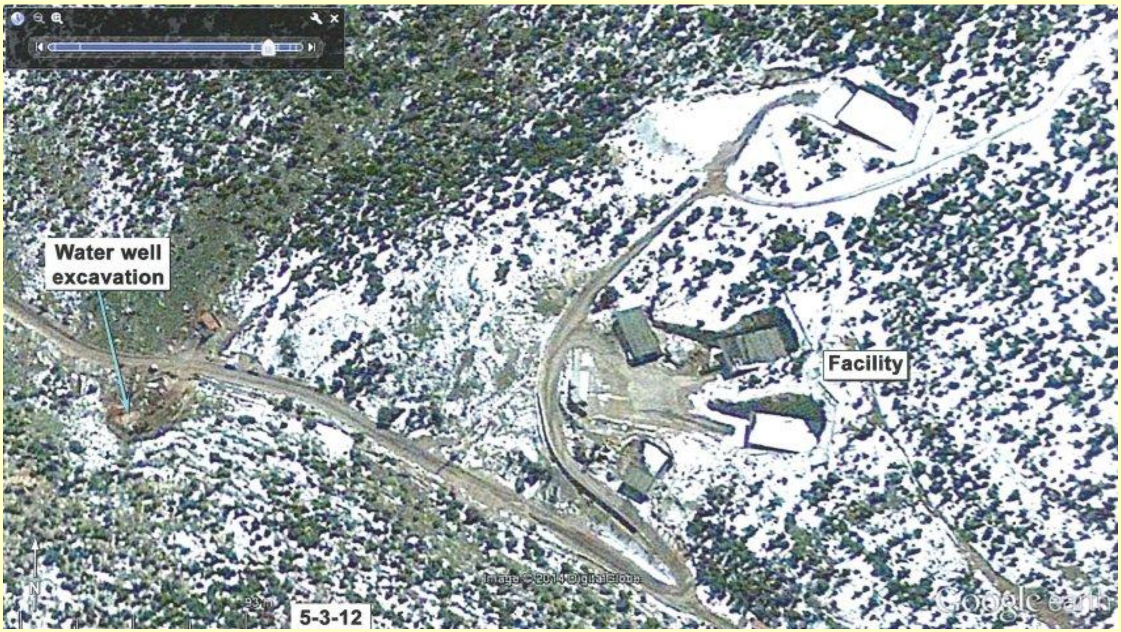
There is some troubling news out of the Levant this week, as if the West needed any more of that. **According to a thorough report in *Der Spiegel* based on documents obtained from "Western intelligence agencies," Bashar al-Assad's Syria is busily developing a nuclear weapon.**

"Analysts say that the Syrian atomic weapon program has continued in a secret, underground location," *Der Spiegel* reported. "According to information they have obtained, approximately 8,000 fuel rods are stored there. Furthermore, a new reactor or an enrichment facility has very likely been built at the site — a development of incalculable geopolitical consequences."

According to intelligence agency analysis, construction of the facility began back in 2009. The work, their findings suggest, was disguised from the very beginning, with excavated sand being disposed of at various sites, apparently to make it more difficult for observers from above to tell how deeply they were digging. Furthermore, the entrances to the facility were guarded by the military, which turned out to be a necessary precaution. In the spring of 2013, the region around **Qusayr** saw heavy fighting. But the area surrounding the project in the mines was held, despite heavy losses suffered by elite Hezbollah units stationed there.

The **most recent satellite images** show six structures: a guard house and five sheds, three of which conceal entrances to the facility below. The site also has special access to the power grid, connected to the nearby city of Blosah. A particularly suspicious detail is the deep well which connects the facility with Zaita Lake, four kilometers away. Such a connection is unnecessary for a conventional weapons cache, but it is essential for a nuclear facility.

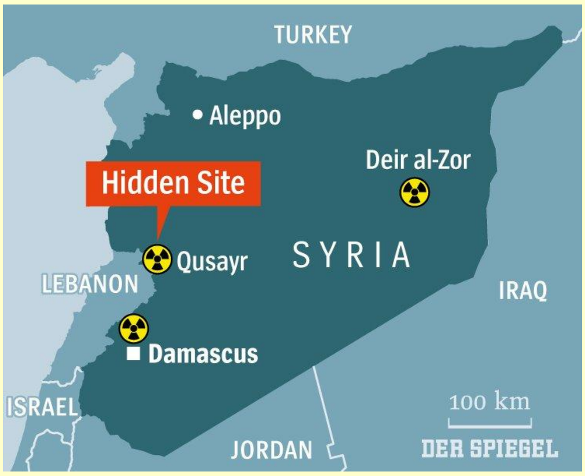
This image purports to show the site where a well has been dug. The well connects the facility with Zaita Lake, four kilometers away. Such a connection is unnecessary for a conventional weapons cache, but it is essential for a nuclear facility.



But the clearest proof that it is a nuclear facility comes from radio traffic recently intercepted by a network of spies. A voice identified as belonging to a high-ranking Hezbollah functionary can be heard referring to the "atomic factory" and mentions Qusayr. The Hezbollah man is clearly familiar with the site. And he frequently provides telephone updates to a particularly important man: Ibrahim Othman, the head of the Syrian Atomic Energy Commission.

The report further indicates that the two remaining members of the old Axis of Evil — North Korea and Iran — are busily aiding Syria in its quest to replace Saddam Hussein's Iraq as a member of that exclusive club. *Der Spiegel* revealed that intercepted conversations indicate that members of Iran's Revolutionary Guard and Yongbyon nuclear reactor developer Chou Ji Bu (thought to have been purged by the government in Pyongyang) are involved in the project to develop a Syrian bomb.

This revelation takes on an added level of urgency as Assad has a recent history of using weapons of mass destruction on civilian populations, and of doing so even amid global condemnation and in defiance of international agreements to which his government consented. Should Syria construct a fissionable device, there is every reason to believe that Assad's government would deploy nuclear weapons against areas controlled by anti-Damascus rebels. It is unlikely Assad can be dissuaded from using such a weapon via traditional methods of deterrence.



The revelation that Assad is developing an atomic device, and is doing so with the likely aid of North Korea and Iran, is about as thorough a repudiation of Barack Obama's approach to the region one could imagine. Obama was handed the reins of American foreign policy under the delusional premise that rogue actors only needed to be engaged diplomatically in order to persuade them to forego their national interests.

That was always a fantasy, but do not expect those who support it to abandon this faulty premise so quickly. Faith-based beliefs do not die easy deaths.

This is an embarrassment for the Obama government, but it is also a clear threat to American national interests in the region and globally. Let's hope that the White House and the press do not attempt to shield the president from humiliation by pretending this dangerous situation does not exist.

Moldova: Police Arrest Seven Uranium Smuggler Suspects

Source: http://www.eurasiareview.com/11122014-moldova-police-arrest-seven-uranium-smuggler-suspects/

Dec 11 2014 – Seven members of an organized criminal group suspected of smuggling uranium have been arrested in Moldova, INTERPOL said on Thursday.

Following an investigation into the activities of the criminal group, Moldova Police and the General Prosecutor's Office carried out searches in the capital Chisinau and two other towns, where they seized 200 g of uranium-238, 1 kg of mercury and 1 kg of an unidentified radioactive material. Mobile phones, computers and accounting documents were also recovered.

Support to the operation was provided by the INTERPOL National Central Bureau (NCB) in Chisinau and the US Federal Bureau of Investigation (FBI).

Police said the uranium, smuggled into the country by train, has a value of EUR 1.6 million. The radioactive substance can be used in the production of dirty bombs, which could cause massive destruction in the hands of a terrorist group.

The seven suspects arrested are aged 32 to 75 and are members of an organized criminal network with specialized knowledge of radioactive substances. Moldova police are liaising with their counterparts in the region to identify other members of the group.

"INTERPOL applauds the skillful work of the Moldova police in preventing such a dangerous product from potentially falling into the hands of terrorists," said INTERPOL's Director of Counter-Terrorism, Public Safety and Maritime Security, Pierre St Hilaire.

"This seizure, combined with INTERPOL's work through its counter-terrorism initiatives Project Geiger and Operation Fail Safe which enhance the capacity of our member countries to deny terrorists access to these weapons, is an important step forward in reinforcing the UN's global strategy to prevent terrorists from developing or acquiring nuclear, chemical or biological weapons," added Mr St Hilaire.

Moldova
Romania
Ukraine
Chisinau
Black Sea

Through its Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) initiatives including Project Geiger and Operation Fail Safe, INTERPOL supports law enforcement efforts to prevent and detect the illicit trafficking of uranium and other potentially dangerous materials worldwide. At the 2012 and 2014 Nuclear Security Summits held in Korea and The Netherlands, world leaders encouraged all countries to share information on individuals involved in the trafficking of nuclear and other radioactive materials via INTERPOL.

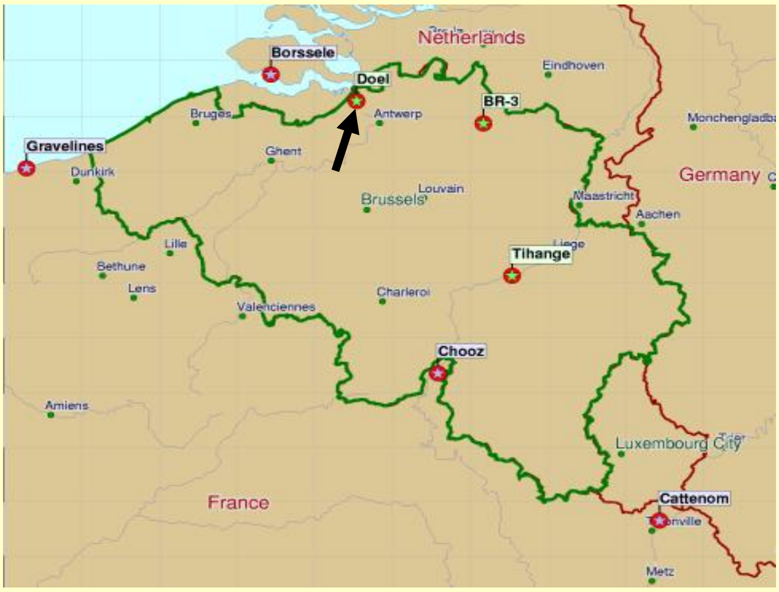
"This successful operation highlights the need for a coordinated international approach to prevent criminals from travelling across borders with radiological substances and either using them to create weapons or selling them to the highest bidder," said Jeffrey Muller, Assistant Director of INTERPOL's CBRNE team.

Drone spotted over Belgium nuclear plant

Source: http://zeenews.india.com/news/world/drone-spotted-over-belgium-nuclear-plant_1518054.html

Dec 21, 2014 – **An unexplained drone was spotted flying over a Belgium nuclear facility, local authorities have said, a day after one of the plant's reactors came back on line after a four-month closure caused by sabotage.**

The mystery appearance by an unmanned aircraft, on which Belgian authorities refused to provide much detail, resembles a spate of similar drone sightings over nuclear plants in neighbouring France this autumn.



Around 20 unidentified drones have been spotted over nuclear plants since October throughout France.

"We can confirm that the East Flanders prosecutor's office has opened an investigation into a drone flight over the Doel nuclear plant," a spokesman for the investigation told Belga news agency.

"We will not provide further information for the time being," the spokesman added, hours after the plant's operator, GDF-Suez unit Electrabel, first disclosed the incident, which took place early yesterday.

The imposing Doel nuclear site sits on a riverbank near the North Sea about 25 kilometres north of Antwerp. It holds four of Belgium's seven reactors.

One of those reactors, Doel 4, was shut urgently in August after a leak, caused by tampering, gushed out 65,000 litres of oil lubricant.

A steam turbine weighing 1,700 tonnes was severely damaged by the loss of lubricant, requiring a 30-million-euro (USD 37-million) repair job that was carried out in Germany.

Belgian prosecutors have refused to confirm the sabotage as an act of terrorism, without excluding it either.

Two other Belgian reactors still remain shut, both due to cracks in their reactor containment vessels.

To face a potential shortfall in power, Belgium's government on Thursday said plans to close the Doel site's two oldest reactors, both nearly four decades old, would be suspended.

The Doel 1 and 2 reactors were due to be the first to be shut as part of Belgium's planned phase out of nuclear power by 2025, but the government said it would seek to keep them operating.

Nuclear plants account for 55 per cent of Belgium's power generation, and the loss of over half of the country's nuclear power has caused concerns of a shortage or even a blackout.

Regulators have put in place special measures to help meet Belgium's needs this winter.

Britain's nuclear power plants 'could be attacked by drones'

Source: http://nuclearpower.einnews.com/article/240874731/4p0hhtusApswUhLs

Britain's nuclear power plants are highly vulnerable and they 'could be attacked by drones', according to a report by an atomic expert.

"In each of the four attack scenarios that I examined, the plant fared very badly indeed — if these scenarios had been for real, then there would have been the potential for a major radioactive release," said British atomic expert John Large in his report.

The report followed a number of unexplained, but apparently co-ordinated, flights of tiny, unmanned vehicles over French nuclear installations, the Independent reported.

"The grave issues uncovered there, said Mr. Large, were equally relevant to the U.K.'s 16 operational reactors, which generate about 18 per cent of the country's electricity," the paper said.

Existing nuclear power plants, Mr. Large said, were not designed to counter the threat of "near-cyborg technology".

Mr. Large's modelling showed that the **"flexible access and manoeuvrability of the drones" means that they were able to fly over and twist around physical barriers that "belonged to a different age".**

Even small, battery-powered drones can lift 10 or more kilograms of cargo, while vehicles available in high street hobbyist shops are "certainly not toys but machines capable of following and discharging intelligent commands".

British officials have looked at Mr. Large's evidence and forwarded it to the Office for Nuclear Regulation, but have not requested a copy of the report itself, the paper said.

Two men and one woman were arrested near the Belleville-sur-Loire reactor in the Cher region, south of Paris, last month after using remote-controlled vehicles in a restricted area within 200 metres of the plant. However, they were released after it emerged that they were simply model aircraft enthusiasts operating in an unfortunate location.

Such incidents have occurred in restricted airspace over 13 French nuclear plants since October. On one evening, there were five co-ordinated flyovers at stations located hundreds of miles apart.

Although the vehicles are believed to be commercial and civilian in nature, there are fears that a terrorist group might be using them for surveillance to evaluate the security of France's 19 nuclear sites, the paper said.

Experts in Germany have warned that the drones could identify weaknesses before sending in an attack helicopter to blow apart thick cement walls. The subsequent meltdown then has the potential to spread radiation up to 180 miles.

David Lowry, a consultant researcher for the World Institute for Nuclear Security in Vienna, said, "My general view is that all nuclear facilities are at risk of malevolent terrorist attack."

Citing a senior Whitehall source, the paper said that the government has increased its focus on nuclear security against "all threats".

EDITOR'S COMMENT: Quite melodramatic report **BUT** if we consider it via a different approach then such scenarios might be serious:

- Small drones : Damage = minor; global press impact = big;
- Big hobbyist drones : Damage = significant; global press index = huge;
- Commercial airctaft : Damage = major/catastrophic; global press impact = immense.

▶ **Watch this video:** https://www.youtube.com/watch?v=4q35xHzjxB0#t=12

Realistic radiation detection training without using radioactive materials

Source: http://www.homelandsecuritynewswire.com/dr20150115-realistic-radiation-detection-training-without-using-radioactive-materials

The LLNL Spectroscopic Injection Pulser prototype directly injects signals into radiation detection equipment, exactly like a real radiation source. This laboratory-scale prototype will support miniaturization to something near the size of a cellphone.

Jan 15 – Training of first responders on the hazards of actual radiological and nuclear threats has been challenged by the difficulties of adequately representing those threats. Training against such threats would involve using hazardous, highly radioactive materials, experiencing actual radiation doses in training, or require the distribution of radioactive material over a large geographical area. **To avoid these issues in exercises to train responders, surrogate radioactive materials have been used. However, these materials do not completely represent real threats due to their non-hazardous size and inability to be geographically distributed.**

An LLNL release reports that Lawrence Livermore National Laboratory (LLNL) researchers have solved the problem by developing a new technology that provides realistic radiation detection training by directly injecting simulated radiation signals into the analog amplifier of the real detectors used by first responders and inspectors. The Spectroscopic Injection Pulser (SIP) will yield training results that are indistinguishable by detection instruments from actual radiation sources.

A handheld radiation identifier, such as that pictured here, connected to the SIP would respond just as if a real radiation source were present.

This technology simulates the presence of live radioactive sources by providing instrument responses such as count rates, energy fingerprints (spectra) and dose rates. Such responses would normally only occur if the instruments were close to a real radiation source.

Depending on the user's requirements, training goals, and radiation scenarios, high-fidelity synthetic radiation data are developed and transmitted to the SIP, which can be attached to the exterior or integrated into actual instruments. The location of the instrument and time of measurement are used to calculate the expected signal from an actual radiation source, and that signal is injected into the detection instrument pulse-by-pulse, just as would be observed by the instrument in a real operation.

With the SIP running in parallel to the instrument, the background environment also would be measured, as would be the case in a real response. This provides first responders with a much more realistic experience.

After training, the SIP can either be switched off or removed from the system's exterior, returning the radiation detector to normal operations.

The SIP's wireless communication capabilities can provide trainers with broader command and control options often needed during an exercise. For example, instructors can observe the actions of team members as they deal with realistic scenarios, provide guidance, monitor health physics, communicate information and data to command centers and deliver technical real-time reach-back guidance. For certain training scenarios, virtual samples could be collected and transmitted to a laboratory for analysis.

"This technology could dramatically improve responder preparedness against more realistic scenarios, including better representation of the actual hazards, while not requiring those same responders to become, for example, certified radioactive or other hazardous material handlers," said Steven Kreek, leader of the Nuclear Detection and Countermeasures R&D Program in LLNL's Global Security Directorate and part of the Lab team that invented the technology. "By working directly with instrument manufacturers, we're hoping they will design future response instrumentation to interface directly with our SIP."

The "Double Nuclear threat" posed by ISIS

Source: http://i-hls.com/2015/01/double-nuclear-threat-posed-isis/

Dirty Bomb or Nuclear suitcase? These are according to experts the options ISIS seeks now for performing huge attacks in the west.

Last year, an ISIS militant has claimed that the group is now in possession of a nuclear weapon. A British ISIS member now based in Syria, claimed on social media that the group obtained the uranium from Mosul University and now possesses a "dirty bomb" that it is now considering detonating in a public area.

Such a device is aimed at spreading radioactive material in a big area.

But in recent days another threat has been studied by intelligence bodies. **This threat is in the form of "suitcase nuke".**

This is the experts say is a very compact and portable nuclear weapon and could have the dimensions of 60 x 40 x 20 centimeters or 24 x 16 x 8 inches. The smallest possible bomb-like object would be a single critical mass of plutonium (or U-233) at maximum density under normal conditions.

The warhead of a suitcase nuke or suitcase bomb consists of a tube with two pieces of uranium, which, when rammed together, would cause a blast. Some sort of firing unit and a device that would need to be decoded to cause detonation may be included in the "suitcase."

Another portable weapon is a "backpack" bomb. The Soviet nuclear backpack system was made in the 1960s for use against NATO targets in time of war and consists of three "coffee can-sized" aluminum

canisters in a bag. All three must be connected to make a single unit in order to explode. The detonator is about 6 inches long. It has a 3-to-5 kiloton yield, depending on the efficiency of the explosion. It's kept powered during storage by a battery line connected to the canisters.

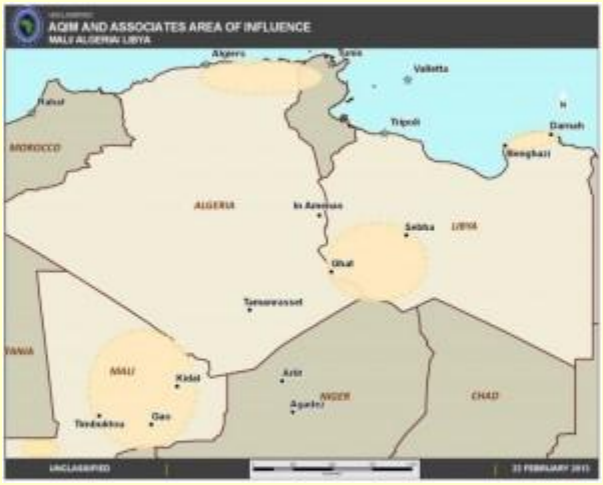
After the Soviet Union was disassembled, there were reports that some "Suitcase Nukes" were stolen and are offered on the international black market. ISIS, according to the experts, is an organization that will not hesitate to use such a device.

Algeria concerned Al Qaida or ISIL could be smuggling uranium

Source: http://www.worldtribune.com/2015/01/18/algeria-concerned-al-qaida-isil-smuggling-uranium/

Jan 18 – **Algeria plans to establish a network to monitor the flow of nuclear material along its borders.**

Officials said the government has approved a plan to install equipment to inspect incoming goods for radiation. They said the equipment would be installed **at border posts amid concern that Al Qaida or Islamic State of Iraq and Levant could be smuggling nuclear or radioactive material through Algeria to such states as Mali and Libya.**



"They will be deployed at port and airport platforms for the monitoring of all product and equipment, which may introduce polluted materials and possibly may represent a radioactive source," Algerian customs chief Mohammed Abdul Bouderbala said.

In a briefing on Dec. 22, Bouderbala said border posts would include customs units that specialize in detecting nuclear or radioactive material. He said the units would consist of officers trained in cooperation with Algeria's Atomic Energy Commission.

"The project will result in the purchase of new screening equipment, which will be added to those set up at port and airport checkpoints, requiring qualified personnel for the use of these equipments," Bouderbala said.

Officials said **Al Qaida and ISIL were believed to be seeking to acquire nuclear equipment, including uranium.** They said Algeria might serve as a waystation for smuggling efforts from Mali to Libya.

The project to track nuclear material has included the Algerian Army and police. Officials said the new customs units would significantly enhance border security.

"They will be bolstered particularly along the borders of Mali and Libya to deal with threats," Bouderbala said.

Three minutes and counting

By Lynn Eden, Robert Rosner, Rod Ewing, Sivan Kartha, Edward "Rocky" Kolb, Lawrence M. Krauss, Leon Lederman, Raymond T. Pierrehumbert, M. V. Ramana, Jennifer Sims, Richard C. J. Somerville, Sharon Squassoni, Elizabeth J. Wilson, David Titley and Ramamurti Rajaraman

Source: http://thebulletin.org/three-minutes-and-counting7938

Jan 19 – ***Editor's note:*** *Founded in 1945 by University of Chicago scientists who had helped develop the first atomic weapons in the Manhattan Project, the* Bulletin of the Atomic Scientists *created the Doomsday Clock two years later, using the imagery of apocalypse (midnight) and the contemporary idiom of nuclear explosion (countdown to zero) to convey threats to humanity and the* *planet. The decision to move (or to leave in place) the minute hand of the Doomsday Clock is made every year by the* Bulletin's *Science and Security Board in consultation with its Board of Sponsors, which includes 17 Nobel laureates. The Clock has become a universally recognized indicator of the world's vulnerability to catastrophe from nuclear weapons, climate change, and new technologies emerging in other domains.*

From: The *Bulletin of the Atomic Scientists* Science and Security Board

To: Leaders and citizens of the world

Re: It is only three minutes to midnight

In 2015, unchecked climate change, global nuclear weapons modernizations, and outsized nuclear weapons arsenals pose extraordinary and undeniable threats to the continued existence of humanity, and world leaders have failed to act with the speed or on the scale required to protect citizens from potential catastrophe. These failures of political leadership endanger every person on Earth.

In 1984, as the United States began a major defense build-up that included the pursuit of a potentially destabilizing ballistic missile defense system, relations between the United States and the Soviet Union reached an icy nadir. "Every channel of communications has been constricted or shut down; every form of contact has been attenuated or cut off. And arms control negotiations have been reduced to a species of propaganda," the *Bulletin* wrote then, in explaining why the hands of the Doomsday Clock had been moved to three minutes to midnight, the closest they had been to catastrophe since the early days of above-ground hydrogen bomb testing.

Today, more than 25 years after the end of the Cold War, the members of the *Bulletin of the Atomic Scientists* Science and Security Board have looked closely at the world situation and found it highly threatening to humanity—so threatening that the hands of the Doomsday Clock must once again be set at three minutes to midnight, two minutes closer to catastrophe than in 2014.

Despite some modestly positive developments in the climate change arena in the past year, reflecting continued advancement of renewable energy technologies, current efforts are entirely insufficient to prevent a catastrophic warming of Earth. Absent a dramatic course correction, the countries of the world will have emitted enough carbon dioxide and other greenhouse gases by the end of this century to profoundly transform Earth's climate, harming millions upon millions of people and threatening many key ecological systems on which civilization relies.

At the same time, efforts to reduce world nuclear arsenals have stalled. The disarmament process has ground to a halt, with the United States and Russia embarking on massive programs to modernize their nuclear triads—thereby undermining existing nuclear weapons treaties—and other nuclear weapons holders joining in this expensive and extremely dangerous modernization craze.

The science is clear: Insufficient action to slash worldwide emissions of greenhouse gases can produce global climatic catastrophe. Even a so-called "limited" nuclear weapons exchange will produce massive casualties and severe effects on the global environment. We implore the political leaders of the world to take coordinated, quick action to drastically reduce global emissions of heat-trapping gases, especially carbon dioxide, and shrink nuclear weapons arsenals.

We also implore the citizens of the world to demand action from their leaders. The threat looms over all of humanity. Humanity needs to respond now, while there is still time.

A climate catastrophe looms—but is not inevitable.

According to US government environmental scientists, 2014 was the hottest year in 134 years of record keeping. Nine of the 10 warmest years on record have all occurred since 2000. This pattern is deeply disconcerting.

In November 2014, the Intergovernmental Panel on Climate Change (IPCC) released its Synthesis Report encapsulating the key findings of its just-completed multivolume assessment of climate change. The IPCC reported that global warming is unequivocal and unprecedented and already responsible for widespread damage. It warned that warming—if unchecked by urgent and concerted global efforts to greatly reduce greenhouse gas emissions—would reach 3 to 8 degrees Celsius (about 5.5 to 14.5 degrees Fahrenheit) by the end of the century.

This may seem like a modest rise in the average global temperature. After all, people at a given location often experience much greater temperature swings in the course of a single day. But that is a local variation, not a change in the average temperature of the surface of the entire planet. A similarly “modest” global average warming of 3 to 8 degrees Celsius brought Earth out of the frigid depths of the last ice age, utterly transforming the surface of the planet and in the process making it hospitable to the development of human civilization. To risk a further warming of this same magnitude is to risk the possibility of an equally profound transformation of Earth’s surface—only this time the planet’s hospitality to humanity can by no means be taken for granted.

US Secretary of State John Kerry spoke passionately of the threat at the recent United Nations Framework Convention on Climate Change negotiations in Lima, Peru. After reciting the year’s litany of weather-related disasters—record-breaking droughts, floods, and storms, mere portents of what can yet be expected—Kerry lamented that the world is “on a course leading to tragedy.”

It is no comfort that Kerry was merely echoing warnings from the 1992 Earth Summit. In the more than two decades since then, human society has shown alarmingly little commitment to curbing greenhouse gas emissions. While efforts to transition to low-emission sources of energy have yielded some encouraging results, the net effect has been far too small, when compared with the scientific requirements for addressing the climate challenge. Emissions rose much more quickly in the 2000-2010 period than in any of the preceding decades, while investments have poured into fossil fuel infrastructure at a rate ofmore than $1 trillion per year, complemented by additional hundreds of billions of dollars in fossil fuel subsidies.

Expectations for earnest action from our leaders have fallen so far that some observers are relieved to see even nominal attention paid to climate change. A recent joint announcement on climate goals between the United States and China is a case in point. Under the agreement, the United States would cut greenhouse gas emissions 26 to 28 percent from 2005 levels by the year 2025; this proposal was lauded as a “historic step” and a “game changer.” Few observers pointed out that the United States was actually back-tracking on a target presented by President Obama five years ago in Copenhagen, when he offered a 30 percent cut by 2025. And the Chinese side of the agreement was remarkable for its vagueness, offering to "peak" its carbon dioxide emissions by 2030, without saying what that peak would be.

The IPCC has made clear that a climate catastrophe is not inevitable. The world has technological and policy options available at entirely acceptable costs. Time is short, but it has not yet run out. Our leaders and our institutions of global cooperation and governance can yet rise to the challenge. But rise they must, and quickly.

As Secretary Kerry said in Lima, "whether we’re able to promptly and effectively address climate change is as big a test of global leadership, of the international order—such as we call it—it’s the biggest test of that that you’ll find.”

It's a test that world leaders must face head on, immediately.

Nuclear modernization programs threaten to create a new arms race.

Although the United States and Russia have reduced their arsenal sizes from Cold War heights, the pace of reduction has slowed dramatically in recent years. According to Hans Kristensen of the Federation of American Scientists, “in terms of warhead numbers, the Obama administration so far has cut the least warheads from the stockpile" of any post-Cold War administration.

Meanwhile, as they slow the pace of disarmament, the nuclear weapon states have given other strong indications that they are committed to retaining nuclear weapons for the indefinite future. The most worrying evidence of this commitment: huge and expensive programs of nuclear arsenal modernization that all nuclear weapon states are pursuing. These massive modernization efforts undermine the nuclear weapons states' promise to disarm, a central tenet of the Nuclear Non-Proliferation Treaty (NPT), and they therefore also threaten the global nonproliferation regime.

Despite a policy of reducing reliance on nuclear weapons, the United States is engaged in a massive overhaul of its nuclear weapons systems and infrastructure. While the *Bulletin* supports efforts to keep existing weapons safe and secure, "modernizing" American nuclear weapons systems would fundamentally alter each leg of the US nuclear weapons triad at astronomical cost: some $355 billion over the next decade and $1 trillion or more over 30 years. Russia is also upgrading its triad, and recent Russian statements on nuclear weapons have emphasized the importance of nuclear missions, rather than de-emphasizing them. This is especially true for non-strategic nuclear weapons, which are currently not limited by any arms control agreements.

Other nuclear weapon states are also engaged in extremely costly nuclear modernization programs. The United Kingdom has decided to continue supporting its Trident nuclear missile submarine, and France is building its own next-generation delivery vehicle, an air-to-ground, nuclear-tipped missile. China is developing a new class of ballistic missile submarine with a new ballistic missile.

Meanwhile, countries outside of the Nuclear Non-Proliferation Treaty are also modernizing their nuclear arsenals. India plans to expand its nuclear submarine fleet, with the first submarine undergoing sea trials and the second one in the early stages of construction. It also tested what has been described as a nuclear-capable cruise missile. For its part, Pakistan appears to have commenced operations at its third plutonium production reactor. Perhaps more dangerously, it has developed a new, short-range, nuclear-capable missile called NASR, which has destabilized the already perilous nuclear situation in South Asia. Israel is also reportedly modernizing some of its undeclared nuclear forces, and North Korea continues its nuclear program without any of the restraints previously applied under the NPT.

As the world's nuclear nations engage in sweeping nuclear weapons modernization efforts, the gears in the machinery of nuclear disarmament seem to be grinding to a slow halt.

Three and a half years after New START entered into force, Russia reportedly has more warheads deployed than when the treaty became active. The United States has also increased its number of deployed warheads in recent months, although the total is still lower than in 2011. These increases in warhead levels are believed to be temporary, and we hope they do not imply a deliberate plan on the part of either country to enlarge its arsenal. Nevertheless, it is disappointing that neither superpower is moving toward the smaller strategic arsenals foreseen by New START with any alacrity. And the other nuclear-armed states are extremely unlikely to reduce their own arsenals until the United States and Russia bring their warhead numbers well below 1,000 each.

Arms control experts have long put faith in dialogue to keep the broader US-Russia relationship on an even keel, but these two countries—which own more than 90 percent of the world's nuclear warheads—cannot seem to agree even to talk. Amid unresolved accusations of violations on both sides of the Intermediate Nuclear Forces Treaty—an important but now threatened bulwark against the reintroduction of medium-range nuclear missiles to Europe—Russia announced it would not attend the 2016 Nuclear Security Summit, matching in some ways President Barack Obama's 2013 decision to call off a planned summit with Russian President Vladimir Putin. And limitations on non-strategic nuclear weapons seem to be off the discussion table indefinitely.

Within the nuclear nonproliferation regime, the failure to organize a conference on a weapons of mass destruction-free zone in the Middle East over the past five years will complicate efforts to make meaningful progress at the 2015 NPT Review Conference to be held this spring in New York. But this will be only the tip of an iceberg of dissatisfaction lurking under the surface of the conference. The nuclear weapon states have largely resisted broad-based efforts by non-weapons states to engage them in discussions on the humanitarian impact of nuclear weapons. The absence of any movement toward ratifying the Comprehensive Test Ban Treaty or negotiating a Fissile Material Cutoff Treaty in Geneva completes the dismal picture of a moribund world disarmament regime.

The innovative Nuclear Security Summits have had limited goals and therefore have accomplished little regarding military stockpiles of fissile materials or separated civilian plutonium. At the very least, countries should have been required to disclose the size of their stockpiles. But for all the positive publicity that has surrounded them, the Nuclear Security Summits have produced no binding agreements, and no requirements that countries disclose their nuclear activities.

There are far too many nuclear weapons in the world, and world leaders—particularly those in the United States and Russia—have failed to live up to their responsibility to control and reduce the nuclear threat.

The leadership failure on nuclear power.

Nuclear energy provides slightly more than 10 percent of the world's electricity-generating capacity, without emitting carbon dioxide. Depending on the type of fossil fuel displaced by the electricity nuclear power plants generate (that is, coal or natural gas), nuclear power plants help the world avoid approximately 0.5 gigatons of carbon emissions annually. But the international community has not developed coordinated plans to meet the challenges that nuclear power faces in terms of cost, safety, radioactive waste management, and proliferation risk.

Nuclear power is growing sporadically in regions that can afford it, sometimes in countries that do not have adequately independent regulatory systems. Meanwhile, several countries continue to show interest in acquiring technologies for uranium enrichment and spent fuel reprocessing—technologies that can be used to create weapons-grade fissile materials for nuclear weapons. Stockpiles of highly radioactive spent nuclear fuel continue to grow (globally, about 10,000 metric tonnes of heavy metal are produced each year). Spent fuel requires safe geologic disposal over a time scale of hundreds of thousands of years.

On Valentine's Day 2014, the world's only operating geologic repository for nuclear waste, the Waste Isolation Pilot Plant in southeastern New Mexico, experienced the accidental release of radioactivity to the surface. The accident also exposed workers to very low levels of radiation, and post-facto assessments of how it occurred revealed a poor safety culture within the plant and elsewhere within the nuclear complex. The facility is not expected to resume operations until 2016. The US strategy for handling the waste from defense programs, the dismantling of nuclear weapons, and commercially generated spent nuclear fuel continues to flounder. Large projects—including a nuclear waste vitrification plant at the Hanford Site and a mixed-oxide fuel-fabrication plant at the Savannah River Site—fall ever further behind schedule, and costs continue to mount, with the US Energy Department spending more than $5.5 billion each year on environmental management of legacy nuclear waste from US weapons programs.

Thanks to such problems, in the United States and in other countries, nuclear power's attractiveness as an alternative to fossil fuels will continue to decrease, despite the clear need for carbon-emissions-free energy in the age of climate change.

Dealing with emerging technological threats.

The world's institutions were proven arthritic during the recent outbreak of Ebola in West Africa. Medical scientists had a good grip on what to do to quell the outbreak of that deadly virus. But social and political institutions stuttered and, at times, failed to respond effectively. In the age of synthetic biology and globalization, world governance must develop ways to react quickly and effectively to confront emerging disease and the possibility of bioterrorism.

Unfortunately, microbes are not the only emerging technological challenges to civil society and international governance.

It is clear from the recent hacking of major organizations and government facilities that cyber attacks constitute a threat with the potential to destabilize governmental and financial institutions and to serve as a medium for new escalations of international tensions. Meanwhile, advances in artificial intelligence have led a number of prominent individuals to express concern about human command and control capabilities in the field, on national and international scales, over coming decades.

The *Bulletin* is concerned about the lag between scientific advances in dual-use technologies and the ability of civil society to control them. The international community needs to strengthen existing institutions that regulate emergent technologies and to create new forums for exploring potential risks and proposing potential controls on those areas of scientific and technological advance that have so far been subject to little if any societal oversight.

The threat is serious, the time short.

The *Bulletin of the Atomic Scientists* does not move the hands of the Doomsday Clock for light or transient reasons. The clock ticks now at just three minutes to midnight because international leaders are failing to perform their most important duty—ensuring and preserving the health and vitality of human civilization.

During the past several years, the *Bulletin*'s Science and Security Board has grown increasingly concerned as world political leaders dithered, leaving an undeniable threat to the future of mankind—climate change—largely unaddressed. In 2014, leaders in the nuclear weapons countries have consented to a mad dash down an expensive and dangerous path toward "modernizing" their nuclear arsenals; in the process, they turned away from reasonable disarmament efforts and allowed an economic dispute between Ukraine and Russia to turn into an East-West confrontation that hinders cooperation on worldwide nuclear security, arms control, and nonproliferation.

These stunning governmental failures have imperiled civilization on a global scale, and so we, the members of the *Bulletin of the Atomic Scientists* Science and Security Board, implore the citizens of the world to speak clearly, demanding that their leaders:

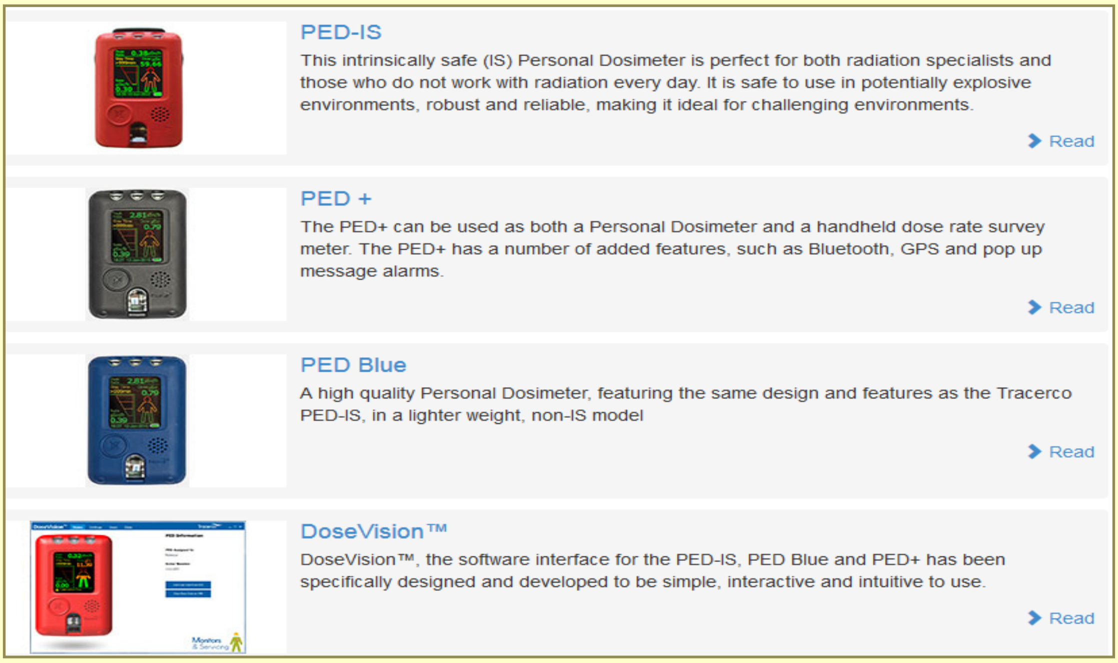
- **Take actions that would cap greenhouse gas emissions at levels sufficient to keep average global temperature from rising more than 2 degrees Celsius above preindustrial levels.** The 2-degree target is consistent with consensus views on climate science and is eminently achievable and economically viable—if national leaders show more interest in protecting their citizens than in serving the economic interests of the fossil fuel industry.
- **Dramatically reduce proposed spending on nuclear weapons modernization programs.** The United States and Russia have hatched plans to essentially rebuild their entire nuclear triads in coming decades, and other nuclear weapons countries are following suit. The projected costs of these "improvements" to nuclear arsenals are indefensible, and they undermine the global disarmament regime.
- **Re-energize the disarmament process, with a focus on results.** The United States and Russia, in particular, need to start negotiations on shrinking their strategic *and* tactical nuclear arsenals. The world can be more secure with much, much smaller nuclear arsenals than now exist—if political leaders are truly interested in protecting their citizens from harm.
- **Deal now with the commercial nuclear waste problem.** Reasonable people can disagree on whether an expansion of nuclear-powered electricity generation should be a major component of the effort to limit climate change. Regardless of the future course of the worldwide nuclear power industry, there will be a need for safe and secure interim and permanent nuclear waste storage facilities.
- **Create institutions specifically assigned to explore and address potentially catastrophic misuses of new technologies.** Scientific advance can provide society with great benefits, but the potential for misuse of potent new technologies is real, unless government, scientific, and business leaders take appropriate steps to explore and address possible devastating consequences of those technologies early in their development.

Last year, with the Doomsday Clock at five minutes to midnight, the members of the Science and Security Board concluded their assessment of the world security situation by writing: "We can manage our technology, or become victims of it. The choice is ours, and the Clock is ticking."

In 2015, with the Clock hand moved forward to three minutes to midnight, the board feels compelled to add, with a sense of great urgency: "The probability of global catastrophe is very high, and the actions needed to reduce the risks of disaster must be taken very soon."

NEW Personal Electronic Dosimeter (PED) Family

Source: http://www.tracerco.com/monitors/ped-family?utm_campaign=PED%20Family&utm_content=11291238&utm_medium=social&utm_source=twitter



PED-IS

This intrinsically safe (IS) Personal Dosimeter is perfect for both radiation specialists and those who do not work with radiation every day. It is safe to use in potentially explosive environments, robust and reliable, making it ideal for challenging environments.

› Read

PED +

The PED+ can be used as both a Personal Dosimeter and a handheld dose rate survey meter. The PED+ has a number of added features, such as Bluetooth, GPS and pop up message alarms.

› Read

PED Blue

A high quality Personal Dosimeter, featuring the same design and features as the Tracerco PED-IS, in a lighter weight, non-IS model

› Read

DoseVision™

DoseVision™, the software interface for the PED-IS, PED Blue and PED+ has been specifically designed and developed to be simple, interactive and intuitive to use.

› Read

Tracerco has designed the PEDs to be the easiest personal radiation monitors on the market to use and understand.

Tracerco
Providing Insight Onsite

Everything on the devices has been designed with the user in mind.

For instance, the display system features radiation graph measurements and a simple diagram of a person who fills with colour, depending on the dose of radiation received. All PEDs include weather, shock and drop proof housings, a smooth clean design and simple to use software.

"NO! NO! That's a Dirty Bomb!"

The latest edition of Al Qaeda's online magazine urges lone wolf attacks on US airlines

By Hana Levi Julian

Source: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/explosives/index_en.htm

Al Qaeda is recruiting wannabe terrorists via its online magazine to carry out lone wolf bombings on U.S. commercial airlines.

SITE
WINTER 2014 | 1436 | ISSUE 13
INSPIRE
...AND INSPIRE THE BELIEVERS
Al-Malahem Media
N€UROTM£I
CUTTING THE NERVES & ISOLATING THE HEAD
OSJ Special
THE HIDDEN BOMB
SIMPLE TO MAKE YET ADVANCED BOMB IN THE HANDS OF ASPIRING MUJAHIDEEN GLOBALLY: MADE WITH SIMPLE KITCHEN MATERIALS.
INTERVIEW WITH THE AQ CHEF | GLAD TIDINGS OF VICTORY | LETTER TO THE AMERICAN PEOPLE | THE BATTLE OF MARATHON

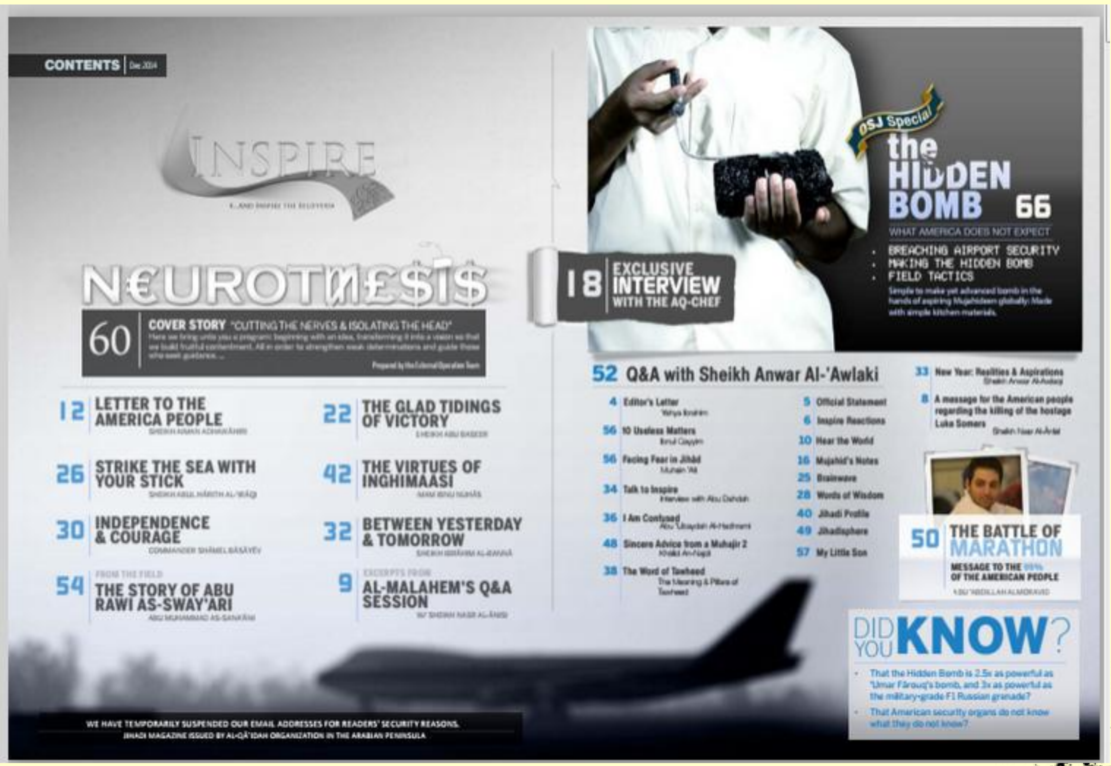
The New York-based Anti-Defamation League sounded the alarm about the terror group's intentions on Wednesday, adding that financial figures and prominent economic personalities were also being targeted.

The 13th issue of "*Inspire*" was released by Al Qaeda in the Arabian Peninsula (AQAP) on Dec. 24, the day before Christmas — one of the busiest travel days in the year.

The magazine contains an article with explicit instructions for easily building a portable bomb inside a 17cm plastic water bottle case. Entitled "The Hidden Bomb," it was posted as a central feature of the English-language magazine.

The entire issue, in fact, is focused on Al Qaeda's strategy for defeating the United States by attacking American military technology, manpower, media and economy.

The magazine suggests the easy-to-build homemade bombs be used against U.S. commercial airliners – specifically American Airlines, Delta, United or Continental — ideally over U.S. soil. Included are instructions about the best location on the



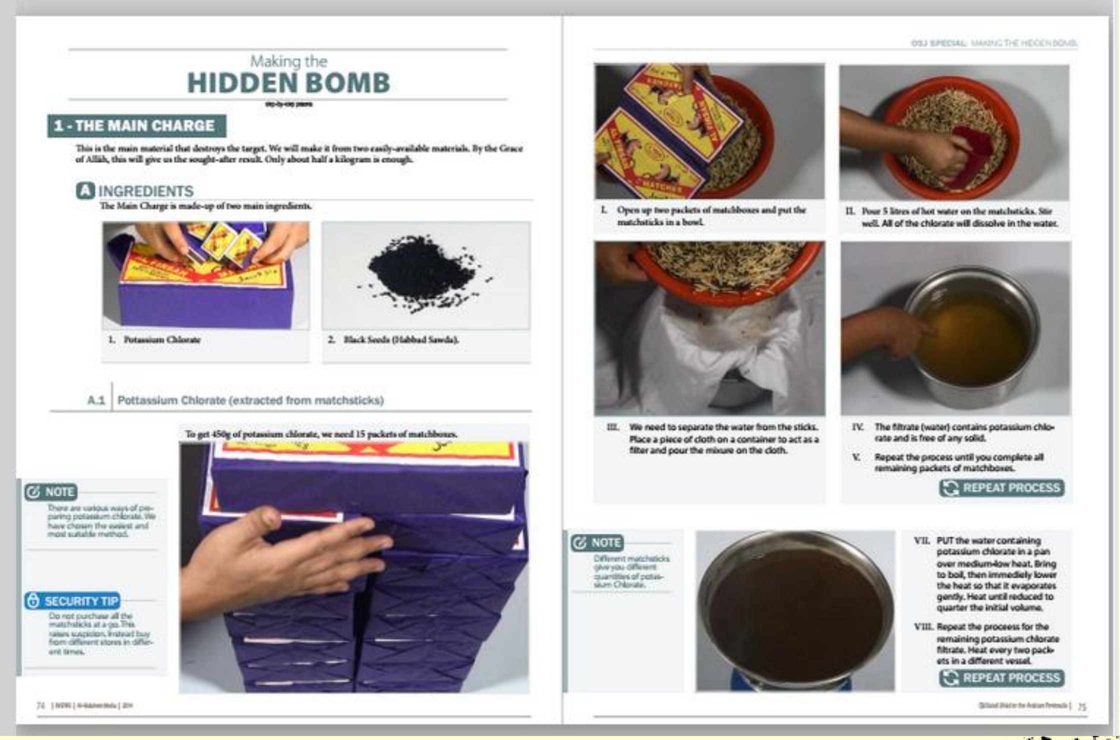
DID YOU KNOW?
- That the Hidden Bomb is 2.5x as powerful as 'Umar Fārouq's bomb, and 3x as powerful as the military-grade F1 Russian grenade?
- That American security organs do not know what they do not know?

WE HAVE TEMPORARILY SUSPENDED OUR EMAIL ADDRESSES FOR READERS' SECURITY REASONS.
JIHADI MAGAZINE ISSUED BY AL-QĀ'IDAH ORGANIZATION IN THE ARABIAN PENINSULA

plane for planting the explosive and the altitude at which to detonate the device. Failing the opportunity to attack a U.S. airline, the magazine suggests aiming at British Airways, Easy Jet, Air France or Air France KL.

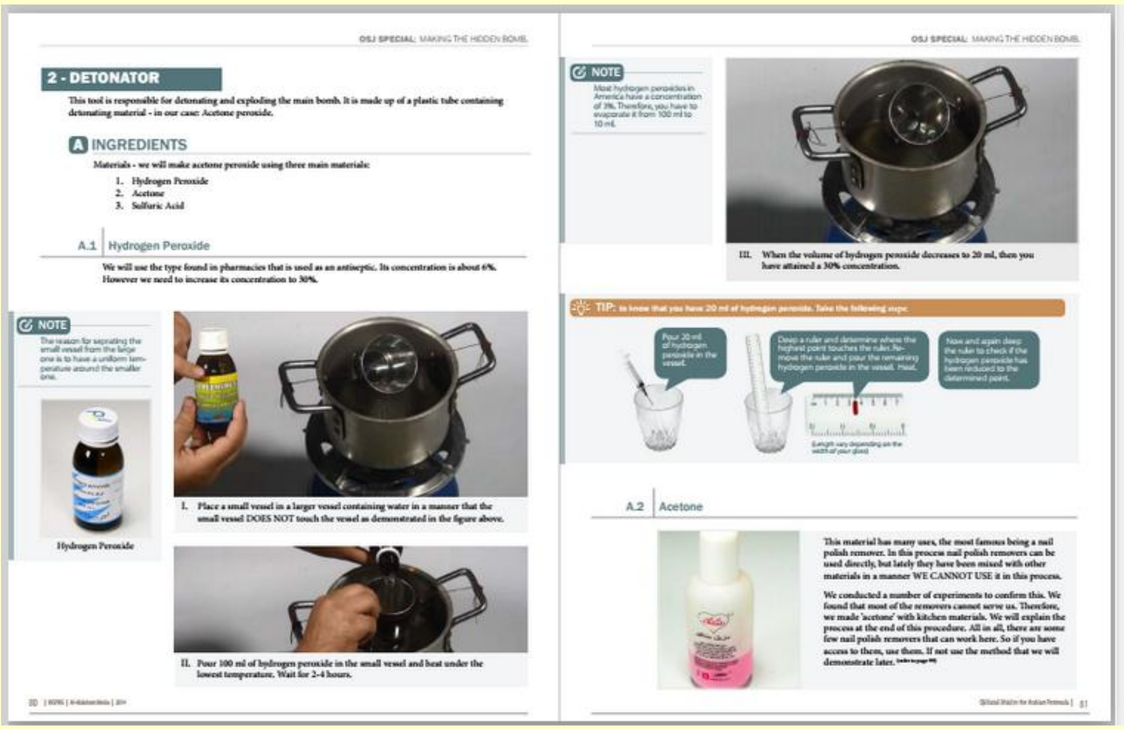
The advantages of this bomb as described in the article is that it is allegedly undetectable by dogs, odor-detecting machines or metal detectors. It is, however, detectable by millimeter wave scanners – a small issue the terrorist group says may not be such a problem because "in most cases they are not used in local airports."

The magazine also praises individuals who have carried out terror attacks for the cause of radical Islam,

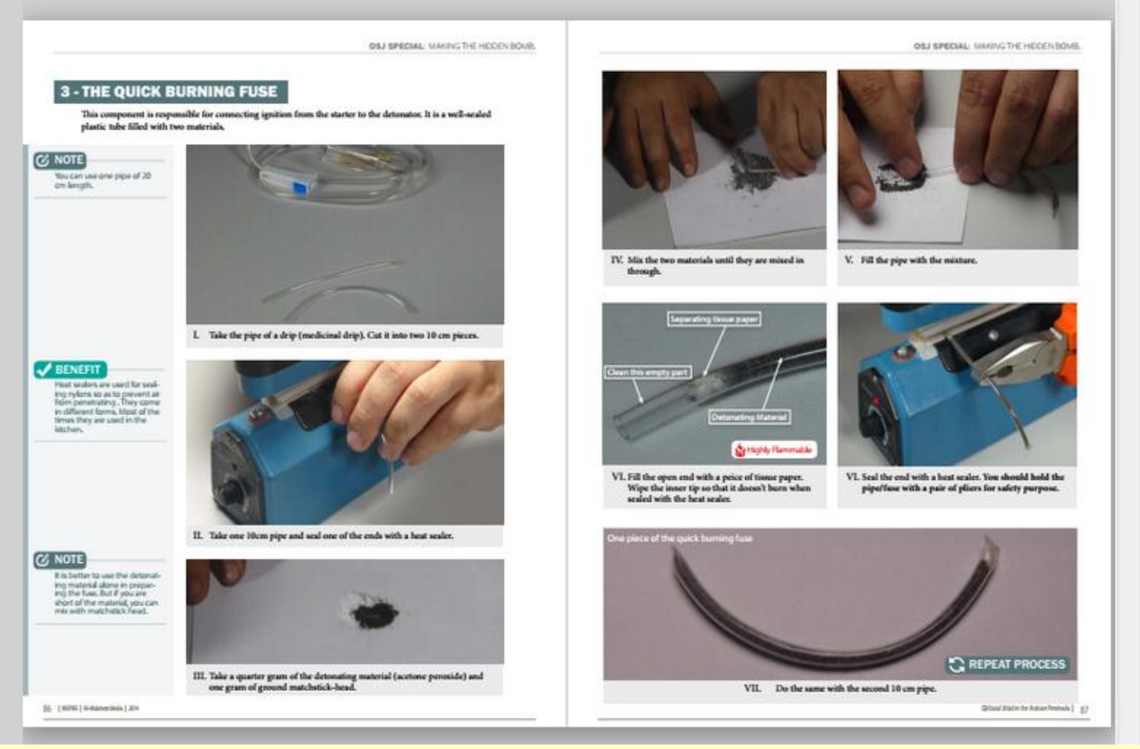


such as Man Haron Monis in Sydney, Australia, who last week held 15 people hostage for hours at the Lindt Chocolate Cafe. Two people died in the attack after police commandos finally stormed the site.

“The Lions of Allah who are all over the globe – some call them lone wolves – should know that they are the West’s worst nightmare.”



The magazine has played a role in the radicalization of multiple domestic extremists, the ADL pointed



out, including the Tsarnaev brothers who were responsible for the Boston Marathon bombing.

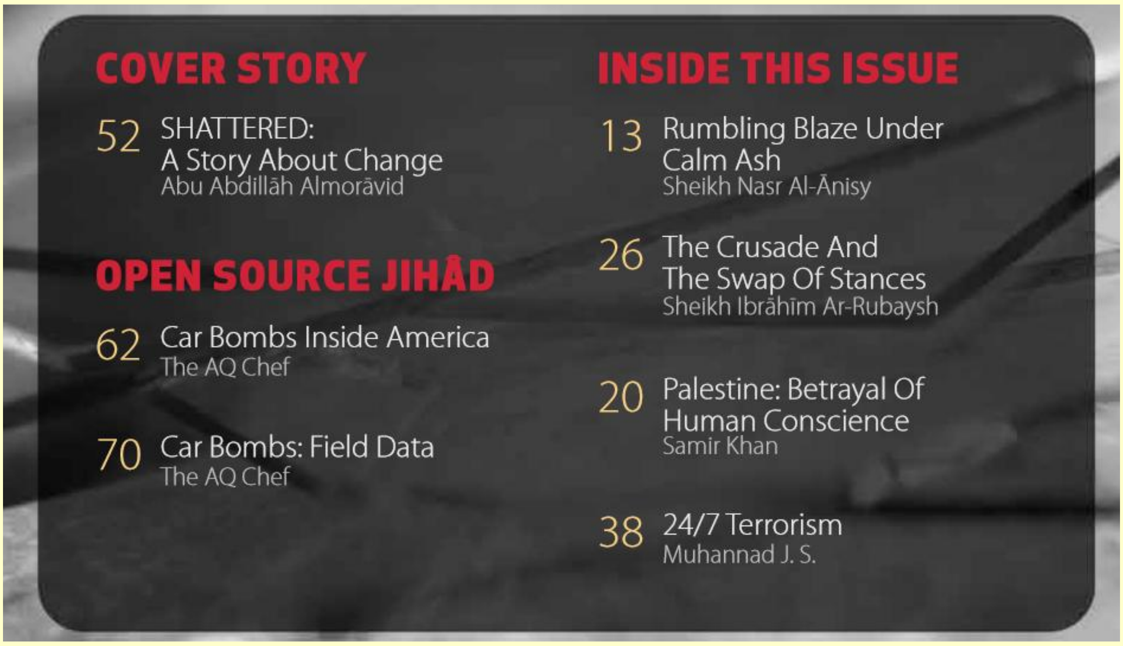
Following notification by the ADL, YouTube removed the video promoting the Inspire 13 magazine from its site.

***Hana Levi Julian** is a Middle East news analyst with a degree in Mass Communication and Journalism from Southern Connecticut State University. A past columnist with The Jewish Press and senior editor at Arutz 7, Ms. Julian has written for Babble.com, Chabad.org and other media outlets, in addition to her years working in broadcast journalism.*

▶ **Read the issue #13 at:** http://worldanalysis.net/14/2014/12/inspire-magazine-issue13/

Contents of #12

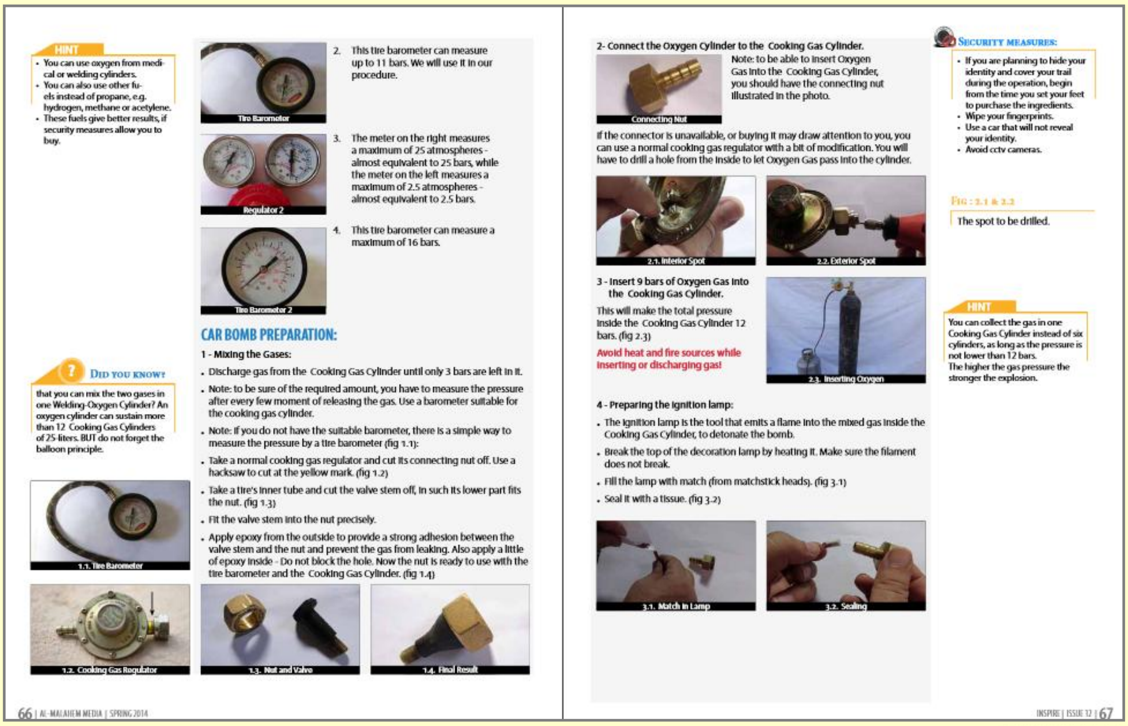
Source: https://azelin.files.wordpress.com/2014/04/inspire-magazine-issue-12.pdf



COVER STORY

OPEN SOURCE JIHĀD

INSIDE THIS ISSUE



HINT

- You can use oxygen from medical or welding cylinders.
- You can also use other fuels instead of propane, e.g. hydrogen, methane or acetylene.
- These fuels give better results, if security measures allow you to buy.

2. This tire barometer can measure up to 11 bars. We will use it in our procedure.
3. The meter on the right measures a maximum of 25 atmospheres - almost equivalent to 25 bars, while the meter on the left measures a maximum of 2.5 atmospheres - almost equivalent to 2.5 bars.
4. This tire barometer can measure a maximum of 16 bars.

DID YOU KNOW?

that you can mix the two gases in one Welding-Oxygen Cylinder? An oxygen cylinder can sustain more than 12 Cooking Gas Cylinders of 25-liters. BUT do not forget the balloon principle.

CAR BOMB PREPARATION:

1 - Mixing the Gases:

- Discharge gas from the Cooking Gas Cylinder until only 3 bars are left in it.
- Note: to be sure of the required amount, you have to measure the pressure after every few moment of releasing the gas. Use a barometer suitable for the cooking gas cylinder.
- Note: If you do not have the suitable barometer, there is a simple way to measure the pressure by a tire barometer (fig 1.1):
- Take a normal cooking gas regulator and cut its connecting nut off. Use a hacksaw to cut at the yellow mark. (fig 1.2)
- Take a tire's inner tube and cut the valve stem off, in such its lower part fits the nut. (fig 1.3)
- Fit the valve stem into the nut precisely.
- Apply epoxy from the outside to provide a strong adhesion between the valve stem and the nut and prevent the gas from leaking. Also apply a little of epoxy inside - Do not block the hole. Now the nut is ready to use with the tire barometer and the Cooking Gas Cylinder. (fig 1.4)

66 | AL-MALAHEM MEDIA | SPRING 2014

2- Connect the Oxygen Cylinder to the Cooking Gas Cylinder.

Note: to be able to insert Oxygen Gas into the Cooking Gas Cylinder, you should have the connecting nut illustrated in the photo.

If the connector is unavailable, or buying it may draw attention to you, you can use a normal cooking gas regulator with a bit of modification. You will have to drill a hole from the inside to let Oxygen Gas pass into the cylinder.

3 - Insert 9 bars of Oxygen Gas into the Cooking Gas Cylinder.

This will make the total pressure inside the Cooking Gas Cylinder 12 bars. (fig 2.3)

Avoid heat and fire sources while inserting or discharging gas!

4 - Preparing the ignition lamp:

- The ignition lamp is the tool that emits a flame into the mixed gas inside the Cooking Gas Cylinder, to detonate the bomb.
- Break the top of the decoration lamp by heating it. Make sure the filament does not break.
- Fill the lamp with match (from matchstick heads). (fig 3.1)
- Seal it with a tissue. (fig 3.2)

SECURITY MEASURES:

- If you are planning to hide your identity and cover your trail during the operation, begin from the time you set your feet to purchase the ingredients.
- Wipe your fingerprints.
- Use a car that will not reveal your identity.
- Avoid cctv cameras.

FIG : 2.1 & 2.2

The spot to be drilled.

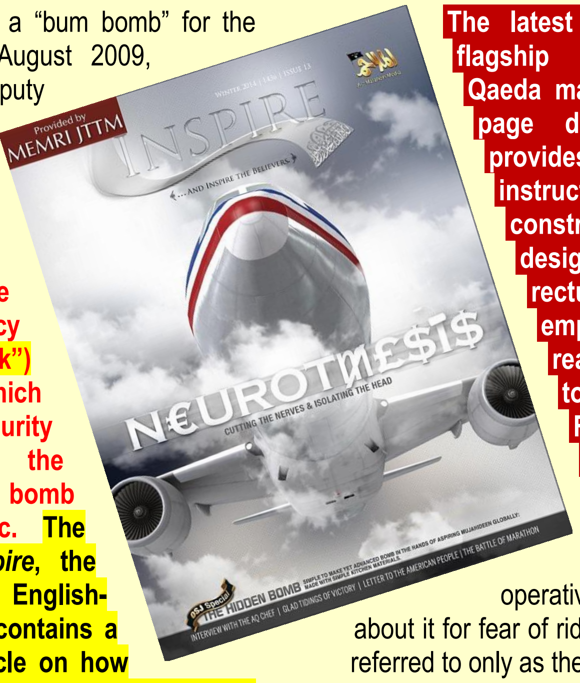
HINT

You can collect the gas in one Cooking Gas Cylinder instead of six cylinders, as long as the pressure is not lower than 12 bars.
The higher the gas pressure the stronger the explosion.

INSPIRE | ISSUE 12 | 67

Building better butt bombs: Al Qaeda's instructions to followers

Source: http://www.homelandsecuritynewswire.com/dr20150106-building-better-butt-bombs-al-qaeda-s-instructions-to-followers


Provided by MEMRI JTTM
INSPIRE
...AND INSPIRE THE BELIEVERS
NEUROTMESIS
CUTTING THE NERVES & ISOLATING THE HEAD
THE HIDDEN BOMB
INTERVIEW WITH THE AQ CHIEF | GLAD TIDINGS OF VICTORY | LETTER TO THE AMERICAN PEOPLE | THE BATTLE OF MARATHON

Five years after using a "bum bomb" for the first time – on 28 August 2009, against the Saudi deputy interior minister – al Qaeda bomb makers are at it again. **Having actively searched for new and better ways to take advantage of privacy ("don't touch my junk") considerations which govern airport security checks, one of the organization's bomb makers goes public. The latest issue of *Inspire*, the organization's English-language magazine, contains a detailed 22-page article on how to construct a butt bomb and conceal it in one's anal cavity.** The article alsoadvises would-be suicide bombers on where to sit on the airplane to ensure the most destruction, and also recommends using the hidden bomb for assassination attempts.

In its efforts to skirt airport security, al Qaeda claims to have come up with improved plans for a deadly "butt bomb" – that is, a bomb which a suicide bombers carries in his rectum.

The *Intercept* reports that the claim comes five years after Nigerian "underwear bomber" Umar Farouk Abdulmutallab tried to bring down a plane en route to Detroit, Michigan on Christmas eve 2009.

More tellingly, the claim comes five years after the 28 August 2009 attempt by an al-Qaeda-affiliated Saudi suicide bomber to use the same method to kill a high-level Saudi official. The suicide bomber, carrying explosives in his anal cavity, managed to get close to the Saudi deputy interior minister and detonate himself – the bomber was killed, but the Saudi minister was unharmed.

Drawing lessons from both incidents, al Qaeda's bomb makers have been actively searching for new and better ways to take advantage of privacy ("don't touch my junk") considerations which govern airport security checks.

The latest issue of *Inspire*, the flagship English-language al Qaeda magazine, includes a 22-page detailed article which provides step-by-step instructions on how to construct the bomb, which is designed to be placed in the rectum where "the [airport] employee do [sic] not reach and have no right to touch or pat, like Umar Farouq did," according to the magazine.

These detailed plans notwithstanding, it appears that al Qaeda operatives are uncomfortable talk about it for fear of ridicule. Often, the device is referred to only as the "hidden bomb."

Inspire goes on mention that al Qaeda has been conducting experiments with simple, easy-to-find materials for such bombs. These include items such as eggs, vinegar, and nail polish, as well as specific tips for potential attackers to avoid detection during airport screenings.

Further, the organization suggests that major Western airlines should be targeted with rectal bombs, advising would-be suicide bombers where to sit on the airplane to ensure the most destruction. The article also recommends using the hidden bomb for assassination attempts, particularly of symbolic figures such as Ben Bernanke, the former chairman of the Federal Reserve, and Microsoft founder Bill Gates (both mentioned by name).

A spokesman for the organization told *Intercept* that al Qaeda sees the hidden bomb as a way of refocusing attention "on external attacks at a time when the group is facing an extended U.S. drone campaign, as well as internal threats in Yemen from the government army and a rising Houti Insurgency."

More importantly, the new bomb "is to show that these threats didn't divert [Al Qaeda} away from its main goal to target America."

The terrorist group waited several years before providing the details on how to construct the bomb, but has now “decided to release it as a part of a complete program for the Lone Mujahid.”

Umar Farouq Abdulmutallab, a Nigerian national who had joined AQAP while studying in Yemen, tried unsuccessfully to blow up a U.S.-bound airline on Christmas Day 2009. Abdumutallab had hidden in his underwear chemical explosives, which he planned to detonate using a syringe. His plan was foiled, a top TSA official later revealed, because the bomber had not changed his underwear for two weeks, thus degrading the explosives. (*Inspire* reassures followers that even if they fail like the original underwear bomber they will still have succeeded.)

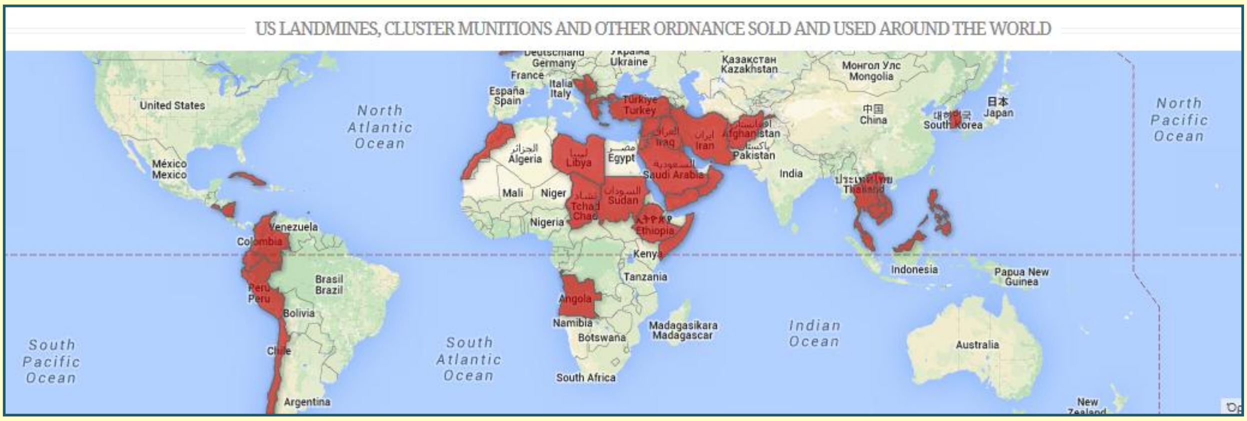
In the line of duty

Egytian EOD dies while attempting to neutralize IED in Cairo…

One more hero down…

Deadly debris: Northwestern U students report on U.S. landmine legacy

Source: http://www.homelandsecuritynewswire.com/dr20150107-deadly-debris-northwestern-u-students-report-on-u-s-landmine-legacy



Jan 07 – Despite a 20-year cleanup effort, the explosive remnants of war left behind by the United States after sustained military campaigns around the world continue to kill and maim thousands of people in Cambodia, Iraq, and other countries, according to a three-month investigation led by a reporting team from Northwestern University's Medill School of Journalism, Media, Integrated Marketing Communications.

The United States has used landmines, cluster bombs, and other lethal conventional munitions during numerous wars and other conflicts around the world, and sold or gave them to dozens of other nations.

Despite a $3.2 billion U.S. effort to clear unexploded ordnance, assist victims, and wipe out aging munitions stockpiles that dates back to 1993, civilians are still dying and the "deadly debris" is inflicting incalculable damage on communities, regions and entire countries, the investigation found.

A Medill School release reports that the team of eight graduate student reporters worked extensively in Washington, D.C. as part of the annual installment of the Medill National Security Reporting Project. They also reported from remote outposts in Mozambique and Cambodia, an epicenter of the cold war in Ukraine, a still-active conflict zone in Kurdistan, Iraq, and neighboring Jordan, and from the United Nations in New York.

Though the United States is a world leader in the cleanup effort and has had some major successes, critics say its efforts are not enough, the reporters found.

The project, titled **Deadly Debris: The U.S. Legacy of Unexploded Remnants of War**, is being published on a Web site created by the reporting team. It is also being published by GlobalPost, the award-winning digital journalism site with a primary focus on world news coverage.

The findings are based on interviews with dozens of experts, victims, and government officials, field reporting on four continents, and a Medill analysis of dozens of reports and studies.

"Deadly Debris" is a comprehensive series of print, video, and interactive stories. As part of its partnership with Medill, *GlobalPost* is also sharing the project with its many clients for publication.

"The students have performed a huge public service by shining a bright light on this important and timely topic," said Josh Meyer, project leader and director of education and outreach for the Medill National Security Journalism Initiative, which awarded scholarships for the Washington-based reporting effort.

The scholarships and the initiative itself are funded through a generous grant from the Robert R. McCormick Foundation.

"This project is accountability journalism of the highest order, and we're grateful to *GlobalPost* for being so enthusiastically supportive of our work, and for publishing our findings to a worldwide audience," Meyer added.

The student team comprised project manager Christopher Walljasper, who designed the Web site and reported along with Carolyn Freundlich, Alexandra Hines, Eliza Larson, Rachel Menitoff, Melanie Saltzman, Matthew Schehl, and Tammy Thueringer.

They were assisted by Meyer, Medill Visiting Professor Matt Mansfield, interactive adjunct and Medill graduate Michelle Minkoff, and photo/video adjunct Allison Shelley.

"It's an honor for *GlobalPost* to help spread to our audience the journalism of Medill and Northwestern," said *GlobalPost* editor Tom Mucha. "As a global news organization we're always grateful for those who put in the hard work to produce a project of this editorial importance, scope and scale."

The release notes that "Deadly Debris" is the fifth in a series of annual investigative reporting efforts which are part of Medill's National Security Journalism Initiative. The initiative was established in January 2009 to equip journalists with the knowledge and skills necessary to report accurately and innovatively on issues related to defense, security and civil liberties and to do so across all digital platforms.

Previous projects have focused on the troubled U.S. global food aid program, the national security implications of U.S. energy policy, and the challenges faced by National Guard and Reserve members returning home from a decade of war. The first project, on the national security implications of climate change, won a national award from the Online News Association.

— Read more in "Deadly Debris: The U.S. Legacy of Unexploded Remnants of War," GlobalPost (25 December 2014).

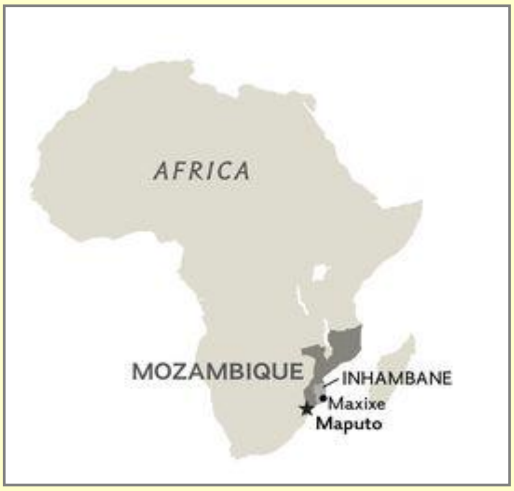
▶ **Read more at:** http://deadlydebris.nationalsecurityzone.org/home-2/overview/

Clearing Land Mines Becomes Women's Work in Mozambique and Beyond

Source: http://www.terrorismwatch.org/2015/01/clearing-land-mines-becomes-womens-work.html

When Biatriz Hernesto was a child, she and her school friends longed to pick fruit in the bush behind her grandparents' house. They knew that's where the best marula fruits and other wild treats grew. But they also knew the area contained land mines, so they seldom ventured there.

Hernesto grew up in Maxixe, in southern Mozambique, in the aftermath of a brutal civil war that lasted from 1977 to 1992 and left the southern African country riddled with deadly, unexploded ordnance.



When she saw people coming to clear the land of mines, she hid. "We thought the de-miners were soldiers who would kill us," says Hernesto, now 25.

Many of them were, in fact, former fighters. Traditionally, mine-clearing efforts in Mozambique, and globally, have employed ex-soldiers as a way to provide them with work and integrate them back into society, says Ashley Fitzpatrick of APOPO, a Belgian NGO headquartered in Tanzania that clears land mines in Africa and Asia.

But those demographics are shifting. In Mozambique and other countries, women are now working as de-miners.

In Cambodia, women began taking up such work in 1995, followed by Kosovo in 1999. The passage of UN Resolution 1325 in 2000, which required the de-mining industry to work toward gender equality, has boosted the trend. Now, about 20 countries employ females in land-clearing occupations, which include de-mining, training, and managing.

The push for women deminers has also come from donors who support the de-mining efforts of humanitarian organizations, says Arianna Calza Bini, director of the Geneva-based Gender and Mine Action Programme.

Those donors, along with the UN and many NGOs, note that in postconflict areas, de-mining is often one of the only economic opportunities available. And workers and funders want to include the larger community in the process—it is, after all, their land that's being cleared. Finally, it's often women who are most at risk of being hurt or killed by land mines in the field.

"Women are the people in Mozambique who are responsible for gathering firewood and water, and for tilling the fields," says Kate Brady of the United Nations Development Programme in Mozambique. "Therefore, they are [most] likely to be affected by land contamination."

In this coastal country, land mines left over from three long-resolved conflicts have resulted in at least 2,458 casualties through the end of last year.

But the horror may finally be coming to an end. With help from women de-miners, more than 300,000 mines have been removed since 1992. Mozambique is expected to be declared mine-free by the end of this year

Mechanics of Mine Clearing

Most of Mozambique's mines were planted during three periods: the civil war, the 1964-1974 anticolonial war with the Portuguese, and the training of Zimbabwean liberation forces in Mozambique in the 1960s and '70s.

Removing the mines from those campaigns is not only dangerous, it's also tedious. For one thing, it involves wearing a cumbersome helmet and a heavy vest similar to those worn when getting an x-ray.

De-miners must wear cumbersome protective vests and face masks in the field. They use color-coded markers to identify areas that have been cleared, areas where a mine has been found, and areas still in the process of being cleared.

But it's something people have to do. While dogs and rats can be trained to detect the scent of explosives used in mines, and machines can clear the land to make searching easier, humans must handle the animals and operate the machines.

Hernesto is small and strong, and little shells decorate the ends of her braids. She was one of the first women to join Handicap International in Mozambique in 2010, when the organization began hiring and training women as de-miners.

The Meaninglessness of Gender

When Mozambique's de-mining process began in 1992, says Alberto Augusto, director of Mozambique's National Demining Institute,

She wears the same bulky boots and heavy de-mining vest as her male colleagues, but a glimpse of polka dots can be seen through the buttons of her work shirt.

During the month and a half she spent in training, she wanted to quit several times. She worried about what would happen if her metal detector failed—if the batteries burned out, for instance, and the device missed a land mine and she stepped on it.

But she stuck with it, largely because of the support of the 11 other women who made up Handicap International's first female de-mining team.

In the field, de-miners maintain a distance of about 50 to 165 feet (15 to 50 meters) between themselves, so that if one of them sets off a mine, others won't be injured.

But that doesn't guarantee safety. The radius of a mine explosion varies, and deadly shrapnel will sometimes travel as far as 325 feet (100 meters).

When a mine is found, it's detonated with other explosives; it's considered safer to destroy it where it is than to try to remove it. De-miners light a fuse that allows them about five minutes to leave the area before the explosion.

people thought it would take a century or more to complete the task.

Now—despite deadly ambushes by rebels from the guerrilla

Mozambican National Resistance (RENAMO) prior to October's elections, during which at least two de-miners were shot in the course of a RENAMO offensive—they expect to have cleared all known areas by January.

While rats and dogs can be used to detect the scent of explosives in land mines, it is ultimately people who must deal with destroying them. Most mines are detonated using other explosives.

That's thanks to strong commitment from both the government of Mozambique and the international community. Roughly 90 percent of the de-mining here is done by humanitarian organizations like APOPO and Handicap International, while commercial groups such as BACTEC (Battle Area Clearance, Training, Equipment, and Consultancy) handle the rest.

Today about 20 percent of the roughly 1,000 active humanitarian de-miners—meaning those who work for NGOs, as opposed to the commercial miners who are paid by the government—in Mozambique are women, says Augusto. Many have been specifically recruited, which initially made some men uncomfortable.

Ismael at Handicap International remembers wondering if separate bathrooms at the campsites where de-miners live would be necessary, and whether the de-miners would work in mixed- or single-sex teams.

But it wound up being simpler than he thought. And, he says, if you look at the rate of clearance, there's no difference between the sexes.

The same seems to be true, at least anecdotally, in the wider international community as well, says Calza Bini of the Gender and Mine Action Programme.

But not all countries have embraced the idea. When she was in Libya last year, Calza Bini was told: "Don't ask—don't even mention female de-miners—because it's completely unacceptable" to the society at large and to many of the women's families.

When Hernesto started work, her parents called daily to check on her. She found her first mine on the third day of the job. She's found dozens more since then, but the initial fear she felt is still with her.

"I'm always scared," she says. "Because if there is any failure, it can be fatal."

Mines have injured two Handicap International de-miners since 1998, when the organization began working in Mozambique. Both were men; both lost a leg. Hernesto had trained with one of them. Seeing what he went through was hard, she says, but the experience did not weaken her resolve.

"If it's not me," she says, "who is going to do it? I have to do it."

"Like a Man in the Field"

Felicidade Matsinhe admits that her main motivation for becoming an APOPO de-miner was **the pay—a little more than $300 (U.S.) a month in a country where the average annual income is $590 (U.S.).**

A 25-year-old widow with a young daughter, Matsinhe sold secondhand clothes in a market before joining APOPO in 2012. Since then she has managed to save enough money to start construction on a two-bedroom house.

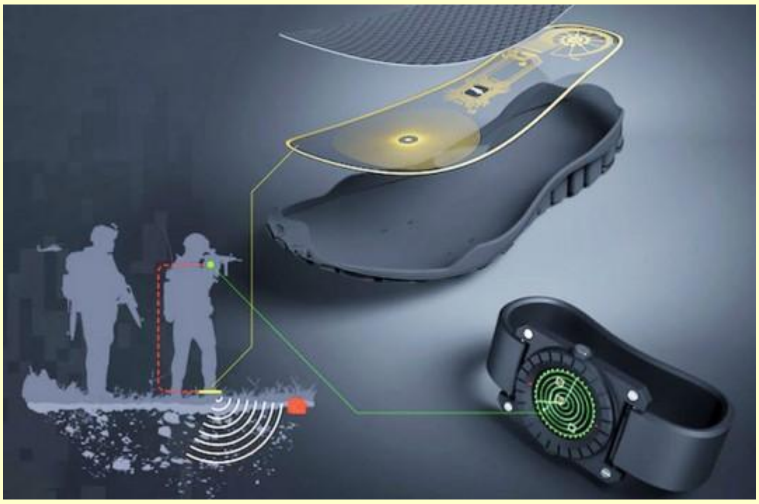
The house will have electricity and running water—a huge improvement over the simple coconut-thatch shacks she grew up in, and something she's dreamed of since childhood.

Matsinhe knows her work as a de-miner is what made it possible. Thankful for her job despite the danger, she keeps a Bible in her tent and prays each afternoon after she gets off work. "I pray so God may protect me," she says, "especially in the area where I am working."

APOPO team leader Januario Bape says he was skeptical when he first heard about women de-miners, unsure if they could handle the job. Now he no longer thinks about it. Instead, he praises Matsinhe's work, giving her what he considers the ultimate compliment: "She is like a man in the field."

Life-Saving Boot Can Detect Active Landmines from 6.5 Feet Away

Source: http://www.terrorismwatch.org/2015/01/life-saving-boot-can-detect-active.html



Bogota-based design firm Lemur Studio has designed a life-saving boot insert which can detect landmines from a distance of 6.5 feet. SaveOneLife was created with soldiers in mind, but civilians and farmers living in areas littered with active mines can also benefit from this groundbreaking technology. The boot sole acts as a metal detector with a built-in radio transmitter and processor which pick up electromagnetic fields produced by large metal objects.

Colombia's fields and jungles are full of active landmines which have, in the last 24 years, killed 2,000 people and injured about 10,000 more. With the goal of saving both soldiers and innocent civilians, Lemur Studio created a boot sole that detects land mines within a radius of 6.5 feet, and alerts the wearer of danger. Embedded within the soles are microprocessors and radio transmitters that send a signal to a wristband interface, which shows the mine's exact location.

saveonelife
Categoria: Concepto

Lemur Studio's designers have received numerous awards for their life-saving design, including the Red Dot Design Singapore Award. SaveOneLife is also one of the contestants for the World Design Impact Prize, the winners of which will be announced in November. The team is currently pitching their concept to the military and seeking additional funding.

Homemade bombs are threats that are not going to go away, and ever closer civil-military cooperation is needed to neutralise them

By Peter Round

Source: http://www.securityeurope.info/homemade-bombs-are-threats-that-are-not-going-to-go-away-and-ever-closer-civil-military-cooperation-is-needed-to-neutralise-them/

Improvised explosive devices remain the single largest killer of coalition soldiers in the war in Afghanistan – and a favoured weapon of Europe's home-grown terrorists as well. This has put the devices at the forefront of public debate, with the acronym 'IED' now used and widely understood well beyond just military circles.

However, even if they have gained a lot of public attention in the last few years, IEDs are nothing new. With their low cost and ability to cause significant damage they have been the weapon of choice for insurgents fighting technologically superior forces for decades.

With this asymmetric warfare likely to remain the norm, IEDs will continue to be the biggest single threat to our soldiers on the ground – as well as being a growing threat to civilian populations. It is vital that the experience and knowledge gained in fighting IEDs in Afghanistan is not lost. Moreover, we need to ensure the best possible collaboration between military and civilian law enforcement entities.

The European Defence Agency (EDA) has played an important role in ensuring that skills and knowledge in tackling IEDs are

maintained. One important element of its counter-IED work is technical exploitation. This refers to the recording and analysing of information related to events, scenes, technical components and the materials used in an IED attack.

The objective of counter-IED exploitation is to gather the technical and tactical data about the attack whilst at the same time identifying the IED "supply chain" in order to gather intelligence about those involved in IED production and use. Exploitation allows bomb disposal experts to better understand the threat they are dealing with, helping them to predict future activity and allowing them to attack the network involved in producing the devices. A number of the EU's civil security research projects financed by the European Commission aim for similar goals, for example.

Counter-IED exploitation was the rationale behind the 2011-2014 deployment of a multi-national theatre exploitation laboratory in Afghanistan, where it helped disrupt networks making and using IEDs. In parallel to that effort, **a new programme, called the "Joint Deployable Exploitation and Analysis Laboratory" (JDEAL) was begun in May 2013. Under Dutch lead**, its aim was to establish a permanent IED exploitation training facility in the Netherlands, staffed by a permanent multinational team. Under the project, a further two deployable laboratories could be procured for use in future operations.

Initiatives such as JDEAL aim to ensure that the knowledge gained at a considerable price in wartime is not lost to other defence actors, but also made available to the bomb disposal community as a whole, whether military or civil. Indeed, IEDs are not only a threat to our soldiers overseas: for decades, they have also been used against civilians in Europe often with lethal results. They will continue as the weapon of choice for individuals planning terror attacks against Europe's homeland.

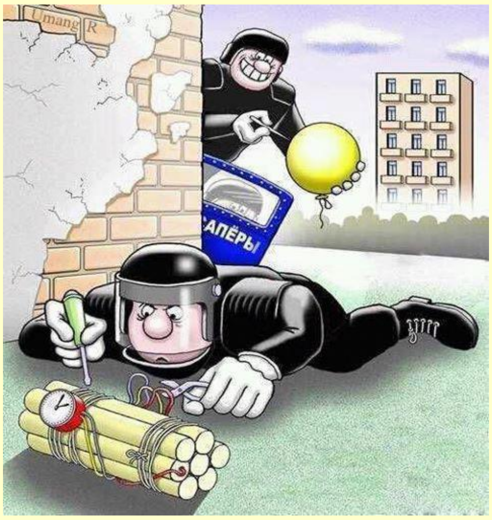
In order to ensure an efficient "spillover" of know-how between these two interconnected worlds, dedicated events have recently been jointly organised by the EDA and Europol. These have brought together experts from as many as 16 different European countries.

The overarching idea is really quite simple: participants take part in realistic training scenarios that involve homemade explosives based on situations experienced in the real world. By doing so, they share best practices and improve their skills through multinational and civil-military cooperation. Even the United States has showed interest in the initiative by sending experts from the FBI and US Department of Justice.

This combined approach ought to be extended to the whole spectrum of C-IED activities – and not just for the disposal of homemade explosives. Other critical skills, such as exploitation techniques currently tackled via the JDEAL project, are needed to win the IED war.

If we want to effectively predict and prevent further IED-related incidents on the battlefield or the homeland – and develop the means to safely neutralise them in a variety of conditions – then we need to push this civil-military cooperation as far as we can. The lives of European soldiers and citizens might very well depend on it.

***Peter Round** is the European Defence Agency's Director of Capability, Armament & Technology.*



Key information security trends in 2015

Source: http://i-hls.com/2014/12/key-information-security-trends-2015/

Cybercriminals are becoming more sophisticated and collaborative with every coming year. To combat the threat in 2015, information security professionals must understand these 3 key trends.
Steve Durbin, managing director of the Information Security Forum (ISF), a nonprofit association, told *cio.com* he foresees 3 security trends that will dominate the year.

1. Cybercrime

Today's cybercriminals primarily operate out of the former Soviet states. They are highly skilled and equipped with very modern tools. Durbin notes they often use 21st century tools to take on 20th century systems.
"In 2015, organizations must be prepared for the unpredictable so they have the resilience to withstand unforeseen, high impact events," he adds. "Cybercrime, along with the increase in online causes (hacktivism), the increase in cost of compliance to deal with the uptick in regulatory requirements coupled with the relentless advances in technology against a backdrop of under investment in security departments, can all combine to cause the perfect threat storm. Organizations must invest in resilience to minimize the impact of the unforeseen."

2. Privacy and Regulation

Most governments have already created, or are in the process of creating, regulations that impose conditions on the safeguard and use of Personally Identifiable Information (PII), with penalties for organizations that fail to sufficiently protect it. As a result, Durbin notes, organizations need to treat privacy as both a compliance and business risk issue, in order to reduce regulatory sanctions and business costs such as reputational damage and loss of customers due to privacy breaches.

3. Threats from third-party providers

Supply chains are a vital component of every organization's global business operations and the backbone of today's global economy. However, Durbin says, security chiefs everywhere are growing more concerned about how open they are to numerous risk factors. A range of valuable and sensitive information is often shared with suppliers, and when that information is shared, direct control is lost. This leads to an increased risk of its confidentiality, integrity or availability being compromised.
"Over the next year, third-party providers will continue to come under pressure from targeted attacks and are unlikely to be able to provide assurance of data confidentiality, integrity and/or availability," Durbin says. "Organizations of all sizes need to think about the consequences of a supplier providing accidental, but harmful, access to their intellectual property, customer or employee information, commercial plans or negotiations."

PROACTIVE
MULTISENSOR FUSION
AND PREDICTIVE REASONING FRAMEWORK

"Predicting terroristic attacks in urban environments: An internet-of-things approach"

By Petris S., Georgoulis C., Soldatos J., Giordani I., Sormani R., Djordjevic D.

Source: http://www.fp7-proactive.eu/publication/predicting-terroristic-attacks-urban-environments-internet-things-approach-petris-s

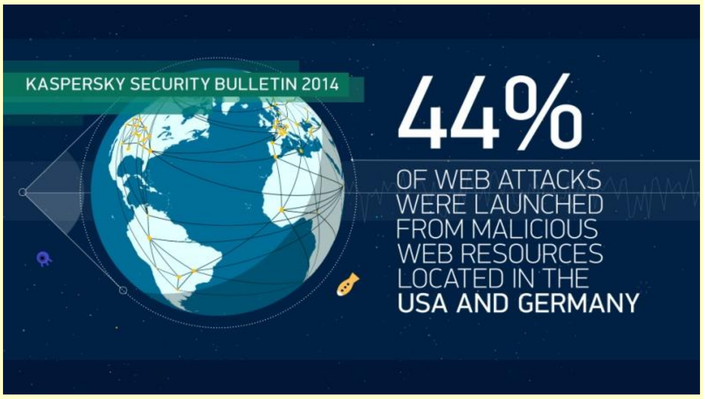
In the recent years we have witnessed a number of important terroristic incidents, in major cities all around the world (e.g., 911 in New York, 11-M in Madrid, 7/7 in London). These incidents have revealed the vulnerabilities of urban environments, against terroristic plans and have created significant pressure towards devising novel tools and techniques for timely predicting the intentions and plans of terrorists. In this paper, we introduce a blueprint

Internet-of-Things architecture for predicting terroristic attacks. The architecture allows Law enforcement agencies to exploit multiple data sources, (including SIGINT, OSINT and HUMINT) towards acquiring information associated with terroristic action, while at the same time providing powerful reasoning capabilities towards transforming raw events into meaningful alerts. We also illustrate the implementation of a terroristic prediction system based on this architecture, along with its use in the scope of a validating scenario.

▶ **Read full paper at IJSIA -** ***International Journal of Security and Its Applications***
http://www.sersc.org/journals/IJSIA/vol8_no4_2014/18.pdf

One billion more: Kaspersky Lab counts up this year's cyber-threats

Source: http://i-hls.com/2014/12/one-billion-kaspersky-lab-counts-years-cyber-threats/


KASPERSKY SECURITY BULLETIN 2014
44%
OF WEB ATTACKS WERE LAUNCHED FROM MALICIOUS WEB RESOURCES LOCATED IN THE USA AND GERMANY

Every year Kaspersky Lab experts evaluate the level of cyber-threats. In 2014 we saw considerable growth in the number of malicious attacks on user computers and mobile devices, further development of financial malware and a change in the vectors of web attacks. In 2013, most web attacks were carried out using malicious web resources located in the USA and Russia while in 2014 Germany hosted more malicious sites than everywhere except the USA. The Netherlands remained in 3rd place.

2014 in figures

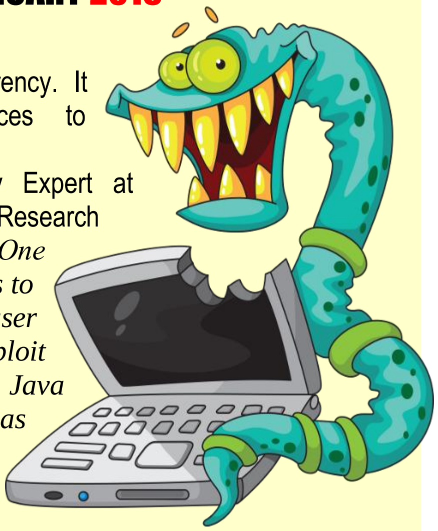
- 6.2 billon malicious attacks on user computers and mobile devices were blocked by Kaspersky Lab antivirus products in 2014, one billion more than in 2013.
- 38% of user computers were subjected to at least one web attack over the year.
- 44% of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US (27.5% of all attacks) and Germany (16.6%). The Netherlands (13.4%) came 3rd.
- Attempts to steal money via online access to bank accounts were blocked on almost 2,000,000 user computers.
- Kaspersky Lab products protected their users from an average of 3.9 million Internet-based attacks a day.
- Kaspersky Lab's web antivirus detected over 123,000,000 unique malicious objects: 74% of them were found at malicious URLs.
- A total of 3.7 million attempts to infect OS X- based computers were blocked by Kaspersky Lab products
- An average Mac user encountered 9 threats during the year
- Kaspersky Lab solutions blocked 1.4 million attacks on Android-based devices, four times as many as last year.
- 295,500 new mobile malicious programs, 2.8 times as many as in 2013
- 12,100 mobile banking Trojans, 9 times as many as last year
- 53% of attacks involved mobile Trojans targeting users' money (SMS-Trojans, banking Trojans)
- 19% of Android users (one in five) encountered a mobile threat at least once over the year.
- Mobile malware attacks were registered in more than 200 countries worldwide

Mobile threats

"2011 was the year of mobile malware formation, especially on Android-based devices; 2012 was when they developed and 2013 was when they reached maturity. In 2014 mobile malware focused on financial issues: the number of mobile banking Trojans was nine times greater than in the previous year and developing in this area is continuing at an alarming rate," said Roman Unuchek, Senior Mobile Malware Analyst at Kaspersky Lab.

Financial threats

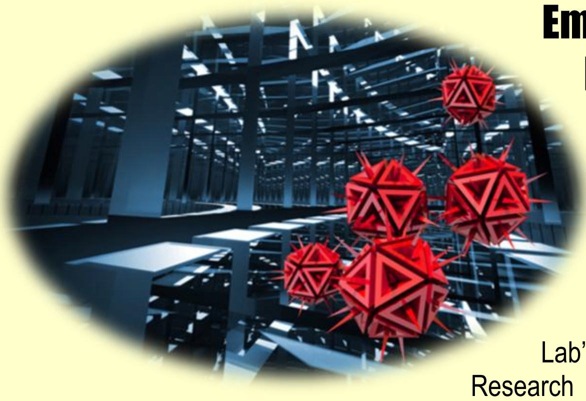
The fraudsters who specialize in mobile financial malware are probably inspired by their experienced "colleagues" who have been stealing money via personal computers for years. Zeus remains the most widespread banking Trojan with ChePro and Lohmys coming second and third. Three quarters of attacks targeting users' money were carried out using banking malware but these are not the only financial threats. Bitcoin wallet theft was the second most popular banking threat (14%). Bitcoin mining software (10%) is another threat related to the crypto currency. It uses computing resources to generate bitcoins.



Maria Garnaeva, Security Expert at Kaspersky Lab's Global Research and Analysis Team, said: *"One of the most effective ways to deliver malware to user computers is to exploit vulnerabilities in Oracle Java and in browsers such as Explorer, Mozilla Firefox, etc. In addition, cybercriminals continue to use exploits for Adobe Reader vulnerabilities. These infection techniques remain popular simply because social engineering techniques are still effective. Each year we see how cybercriminals are creative more inventive ways of luring in their victims. That is why recipients are still willing to read a seemingly harmless e-mail from an unexpected source and then open attachments or follow links that expose them to malicious programs."*

Emerging Threats in the APT World: Predictions for 2015

Source: http://i-hls.com/2014/12/emerging-threats-apt-world-predictions-2015/



For several years now, Kaspersky Lab's Global Research and Analysis Team (GReAT) has shed light on some of the world's biggest Advanced Persistent Threat (APT) campaigns, including RedOctober, Flame, NetTraveler, Miniduke, Epic Turla and Careto/Mask, among others.

By closely observing more than 60 threat actors responsible for cyber-attacks worldwide, the team of experts has now compiled a list of the top emerging threats in the APT world.

These include:

- The fragmentation of bigger APT groups. A growing number of smaller threat actors is likely to lead to more companies being hit. And larger organizations are expected to experience a greater number of attacks from a wider range of sources.
- APT-style attacks in the cybercriminal world. The days when cyber-criminal gangs focused exclusively on stealing money from end users are over. Criminals now attack the banks directly because that's where the money is. And they use APT techniques for these complex attacks.
- Targeting executives through hotel networks. Hotels are perfect for targeting high profile individuals around the world. The Darkhotel group is one of the APT actors known to have targeted specific visitors during their stay in hotels.
- Enhanced evasion techniques. More APT groups will be concerned about exposure and will take more advanced measures to shield themselves from discovery.

- New methods of data exfiltration. In 2015, more groups are expected to use cloud services in order to make exfiltration (the unauthorized transfer of data from a computer) stealthier and harder to detect.
- The use of false flags. APT groups are expected to exploit government intention to 'naming and shaming' suspected attackers by carefully adjusting their operations to plant false flags (that make it appear as if the attack was carried out by another entity.)

"If we can call 2014 'sophisticated', then the word for 2015 will be 'elusive'. We believe that APT groups will evolve to become stealthier and sneakier, in order to better avoid exposure. This year we've already discovered APT players using several zero-days, and we've observed new persistence and stealth techniques. We have used this to develop and deploy several new defense mechanisms for our users," comments Costin Raiu, Director of GReAT at Kaspersky Lab.

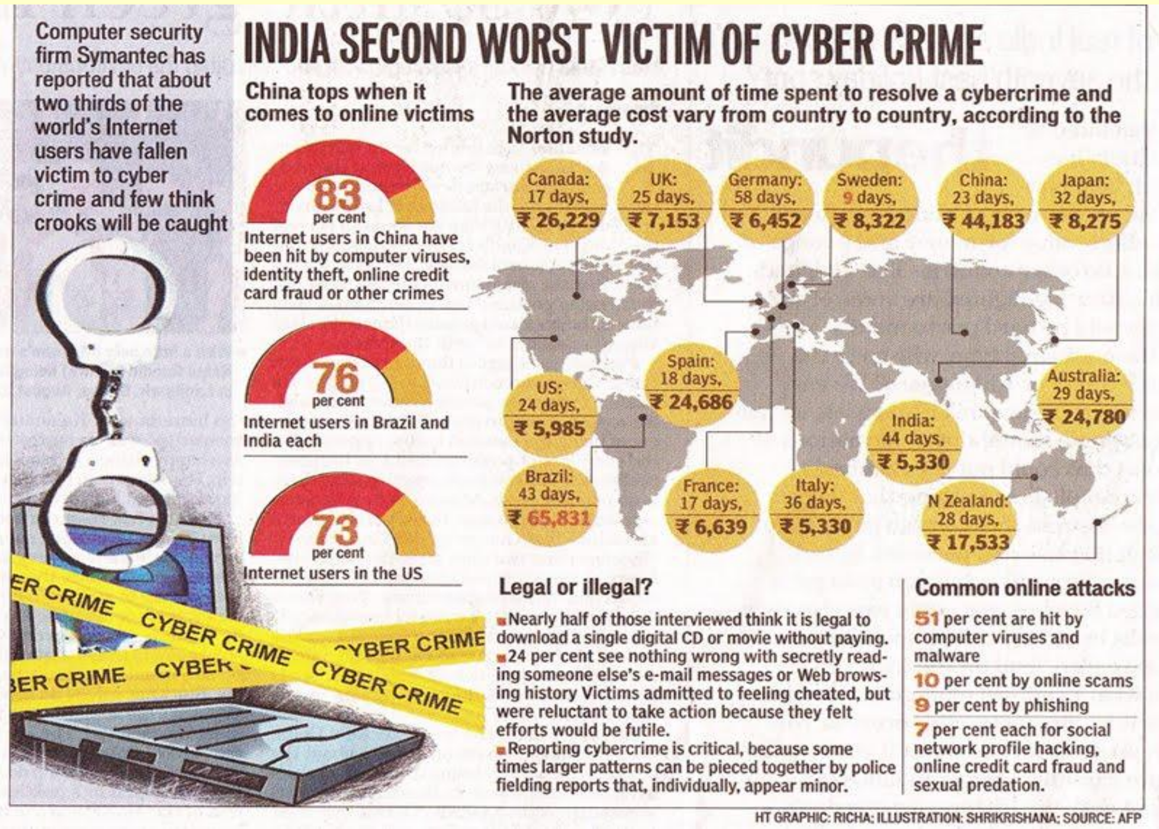
India records a 40 percent rise in cybercrime

Source: http://www.digit.in/internet/india-records-a-40-percent-rise-in-cybercrime-24850.html

Hacking, phishing, credit card and banking frauds have increased by 40% in the country in the past two years, according to a government report.

A Home Ministry official stated that there has been an annual increase of more than 40% in cyber crime cases registered in the country during the past two-three years. He added that India with a fast growing economy is susceptible to international and domestic cyber attacks and there is a need to ensure cyber crime-free environment.

According to Home Ministry statistics, more than 71,780 cyber frauds were reported in 2013, while in 2012, 22,060 such cases were reported. This number has increase sharply in 2014 with more than 62,189 incidents of cyber frauds were reported.



Computer security firm Symantec has reported that about two thirds of the world's Internet users have fallen victim to cyber crime and few think crooks will be caught

83 per cent Internet users in China have been hit by computer viruses, identity theft, online credit card fraud or other crimes

76 per cent Internet users in Brazil and India each

73 per cent Internet users in the US

The average amount of time spent to resolve a cybercrime and the average cost vary from country to country, according to the Norton study.

Legal or illegal?

- Nearly half of those interviewed think it is legal to download a single digital CD or movie without paying.
- 24 per cent see nothing wrong with secretly reading someone else's e-mail messages or Web browsing history Victims admitted to feeling cheated, but were reluctant to take action because they felt efforts would be futile.
- Reporting cybercrime is critical, because some times larger patterns can be pieced together by police fielding reports that, individually, appear minor.

Common online attacks

51 per cent are hit by computer viruses and malware

10 per cent by online scams

9 per cent by phishing

7 per cent each for social network profile hacking, online credit card fraud and sexual predation.

HT GRAPHIC: RICHA; ILLUSTRATION: SHRIKRISHANA; SOURCE: AFP

Home Minister Rajnath Singh has said in Parliament recently that there was a need to strengthen cyber monitoring in the wake of growing use of Internet and social media by global terror outfits like ISIS to indoctrinate the youth. The Home Minister was responding to increase concerns by MPs in the wake of arrest of Bangalore professional Mehdi Masroor Biswas for operating a pro-ISIS Twitter account.

The Indian government has set up an expert group to chalk out strategies for effective tackling of cyber crime. The five-member expert study group will prepare a road map for effectively tackling cyber crime in the country and give suitable recommendations on all its facets.

The report stated that obscene publication, transmission of unauthorized contents, credit card and banking frauds are the widespread cyber crimes faced globally. Other cases include spam, phishing, scanning, malicious code and website intrusions. Cyber attacks originated from a number of countries including the US, Turkey, China, Pakistan, Europe, Brazil, Bangladesh, Algeria and the UAE.

Global Futures and Foresight Tweets 2014

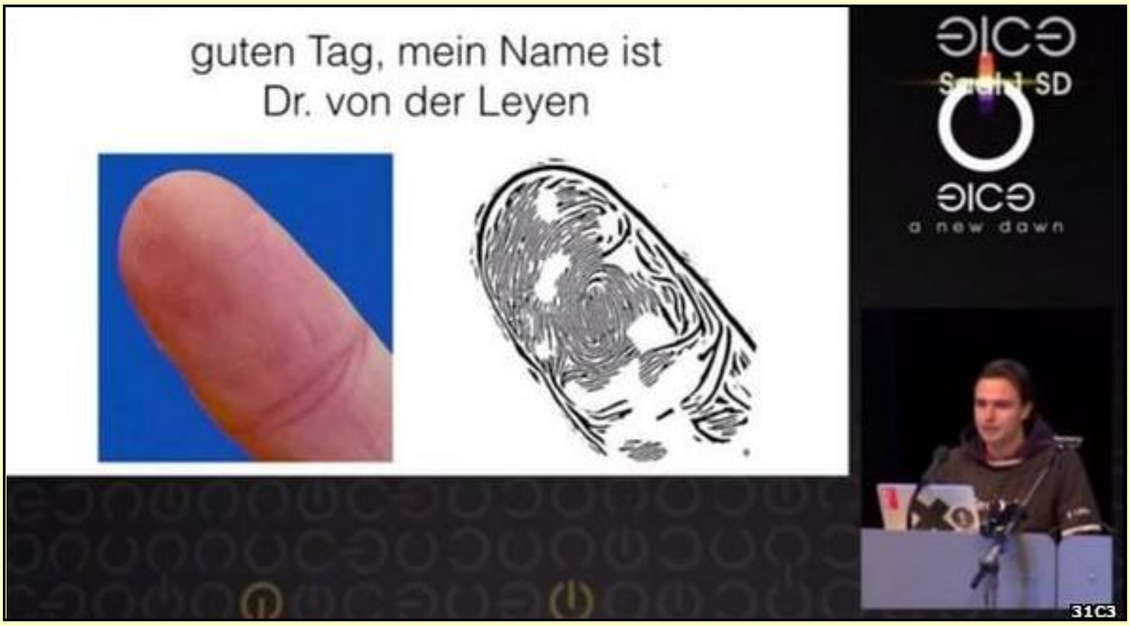
GFF Tweet Deck 2014

Source:http://www.thegff.com/Articles/425685/Global_Futures_and/Reports/GFF_Tweet_Deck/GFF_Tweet_Deck.aspx

Interesting Tweet collection on many topics: Artificial intelligence, big data & analytics, future of education, learining and training, future of health and wellness, future of work, global economy, innovation and business models, IoT, leadership, manufacturing, media, sustainability, urban futures and demographic dividends, what's hot in technology in 2014 **and many more!**

Politician's fingerprint 'cloned from photos' by hacker

Source: http://www.bbc.com/news/technology-30623611



Mr Krissler provided details of his technique at a convention in Hamburg

A member of the Chaos Computer Club (CCC) hacker network claims to have cloned a thumbprint of a German politician by using commercial software and images taken at a news conference.

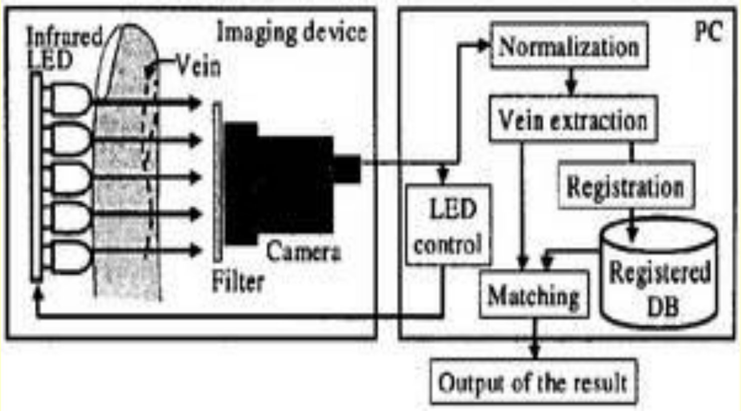
Jan Krissler says he replicated the fingerprint of defence minister Ursula von der Leyen using pictures taken with a "standard photo camera".
Mr Krissler had no physical print from Ms von der Leyen.
Fingerprint biometrics are already considered insecure, experts say.
Mr Krissler, also known as Starbug, was speaking at a convention for members of the CCC, a 31-year-old network that claims to be "Europe's largest association" of hackers.

'Wear gloves'
He told the audience he had obtained a close-up of a photo of Ms von der Leyen's thumb and had also used other pictures taken at different angles during a press event that the minister had spoken at in October.

German defence minister Ursula von der Leyen's fingerprint was cloned just from photos, the hacker claims

Mr Krissler has suggested that "politicians will presumably wear gloves when talking in public" after hearing about his research.
Fingerprint identification is used as a security measure on both Apple and Samsung devices, and was used to identify voters at polling stations in Brazil's presidential election this year, but it is not considered to be particularly secure, experts say.

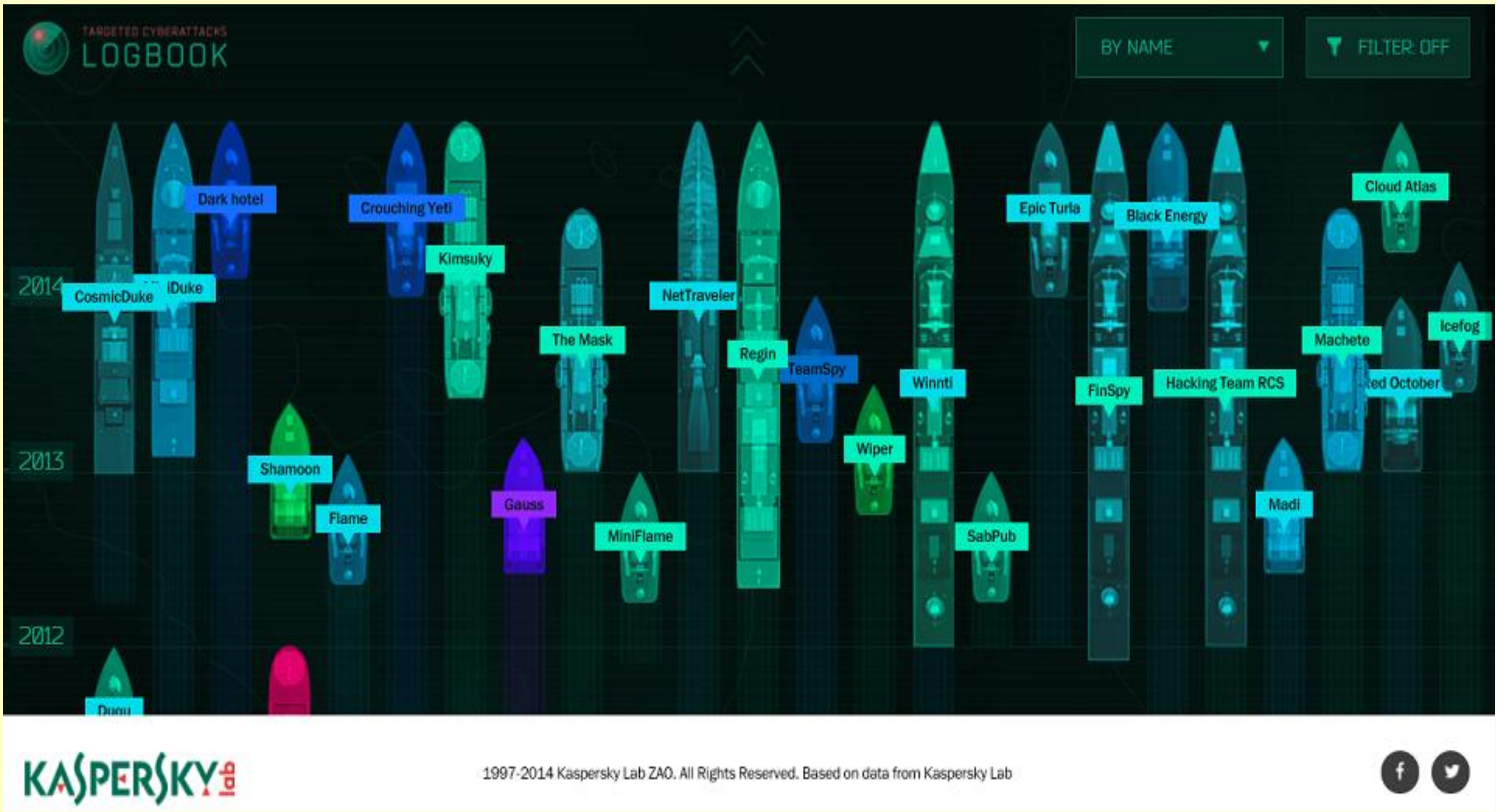
Living biometrics
"Biometrics that rely on static information like face recognition or fingerprints - it's not trivial to forge them but most people have accepted that they are not a great form of security because they can be faked," says cybersecurity expert Prof Alan Woodward from Surrey University.
"People are starting to look for things where the biometric is alive - vein recognition in fingers, gait [body motion] analysis - they are also biometrics but they are chosen because the person has to be in possession of them and exhibiting them in real life."



In September this year Barclays bank introduced finger vein recognition for business customers, and the technique is also used at cash machines in Japan and Poland.
Electronics firm Hitachi manufactures a device that reads the unique pattern of veins inside a finger. It only works if the finger is attached to a living person.
Trials in the intensive care unit at Southampton General Hospital in 2013 indicated that vein patterns are not affected by changes to blood pressure.

Kaspersky Lab Launches Online Radar for the Most Dangerous Cyberthreats

Source: http://i-hls.com/2014/12/kaspersky-lab-launches-online-radar-dangerous-cyberthreats/



1997-2014 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab

As complex operations become an increasingly frequent feature of contemporary cybercrime, Kaspersky Lab is launching an online service that brings together all the information it holds on the most sophisticated cyber campaigns. The interactive Targeted cyberattacks logbook project displays the research and analysis of the company's renowned Global Research and Analysis Team.

Currently, the team's portfolio contains several years' worth of research into 29 major targeted attacks, including high-profile campaigns such as Regin, Darkhotel, Cloud Atlas, and more. Through the new service users can explore links between threats as well as their trends and impact, or investigate the behavior of specific threats.

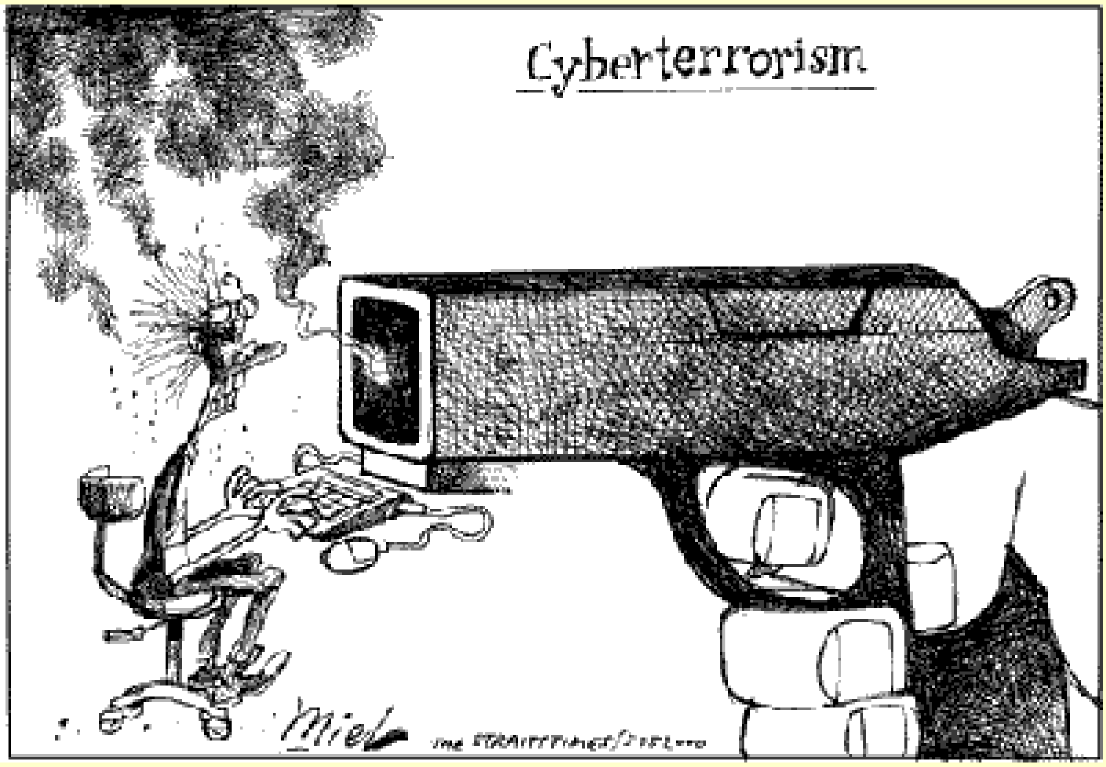
Each cyberattack is displayed on the timeline in the form of a ship: the bigger the vessel, the longer the attack has been in operation. The wake behind the ship shows the time from the detection of the first malware samples to the publication of the results of the research project. The color gradient indicates the number of victims (See above image).

The service makes it possible to view links between different cyber campaigns and retrieve detailed information on each of them, including the geography of infections, the ways in which malware was spread, the cybercriminals' targets and the special features of each attack. A convenient filter helps to sort the attacks by categories, making it possible to home in on those that, for example, only targeted information from private companies, in a specific country, and using certain techniques.

"Four years ago we could regard targeted cyber campaigns as one-offs, but now we are investigating more and more of these incidents every year. They are no longer unique events; they have found a special niche in the world of cyberthreat and demand special attention. That's why we are launching this new online service. We want to demonstrate the scale of sophisticated cyber campaigns and provide a means of evaluating their growth and reach. In 2014 alone, we recorded more than 4,400 victims of targeted attacks on the corporate sector," said Alexander Gostev, Chief Security Expert at Kaspersky Lab.

The Problem With Calling Cyber Attacks 'Terrorism'

Source: http://www.terrorismwatch.org/2015/01/the-problem-with-calling-cyber-attacks.html



Jan 06 – Yesterday, Sen. Robert Menendez (D-NJ), the ranking member of the Senate Foreign Relations Committee, appeared on CNN's*State of the Union* where he proposed placing North Korea on the State Department's State Sponsors of Terrorism list. Menendez contended that the additional sanctions announced by the White House last week were insufficient, and that "we need to look at putting North Korea back on the list of state sponsors of terrorism, which would have far more pervasive consequences." Beyond claiming this would have additional consequences for North Korea, he disagreed with President Obama's characterization of the alleged Sony hack as "an act of cyber vandalism":

"Vandalism is when you break a window. Terrorism is when you destroy a building. And what happened here is that North Korea landed a virtual bomb on Sony's parking lot, and ultimately had real consequences to it as a company and to many individuals who work there."

I recently wrote a piece that questioned the wisdom of placing North Korea on the State Sponsors of Terrorism list, given that—according to the State Department—the "The Democratic People's Republic of Korea (DPRK) is not known to have sponsored any terrorist acts since the bombing of a Korean Airlines flight in 1987." There is no question that North Korean agents engage in any number of malicious and even violent actions in South Korea and beyond, which might be labeled by some as acts of "terrorism." However, the U.S. Secretary of State, who is empowered under the 1979 legislation to determine which countries should be included on the list, concluded that North Korea should not be on the list, and, in fact, the Bush administration removed the country in 2008. Moreover, just as removing North Korea from the list did not open up the country to U.S.exports given the multitude of overlapping sanctions and restrictions, placing them back on it will not have any demonstrable impact.

There are two other points worth mentioning. First, the State Sponsors of Terrorism list was explicitly intended to deal with countries that "aid, encourage, or give sanctuary to those persons involved in directing, supporting, or participating in acts of international terrorism." The list was not supposed to cover what could be considered "state terrorism," which was then a common charge leveled against countries like the United States, Israel, and South Africa at the time. Rather, it was to prevent the sale of weapons to those governments that—over a sustained period of time—had sponsored international terrorism committed by non-nationals. If Menendez believes North Korea belongs on the State Sponsors of Terrorism list, then the original legislation should be re-written to cover all acts of international terrorism conducted by state agents. Or, there should be two lists: one for state sponsors of terrorism, and one for state terrorism.

Second, the Sony hack does not meet the Code of Federal Regulations definition of "terrorism:"

"Terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

If cyberattacks—whether designed to steal, corrupt, disrupt, degrade, or destroy—are considered the equivalent of a "use of force" or "violence" as the definition of terrorism suggests, then there any number of countries that and individuals who should be labeled as terrorists.

In fact, North Korea is not a leading source of malicious cyber activity—the United States is consistently ranked first, and other top sources remain debated. **Symantec reported that the top three country sources of malware in 2013 were the United States (17 percent), China (9 percent) and India (5 percent). Alternatively, though Kapersky also estimates that the United States is the leading source of malicious activity (25 percent), it ranks Russia second (19 percent), followed by the Netherlands (12 percent).**

Rather than misapplying the existing policy tools or diminishing the physical harm and psychological toll of terrorism, Congress should reexamine what new legislation is required to prevent or counter significant costly or damaging cyberattacks. If malicious cyberattacks are considered terrorism, this will result in a default categorization of the United States and many of its allies as sponsors of terrorism. Obviously, it's highly unlikely that the Secretary of State would designate the United States or its allies as such.

Attack on airport VPN bypassed multi-factor authentication

Source: http://www.techworld.com/news/security/attack-on-airport-vpn-bypassed-multi-factor-authentication-security-firm-reports-3375826/

Cybercriminals have found a way to circumvent the multi-factor authentication systems used to protect business VPNs (Virtual Password Networks), according to security firm Trusteer, which has reported a recent targeted attack on an airport network using this method.

For security reasons, Trusteer doesn't reveal the name of the airport, but the attack involved an innovative mixture of standard VPN login grabbing using the Citadel Trojan followed by screen scraping to discover the one-time password (OTP) presented by the gateway authentication system.

The OTP presented was in the form of an on-screen CAPTCHA using 10 digits embedded in an image, hence the need to grab it as a bitmap rather than by intercepting keyboard presses.

According to Trusteer, the unnamed authentication system used a dual-channel approach, offering users the choice of having the OTP sent via the PC (in-band) or to a mobile as an SMS (out-of-band).

The Citadel attack would only work where the PC/in-band option was chosen, which in this case happened to be the default access authentication method for airport employees.

That an airport was attacked was not coincidental, Trusteer said, which means that the criminals were seeking access to the VPN because it was a way into the organisation's systems.

"Once an attacker steals a victim's VPN credentials they can login as the authorized user and have unfettered access to the information and resources associated with the account," said Trusteer's Amit Klein, underlining the obvious security threat.

"It also demonstrates how enterprises that rely on strong authentication approaches are still at risk from targeted attacks if they lack cybercrime prevention security on endpoint devices," he said.

The significance of the attack (apart from the intriguing airport theme) is that criminals have figured out how to get round two-factor authentication using the simple principle of screen grabbing. This is not unheard of but its use in the field to target business systems is still unusual.

It is also possible to infer that in this incident that weaknesses' in the authentication system used to defend the VPN were part of the targeting.

Because the specific authentication CAPTCHA was derived from a static PIN (i.e was a random variation on that PIN), capturing the master CAPTCHA allowed the criminals to reverse engineer the OTP, which meant that access could happen at any point in time, even when the OTP had apparently expired.

The choice of the Citadel banking Trojan is interesting. The software's creators have repotedly developed the malware on an open source platform which is probably why their handiwork now turns up as a ocmpeonnent of all sorts of attacks. Citadel is like a sort of 'drop-in' keylogger.

DRY-CLEANER
USB-STICK-GRIP-AND-READ-OUT-DEVICE
AS OF TODAY: 03526 GB
HERE IS YOUR USB-STICK WITH CONFIDENTIAL INFORMATION ON IT. YOU'D LEFT IT IN YOUR TROUSER POCKET.
THANK YOU FOR YOUR HONESTY, IT'S MUCH APPRECIATED!
CLEANING REVENUES
DATA TRADING REVENUES
© Götz Wiedenroth 2009
www.wiedenroth-karikatur.de

12 Biggest Mistakes when preparing for a disaster

By Juan J Agudelo PhD

Source:https://www.linkedin.com/groupItem?view=&item=5951351550084415488&type=member&gid=106846&trk=eml-b2_anet_digest-hero-7-hero-disc-disc-0&midToken=AQHamrjPnw68nw&fromEmail=fromEmail&ut=0JggSnnE50USw1

Mistake 01

Buying products that require clean water to work. One of the most common effects of a disaster zone is the inability to get clean water".

Mistake 02

Buying products that are heavy and difficult to carry.You have to assume that you may be injured and/or may not have the strength to carry heavy objects after a disaster occur.

Mistake 03

Buying products that are scented or have strong odors. Wildlife is attracted to scent. From mosquitoes to large predators their sense of smell is one of their most effective sources for finding food.

Mistake 04

Buying products that depend on electrical power. One of the first things that fail when a disaster of any kind strikes is electrical power, buying products that require electrical power may be just a waste of money.

Mistake 05

Buying products with short shelf life. Products with less than 3 years of shelf life may be expired and unusable when you really need them.

Mistake 06

Buying only first aid products and forgetting hygiene products that are needed on a daily basis

People will use hygiene products regardless if they are injured or not, but most people buy first aid products and forget what they use on a daily basis.

Mistake 07

Buying based on how cheap the product is instead on how good it works. Everybody wants to save money but when a disaster call you need to have the best most reliable products... your life my depend on them

Mistake 08

Buying products that can't perform for at least 72 hours. The first 72 hours after a disaster are key, most emergency and survival support agencies and institutions can't reach you. If you don't have enough to survive those 72 hours a simple thing such as antibacterial protection could become a serious health issue.

Mistake 09

Taking some common things like wind, sunshine, protection from bugs and water for granted.

When disaster strikes your "normal" environment disappears and too much wind, sunshine and/or bugs can make your survival very challenging.

Mistake 10

Not knowing that after food and shelter is secured the most important issue is your hygiene

In a disaster the possibility of getting sick by contagious diseases grow exponentially with time, hygiene products are just as essential as shelter and food, make sure you have enough.

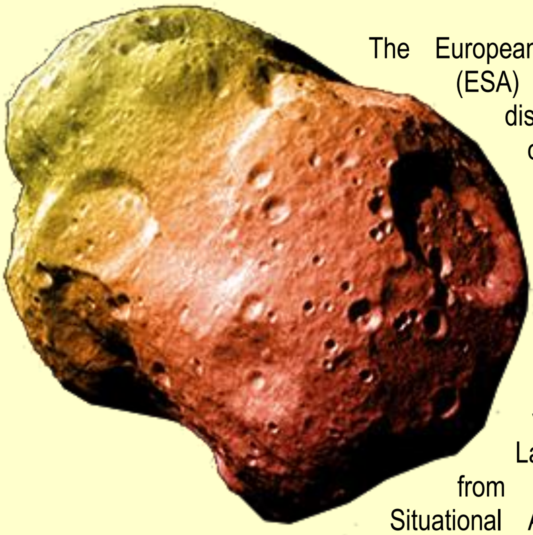
Mistake 11
Counting minimum heads. When people buy their products they should take into account that some people close to them (neighbors for example) may not have theirs or could have lost them in the disaster and then everyone would have to share...

Mistake 12
Buying products that were not designed for an emergency. People sometimes buy products based on price rather than effectiveness and at the time of a disaster they wonder why their products don't perform to the task ahead.

***Juan J Agudelo PhD** is CEO at UNITED SPIRIT OF AMERICA.*

Be prepared: What to do if an asteroid is heading our way

Source: http://www.homelandsecuritynewswire.com/dr20141219-be-prepared-what-to-do-if-an-asteroid-is-heading-our-way



The European Space Agency (ESA) and national disaster response offices recently rehearsed how to react if a threatening space rock is ever discovered to be on a collision course with Earth.

Last month, experts from ESA's Space Situational Awareness (SSA) program and Europe's national disaster response organizations met for a two-day exercise on what to do if an asteroid is ever found to be heading our way.

In ESA's first-ever asteroid impact exercise, they went through a countdown to an impact, practicing steps to be taken if near-Earth objects, or NEOs, of various sizes were detected.

An ESA release reports that the exercise considered the threat from an imaginary, but plausible, asteroid, initially thought to range in size from twelve m to thirty-eight meters — spanning roughly the range between the 2013 Chelyabinsk airburst and the 1908 Tunguska event — and travelling at 12.5 km/s.

Critical times to take action

Teams were challenged to decide what should happen at five critical points in time, focused on 30, 26, 5, and 3 days before and one hour after impact.

"There are a large number of variables to consider in predicting the effects and damage from any asteroid impact, making simulations such as these very complex," says Detlef Koschny, head of NEO activities in the SSA office.

"These include the size, mass, speed, composition and impact angle. Nonetheless, this shouldn't stop Europe from developing a comprehensive set of measures that could be taken by national civil authorities, which can be general enough to accommodate a range of possible effects.

"The first step is to study NEOs and their impact effects and understand the basic science."

How should Europe react

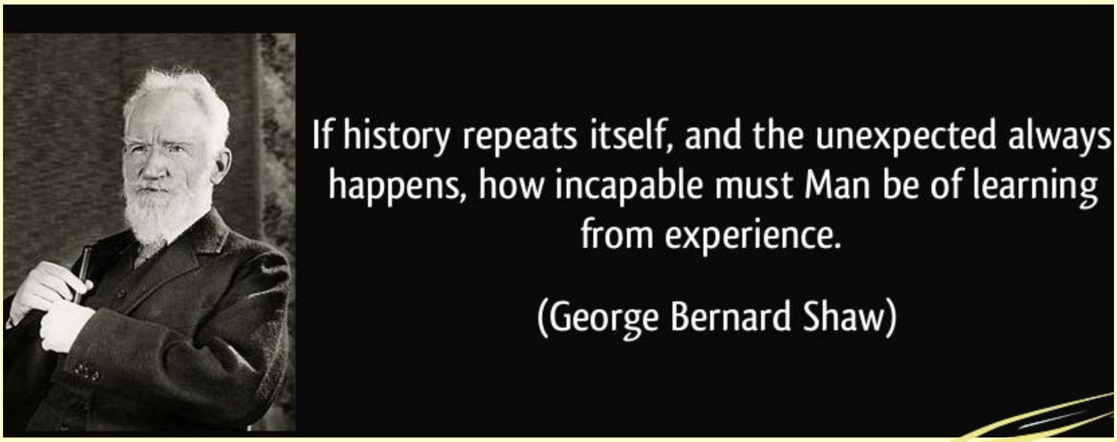
Participants came from various departments and agencies of the ESA member states Germany and Switzerland, including Germany's Federal Office of Civil Protection and Disaster Assistance. They studied questions such as: how should Europe react, who would need to know, which information would need to be distributed, and to whom?

"For example, within about three days before a predicted impact, we'd likely have relatively good estimates of the mass, size, composition and impact location," says Gerhard Drolshagen of ESA's NEO team.

"All of these directly affect the type of impact effects, amount of energy to be generated and hence potential reactions that civil authorities could take."

Chelyabinsk: Injuries due to overpressure

During the 2013 Chelyabinsk event, for instance, the asteroid, with a mass of about 12,000 tons and a size of nineteen meters, hit the upper atmosphere at a shallow angle and a speed of about 18.6 km/s, exploding with the energy of 480 kilotons of TNT at an altitude of 25-30 km.



If history repeats itself, and the unexpected always happens, how incapable must Man be of learning from experience.

(George Bernard Shaw)

While potentially a real hazard, no injuries due to falling fragments were reported. Instead, more than 1,500 people were injured and 7,300 buildings damaged by the intense overpressure generated by the shockwave at Earth's surface.

Many people were injured by shards of flying glass as they peered out of windows to see what was happening.

"In such a case, an appropriate warning by civil authorities would include simply telling people to stay away from windows, and remain within the strongest portions of a building, such as the cellar, similar to standard practice during tornados in the United States," says Gerhard.

In a real strike, ESA's role would be crucial. It will have to warn both civil protection authorities and decision-makers about the impact location and time. It would also have to share reliable scientific data, including possible impact effects, and provide trustworthy and authoritative information.

Establishing internationally coordinated procedures

The exercise ended on 25 November, a significant step forward at highlighting the unique factors in emergency planning for asteroid strikes, and possible courses of action. It also clarified a number of open points, including requirements from civil protection agencies and the type and

time sequence of information that can be provided by ESA's SSA.

It is another step in the continuing effort to set up an internationally coordinated procedure for information distribution and potential mitigation actions in case of an imminent threat.

The release notes that ESA's NEO team is also working with international partners, agencies and organizations, including the UN, to help coordinate a global response to any future impact threat (see "Getting ready for asteroids").

With the aim of strengthening ESA's and Europe's response, similar exercises will be held in the future. The next, in 2015, will include representatives from additional countries.

High Rise Buildings: A Unique Emergency Response Challenge

Source: http://www.d4h.org/blog/post/20141219-high-rise-buildings-a-unique-emergency-response-challenge

The multiple floors of a high-rise building create the effect of requiring a great number of people to travel distances on stairs in order to evacuate the building. High-rise buildings have drawn significant attention in the fire safety world over the years. Here are some of the challenges faced in a high-rise building;

Fire Department Access

Even with modern aerial apparatus, fire services can still only reach six or seven floors of a building, so exterior rescue and firefighting operations are restricted to the lower floors. With fires above this level, firefighters must move vertically inside the building and fight the fire at the same time as occupants are descending the stairs.

Emergency Egress Systems

There is considerable potential for crowding and slow movement on exit stairs in high buildings because of the number of floors and because these stairs do not normally increase in width as they descend, Stair shafts are also one of the primary means by which smoke moves vertically

Effects Of Nature

Stack effect and winds have a major impact on the movement of smoke in high buildings, and tend to be worse the higher the building.

Complex Utility Services

High-rise buildings contain a complex series of pipes, ducts, cables and conduits running vertically. Fire protection water supplies must also be provided from either the top or bottom of the building – both with associated problems.

The 2 Most Rapidly Developing Emergency Management Issues

By Gerald Baron

Source: http://www.emergencymgmt.com/emergency-blogs/crisis-comm/The-Two-Most-Rapidly-Developing-Emergency-Management-Issues.html

Dec 19, 2014 – With Christmas approaching with the speed of an asteroid, it's time to start looking forward to another new year. I'd be interested to hear your thoughts on the big issues facing emergency management and crisis communication.

My two biggies are situation awareness and UAVs. I thought they were two, but as I think about them, they are close to being one and the same issue as I'll explain. Both are going to be central to developments in crisis and emergency communication both will draw the PIO, JIC and comms functions closer into command and operations management and both are driven by absolutely exploding technological innovation.

Knowing what is going on is essential. Sun Tzu pointed that out in *The Art of War* about 2,500 years ago. Emergency management is not war, but if you don't know the situation on the ground, what is happening and what may happen, you are at a severe disadvantage. The opportunities to improve situation awareness have been increased greatly in the past decade, even more in the past two to three years. Yet most response organizations from police and fire all the way to multi-agency disaster response seem to organize and manage using methods that were developed before smartphones and even the Internet were envisioned.

You want a simple example? I would suggest that if the police in Ferguson, Mo., had any idea of what citizens using Twitter and their smartphone cameras were doing and saying, and if they had any idea how that information — false as it may have been — was being shared around the neighborhood and country and globe, would they have responded at the glacial, old world speed they did? I suspect their understanding of the situation on the ground is a bit different today than it was then.

The truth is that managers have access to unprecedented information. Information is not intelligence as many will be quick to point out. But there is little intelligence without information. Much of the technology that will rapidly change situation awareness in the next year or two is focused on this issue of signal versus noise, of information versus intelligence. The best source I know for keeping up on all things related to this is Brandon Greenberg's extremely useful newsletter and website DisasterNet.

But while Brandon did a masterful job of rounding up the Web-based technologies, I think he forgot to look up when talking about technology and situation awareness. In my mind, by far the biggest issue to hit emergency management in general, and situation awareness in particular, in the next five years is in the sky. The eyes in the skies: UAVs or drones. It's true the FAA is doing its darndest to keep these things on the ground — and in the process, according to *The Economist* anyway — forcing innovation in one of the most exciting and promising new tech fields to come along since, well, the WWW, into places like China, Germany and Switzerland. But I am convinced that despite the FAA's best efforts, the eyes in the skies will be with us. And that means for good or ill, emergency managers and communicators will need to deal with the implications.

As an example of just how far the discussion is coming, I strongly encourage you join up with Patrick Meier's (irevolution.net) forum called UAViators (pronounced "waviators"). On Nov. 6 a meeting was held at the United Nations to get a discussion going about the humanitarian use of drones (I've given up on trying to change to UAVs, drones it is). The result is very interesting and worth a close look. You will learn what is happening around the world as governments, companies and humanitarian organizations begin to adopt and deploy this important technology.

I know, I know. You are thinking, jeez, I just started getting used to the idea of Twitter and tweeting and this crazy social media stuff and now you tell me I have to get educated about drones. Well, yes. Because the eyes in the skies, combined with the world's biggest transmitters we carry in our pockets will combine to share information around the world faster, with greater depth and detail, and with more storytelling oomph than ever before. Did we need more storytelling oomph than that demonstrated by @theepharoah in the shooting of Michael Brown? Imagine the scene captured by the eyes in the skies.

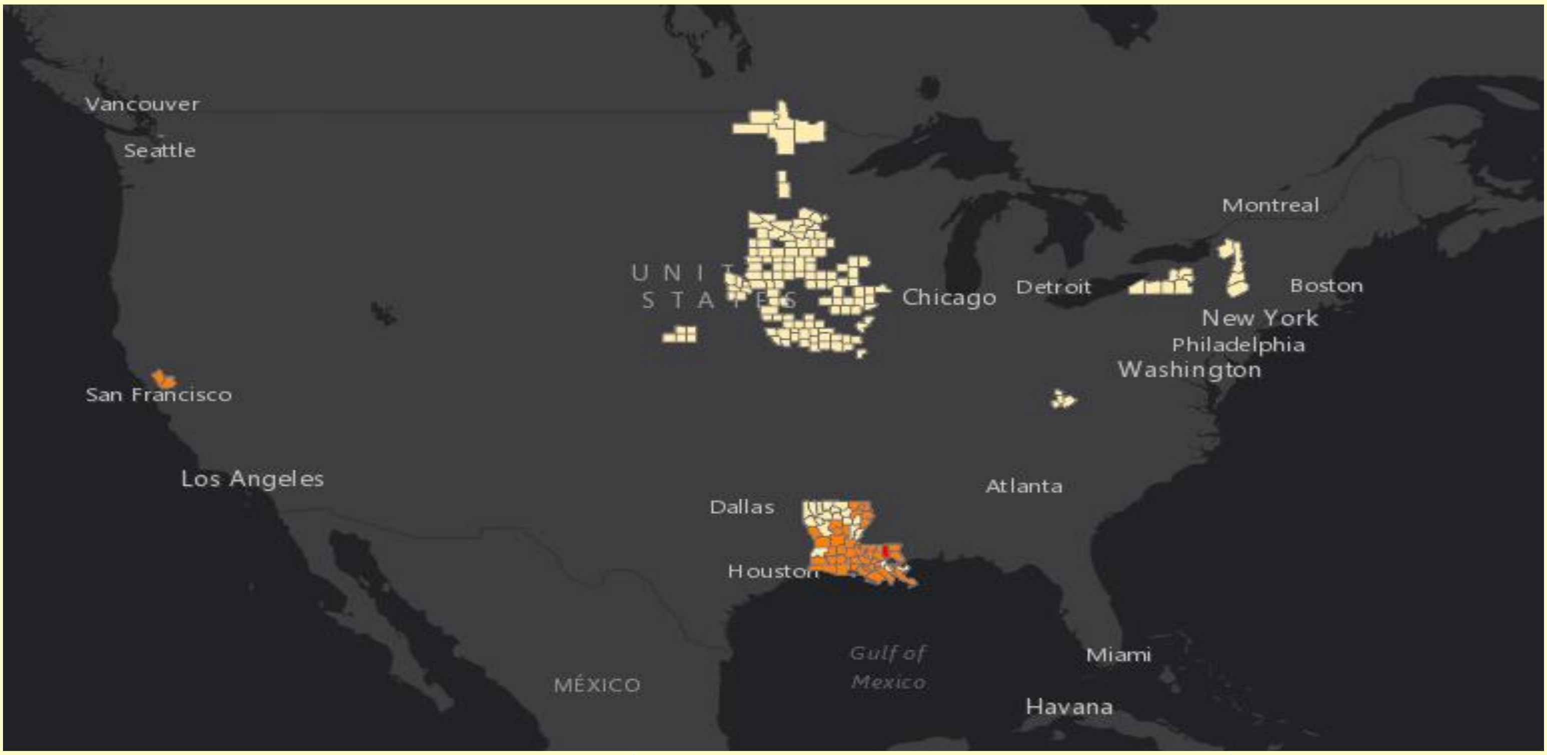
Imagine the eyes in the skies after an earthquake, flood or landslide. Imagine them during an oil spill or huge toxic release. Imagine them during an active shooter, another marathon bombing, an apartment fire. They will be there. And both incident commanders and PIOs will soon be dealing with them.

Of course, I may be wrong about all this. After all, I'm the one who said after Twitter came out, who in the world will want to know what kind of latte I'm drinking?

*Crisis Comm by **Gerald Baron** covers crisis and emergency communication strategies.*

White House Launches Open Data Disaster Portal

Source: http://www.emergencymgmt.com/disaster/White-House-Open-Data-Disaster-Portal.html



Disasters.data.gov was designed to foster collaboration and the continual improvement of disaster-related open data and tools.

Dec 16, 2014 – The White House launched a new open data portal on Dec. 15, targeting the needs of first responders and emergency survivors. The website, found at disasters.data.gov, features disaster-related data sets, tools and resources for those who want to join a larger community of data-minded first responders.

The website features data (more than 100 sets) that can be sorted by type of disaster — earthquakes, floods, hurricanes, severe winter weather, tornadoes and wildfires — as well as tools and apps, and information about how to get involved or join challenges like the current Innovator Challenge, which calls for ideas on how to reduce flooding fatalities.

The **Innovator Challenge** listed as of the date of this report is the first in a series that are intended to highlight the needs of the disaster preparedness community.

The website was born from the White House Innovation for Disaster Response and Recovery Initiative, a project launched in response to Hurricane Sandy that aims to turn technology into empowering tools that can save lives. The initiative has manifested in the form of a hardware hackathon for disaster preparedness and partnerships with both the private and public sectors, but this portal represents the first unified online resource for such efforts.

Emergency Response: The Importance of Fire Extinguishers

Source: http://www.d4h.org/blog/post/20141226-emergency-response-the-importance-of-fire-extinguishers

With all of the benefits that fire extinguishers provide for us, it is surprising that we don't appreciate them more. In fact, the only time we tend to think about them is when we need them in an emergency. The only time we really hear about them is when they are unavailable, or when they are unable to do their job.

Fire extinguishers are the most common types of fire safety equipments that are installed in almost every types of establishment these days. There are a number of different types to be aware of:

Different Kinds of Fire Extinguishers

Wet chemical extinguishers

Fire caused due to oil is difficult to extinguish by water as it floats above the layer. This where Wet chemical extinguishers come in.

Carbon-dioxide extinguishers

This is used to deal with electrical fires that break out in certain areas.

Wet chemical

Carbon-dioxide

Water fire

Powder fire

Water fire extinguisher

This type of Fire extinguisher is useful in combating with fire caused due to flammable substances such as paper, wood and other organic materials. As it is water based, so extinguishing fires caused by short-circuits is not possible.

Powder fire extinguisher

This type of extinguisher is used to deal with fires that are caused by flammable solids, liquids and gases as well as electric fires. Developed recently, these extinguishers are found in almost every building these days.

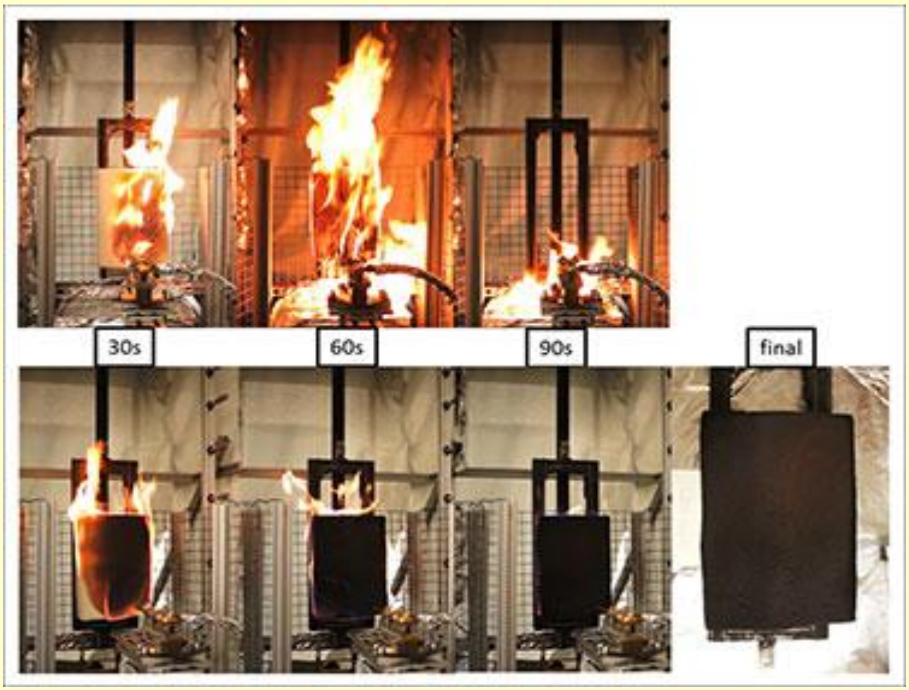
Foam extinguishers

It is the choice for tackling fires caused by flammable liquids and solids. Not suitable for electrical fires.

Nanomaterial proves to be a better flame retardant than chemical alternative

Source: http://www.homelandsecuritynewswire.com/dr20141229-nanomaterial-proves-to-be-a-better-flame-retardant-than-chemical-alternative

In a face-off between two promising flame retardants, the challenger — a nanomaterial that maintains a positive façade while sheltering a negative interior — outperformed its chemical antithesis. This material already is a leading candidate for environmentally friendly fire-resistant coatings on furniture foam.



Open-flame tests compare the flammability of untreated polyurethane foam (top) and an identical foam sample surface treated with a sandwich-like coating incorporating layered double hydroxides. By 90 seconds after ignition the untreated foam is completely consumed. The experimental flame retardant formed a protective residue that caused the size of the flames to decrease and then to extinguish. Credit: NIST

Gram for gram, sandwich-like coatings with a so-called layered-double-hydroxide (LDH) center reduce the flammability of polyurethane foam more than comparable surface treatments with montmorillonite clay, report fire prevention researchers at the National Institute of Standards and Technology (NIST). NIST says that Montmorillonite clay already is considered a promising, environmentally friendly replacement for older flame retardants, but LDH-based coatings can be applied in smaller amounts, resulting in fewer fabrication steps, according to the NIST team.

Both coatings are about twice as effective in blocking fire in polyurethane foam than current commercial flame retardants, several of which have been linked to human health risks and environmental problems. Polyurethane foam, which is extremely flammable, is the primary cushioning material used in furniture and other soft furnishings. Upholstered-furniture fires cause the largest number of household fire deaths and injuries, according to the National Fire Protection Association.

Discovered in 1942, naturally occurring LDH materials — and, more recently, their synthetic counterparts — are being eyed for a variety of uses, including controlled drug release, anticancer therapies and catalysis. These potential applications would exploit the same chemical structure that appears to make LDH materials good flame suppressants.

With a molecular structure of two positively charged outer layers that cloak a negatively charged middle, LDH forms a protective char layer when exposed to fire. Montmorillonite clay acts much the same, but has the opposite arrangement of electric charges. The LDH configuration confers two apparent advantages, the scientists say. First, LDH releases water at high temperatures, which dilutes the underlying foam. Second, LDH's outer layers absorb heat as they breakdown, which reduces the temperature of the foam.

As in their previous research on experimental flame retardants, the NIST team inserted the competing nanomaterials between layers of common polymers to create a three-layer arrangement. They then pile the trilayers one on top of another, creating stacks one to five trilayers high. In the case of LDH, layer-by-layer assembly resulted in uniform distribution of the material, which has been difficult to achieve with other methods.

In benchtop open-flame tests, the scientists found that two stacks of trilayers containing LDH provided the best protection. Compared with untreated polyurethane foam, the double-decker arrangement reduced peak heat release by 41 percent and average heat release by 79 percent, performing slightly better than triple-decker stacks of trilayers containing montmorillonite clay.

Although the two types of coatings performed similarly, "the LDH was at least 60 percent lighter and 50 percent faster to fabricate than the best montmorillonite clay coating," the researchers write.

If maximum flammability reduction is desired, the researchers recommend considering another experimental formulation they have tested: a bio-based coating that incorporates DNA, chitosan (a material in crab and shrimp shells), and montmorillonite clay. Combinations of these ingredients, however, must be stacked twenty layers high to achieve optimal performance.

— Read more in Yu-Chin Li et al., "Layered double hydroxide-based fire resistant coatings for flexible polyurethane foam," Polymer *(15 November 2014) (doi:10.1016/j.polymer.2014.11.023); and see "All-Natural Mixture Yields Promising Fire Retardant" in NIST* Tech Beat, *3 June 2014*

Italy ferry fire: Criminal probe launched as eight confirmed dead while Norman Atlantic boat found to have safety 'deficiencies'

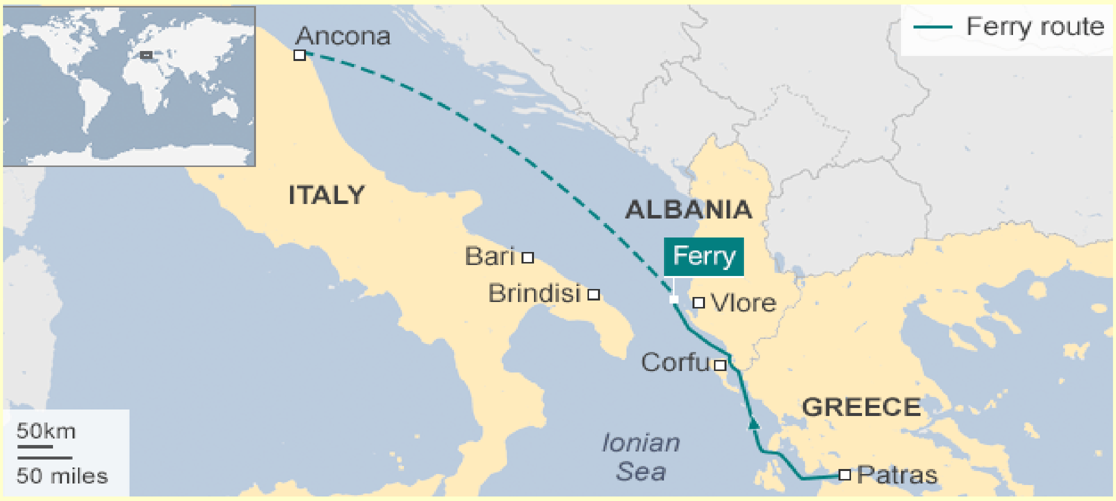
Source: http://www.independent.co.uk/news/world/europe/norman-atlantic-ferry-fire-criminal-probe-launched-into-how-blaze-started-and-escalated-9947905.html

Dec 29, 2014 – Italy opened a criminal investigation today into the ferry fire which broke out yesterday morning and killed five as a safety inspection prior to sail shows there were "deficiencies" with the fire doors and emergency systems.

Prosecutors in the Italian port of Bari opened the case to examine whether negligence played a part in the catastrophe on the Norman Atlantic vessel.

Eight people have died, coastguard spokesman Nikos Lagadianos confirmed, and all the passengers and crew on the ship have since been evacuated.

The Italian owner of the boat, Visemar Di Navigazione, has insisted that the vessel was in full working order and had passed a technical inspection on 19 December, as reported by AFP.



However, an online report by ship safety organisation Paris MoU into the same investigation on 19 December states that some fire doors had malfunctioned and emergency system parts were "missing".

It is not known if they were repaired before the ferry left the port.

One Greek man was found dead after he became trapped in a lifeboat chute with his wife, who suffered injuries. Nearly 480 people were stranded and sleeping on the cold and wet top decks overnight while trying to escape the spreading flames.

The investigation will also explore how the blaze on the car deck had started, at 6am local time, and how it had spread so quickly that the plastic on passengers' shoes started to melt.

A cook on the ship is reported to have said in a call to his wife: “I cannot breathe; we are all going to burn like rats. God save us.”

The news of the four subsequent deaths reached dry land when a cargo ship that had rescued 49 people, including four children, docked in Bari.

Six British people were on board the Italian-owned Norman Atlantic vessel that was sailing to Greece from Italy.

Greek Shipping Minister Miltiadis Varvitsiotis has said that due to the stormy conditions the rescue operation proved extremely difficult in saving passengers.

He had said: “We are doing everything we can to save those on board and no one, no one will be left helpless in this tough situation.

“It is one of the most complicated rescue operations that we have ever done.”

EDITOR'S COMMENT: I followed this tragic incident from the very beginning. Below are the first lessons learned:

- Ship's captain delayed (hours) to declare a state of emergency;
- Weather front was so tremendous that forbitten Greek S&R helicopters to approach the burning vessel (we have to realize that helis are machines with certain limitations – although often called "all weather" helicopters). In the mean time burning flame entered Italian national seas;
- Ship's crew was not prepared to execute evacuation of passengers (this is the importance of "exercise-exercise-exercise" we always say to others but never do it in our own premises for a once in a life time emergency);
- Any deviation from SOPs leads to bloodshed and death (trucks' drivers were allowed to sleep in their vehicles in sealed compartments of the ship – and burned);
- Ship' s crew did not perform security check in loaded trucks usually carrying illegal immigrants from Greece to Italy (they enter after security checks in Patra's Port);
- Ship was not towed to closest port in Albania; instead it was towed to Brendisi Port, Italy;
- Communication between Italian (in charge) and Greek (supporting) Operations Centers was problematic; mass media provided better public information then official gov bodies;
- Passengers never participated in an on-board emergency drill and alarms did not activated (or were not strong enough to be heard);
- Evacuation of passengers did not follow the traditional sea rules (children, women, elderly, men) – the low of the strongest prevailed (mainly because there were no ship's officers in charge of the process);
- Passengers were left for hours without water and food (somebody should have thougth about it);
- Greece provided an additional frigate (traveling for hours in full speed under extreme difficult weather conditions from Aegean Sea to the incident site. Italian Navy was not activated from the very beginning. And when *San Giorgio* class amphibious transport dock (LPD) arrived close to Norman Atlantic had no helicopters on it (used as a landing base for operating Italian helis);
- There is no space for national selfishness (I can do it no matter what); Greece had a heli fleet ready to operate but did not get final approval (or got late approval). Bigger helis should be used to minimize evacuation time;
- Evacuated passengers distributed in many different places and until know nobody knows who is where (to make a list with names [written with the right spelling] and inform Operational Center in charge is easy but somebody forgotten to ask for it);
- Finally: it is a crime to let vessels like Norman Atlantic to carry souls and properties just because some papers give permission for this.

Accidents like this one are rare but the unexpected always happens! Let us pray that this time "problems identified" will become "lessons learned"!

We applause both Italian and Greek resque crews (civilian and military) for their high professionalism and self-sacrifice they showed under extreme weather conditions trying to save their fellow citizens!

S&T's Interoperable Solution Makes It Easier and Cheaper for First Responders to Communicate

Source: http://www.dhs.gov/science-and-technology/can-you-hear-me-now

A new low-cost interoperability solution developed by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) could save the first responder community millions of dollars.

The **Radio Internet Protocol Communications Module (RIC-M),** used by local, state and federal responders, is a low-cost, external, stand-alone, interface device that connects radio frequency (RF) system base stations, consoles and other RF equipment – regardless of brand – over the Internet or Private Internet Protocol (IP) network. **The RIC-M converts from a commonly used V.24 serial communications protocol to an open-standard Voice-over-Internet-Protocol (VoIP). Both encrypted and unencrypted Project 25 (P25) digital communications are supported, and it can also operate with analog communication equipment.**

"In the past, legacy systems were not interoperable," explained S&T First Responders Group (FRG) Program Manager Christine Lee. "If you bought one brand of base station, you had to buy the same brand for the all other components even if other brands offered more economical choices or better options. RIC-M allows first responder organizations to be free from dependence on expensive, single-vendor communication solutions, offering cost savings and wider variety."

Base stations are used by law enforcement, medical and other agency dispatchers to communicate with first responders and agents in the field. **Using the RIC-M, agencies can easily upgrade and reconfigure legacy systems for less than $500**, Lee stressed.

"Instead of having to replace an entire system – which can cost as much as $15,000 – when one component breaks or becomes obsolete, organizations can use any RIC-M compatible product to extend the system's life for another 10 to 20 years," she said.

Since its conception in 2012, RIC-M has been successfully field tested with various state and federal response agencies including Montgomery County, Maryland; U.S. Customs and Border Protection; Federal Protective Service; the Federal Bureau of Investigation; the U.S. Marshals Service; the Department of Justice and the Department of the Interior, Office of Law Enforcement and Security.

"The biggest benefit of the RIC-M is that it will allow agencies continue to use current stock pile and installed legacy equipment," said Carter Blumeyer of Rivada Port Graham Solutions, who participated in the fielding as an evaluator. "This legacy equipment is solidly built and still could last more than 10 years from now."

FRG has submitted patent and trademark applications for RIC-M. They also worked with the inventor, who recently signed a licensing agreement allowing for RIC-M's commercialization. This is the first licensing agreement S&T has signed with an inventor. In addition, S&T plans to provide licensing agreements with other vendors to commercialize the RIC-M.

Injectable treatment for internal bleeding could save lives in out-of-hospital emergencies

By Emily Hough

Source: http://www.crisis-response.com/comment/blogpost.php?post=65

Jan 07 – **A team of researchers from Texas A&M University and Massachusetts Institute of Technology (USA) is developing a revolutionary injectable treatment for internal bleeding, the leading cause of death on the battlefield.**

Currently, many treatments for internal bleeding rely on putting pressure on the affected area to staunch the flow of blood. But some injuries are incompressible, and getting injured victims to a medical facility can take at least half an hour to an hour in an emergency situation. For those with internal bleeding, this hour could be fatal.

The researchers from MIT and Texas A&M set out to solve this problem. **Using hydrogel and two-dimensional nanoparticles, they created an injectable substance that works without applied pressure and rapidly decreases the time it takes for blood to clot.** **Animal models have shown the treatment to reduce clotting time from five minutes to one minute.**

Unlike other injectable treatments, which can spread to other parts of the body and cause harmful clotting, this team's treatment solidifies at the site of the wound to aid in coagulation solely in the targeted area.

Akhilesh Gaharwar, assistant professor of biomedical engineering at Texas A&M and a member of research team, revealed that the team plans on further developing the biomaterial to create a two-pronged treatment that would not only aid in coagulation, but also in the formation of new blood vessels.

Research is still in early testing, but this treatment could be lifesaving, both on the battlefield and in crisis response.

First responders could carry around syringes with this injectable treatment, and administer it to patients with haemorrhaging. This would provide these patients with enough time to get to a medical facility, thus significantly increasing their chances of survival.

Ingestible sensors can deliver vital signs to doctors in a disaster

By Emily Hough

Source: http://www.crisis-response.com/comment/blogpost.php?post=57

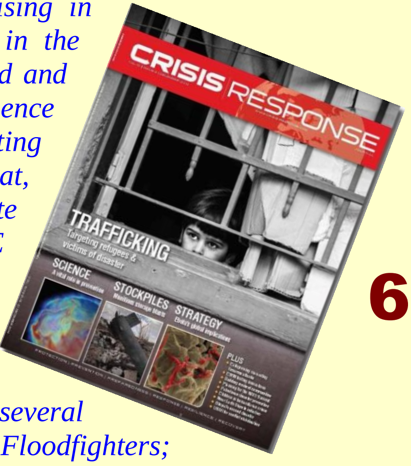
Imagine a massive earthquake strikes a major metropolitan area. Hundreds, if not thousands, wait for medical attention. Simple triaging and monitoring patients requires manpower in an already stressed and overworked environment. What if patients could take a pill that will digitally transmit vital patient information to health care workers on their smart phone? This scenario may happen sooner rather than later.

The FDA recently approved ingestible sensors that will deliver vital signs on a patient's medical adherance and response to therapy to doctors on their phones. **Proteus Digital Health, Inc. has developed a sand grain-sized device, the Ingestion Event Marker (IEM) that can be taken orally and once it reaches a patient's stomach it sends a unique signal to a patch worn on the patient's skin.** The information received by the patch determines the time the ingestible sensor was taken, the amount of time it took for it to digest, and other physiological and behavioral metrics like heart rate. Healthcare workers can access this information on their smartphone.

Ingestible health sensors can be taken orally and, once they reach a patient's stomach, send a unique signal to a patch worn on the patient's skin - healthcare workers can access this information on their smartphone. Photo courtesy Proteus Digital Health, Inc

This new technology is designed to monitor vital signs and medication adherence and patience response to therapy. However, it is not farfetched that in the near future a similar ingestible sensor may be developed specifically for disaster response. Triaging patients in an emergency situation may become more efficient, thus allowing healthcare workers to efficiently serve those in dire need.

***Emily Hough** is Editor in Chief of Crisis Response Journal, which she launched ten years ago. She works both in print and online, specialising in international publishing, events and conferences, mainly in the fields of disaster and crisis management. Emily has founded and organised high-level conferences and seminars in the resilience and response field, identifying global trends and anticipating future hazard scenarios. She has chaired, spoken at, moderated, acted as rapporteur and helped to curate numerous international events, including: The 22nd OSCE Economic and Environmental Forum in Vienna, Austria, (2014); the United Nations Global Platform in Geneva, Switzerland (2013); UNISDR Heritage and Resilience event in Venice, Italy (2012); several European Commission Civil Protection Forums, Brussels, Belgium; several IDER conferences (Rome, Italy; Brussels, Belgium); Floodfighters; National Risk; Counter-Terror Expo; and events at the Royal United Services Institute and the UK Foreign and Commonwealth Office's Wilton Park.*

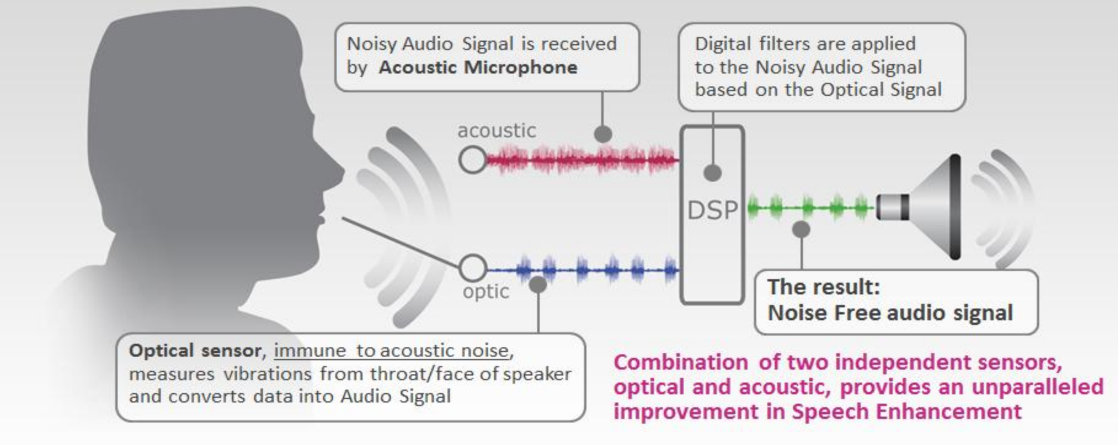


New optoelectronic microphone substantially enhances a speaker's voice over any background noise

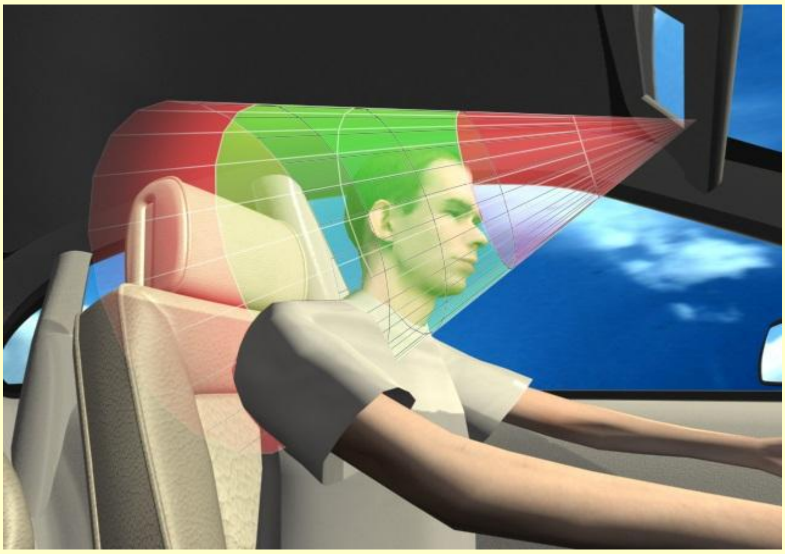
Source: http://i-hls.com/2015/01/new-optoelectronic-microphone-substantially-enhances-speakers-voice-background-noise/

In the course of unfolding criminal incidents, terrorist attack and other homeland security events, one of the primary factors disrupting communications between the various first response forces is none other than background noises. Whether the vocal data is relayed between two people or whether it is designed to activate digital systems, the higher and clear the sound that is

being relayed, the better the performance human systems and elements can achieve.
Development of unique optoelectronic microphone is at the foundation of the technological effort to screen background sound and improve audio quality. This technology enables enhancing the speaker's voice using two sensors: a standard acoustic microphone and an optic sensor capable of deciphering the user's voice while screening background noises.
Established in 2009, Israeli startup company VocalZoom has developed the unique laser-based technology called SEEON – Speech Enhancement Electro Optical Microphone, thanks to which a unique optoelectronic microphone is able to substantially enhance a speaker's voice over any background noise. The technology creates a "virtual cube" in space, sensing sound from only within the cube. This enables highly significant speech enhancement and precise speaker isolation, which are the key elements missing today to enable mass-usage of voice-driven applications for devices such as radios and smartphones. This was recently patented in the US.


Noisy Audio Signal is received by Acoustic Microphone
Digital filters are applied to the Noisy Audio Signal based on the Optical Signal
acoustic
DSP
optic
The result: Noise Free audio signal
Optical sensor, immune to acoustic noise, measures vibrations from throat/face of speaker and converts data into Audio Signal
Combination of two independent sensors, optical and acoustic, provides an unparalleled improvement in Speech Enhancement

VocalZoom's innovation has caught Motorola's attention. The latter recently announced that its investment arm Motorola Solutions Venture Capital has invested in the Israeli startup company, dubbed 'a leading developer of sensors for speech enhancement'. Other VocalZoom investors in this series of funding include existing investors 3M and OurCrowd, as well as new investor FueTrek (Japan). The terms of the transaction were not disclosed, but Motorola usually invests in the framework of cash-for-shares swap deals.



VocalZoom's innovation is applicable to both military and civil uses. Pic: courtesy of VocalZoom.

Motorola Solutions *Sr. Investment Manger* Ami Isakov told *i-HLS* that prior to the investment, Motorola looked into this technology and the potential to integrate it into its own systems. "We are currently in the process of evaluating the technology. We believe VocalZoom's highly accurate sensor will enable us to greatly enhance the company's value and underscore the distinction of our out solutions, some of which have been developed in Israel."
"SEEON has the potential to be the difference of whether a firefighter or a police officer can communicate at a dangerous incident or a fire scene," said Paul Steinberg, chief technology officer at Motorola Solutions. This can be the difference between life and death for them or the people they are protecting, or the difference between whether a criminal is apprehended or escapes."

Are You Prepared for a Mass Shooting at Work?

Source: http://codenameinsight.blogspot.it/2015/01/are-you-prepared-for-mass-shooting-at.html

Jan 8 – **A few decades ago, a mass shooting was a rare event.** These days it is happening with more and more frequency. Yesterday's mass shooting in Paris is the most recent even to send the media into frenzy and the general public into a minor panic.

I say minor because no one ever thinks such a thing will happen to them. Yes, we know that it *could happen* but really, what are the odds? Whether the shooter is a mentally ill person targeting children at school or religious terrorists striking in such a way as to receive the most media coverage possible, there is a very, very slight possibility that such a thing could happen to *you*. Are you prepared?

Now I won't say that the office workers targeted in Paris weren't prepared--one of the people targeted even had his own police guard because there had been threats on his life and if you aren't even safe with someone guarding you then, well, there isn't much that I can say that would be of use. However, **for the average person, there are some things that can be done to prepare for such a scenario:**

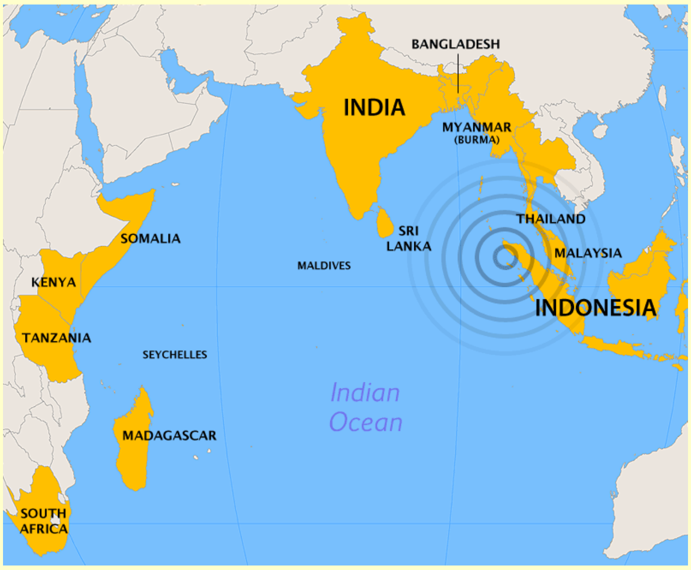
- Always be on alert. Be aware of your situation--where you are, who is around you, what is happening. Most people wander around on auto pilot and someone could be pulling out at Uzi and the people walking by wouldn't even take notice of such a thing.
- Be inconsistent. Obviously this is easier for some people than others but being consistently inconsistent in your schedule and activities makes you, specifically, a more difficult target.
- Make sure your workplace has a security plan. The more comprehensive the plan, the better.
- Carry a concealed firearm and know how to use it. When it comes down to it, the (second) best response to someone shooting at you is for you to be able to shoot back.
- I say that shooting back is the second best response because, if possible, your best response to an active shooter situation is for you to be able to escape immediately from the area. Sometimes this is possible, sometimes it isn't, but by the time you get into a firefight, it's iffy if you will even survive such a confrontation.
- Practice multiple responses to a mass shooter in your home/office/work area/etc. Where would you hide? How many ways could you escape? Is there cover and concealment if you do need to take up a defensive shooting position?
- If you are going to carry a firearm is it licensed? Are you licensed to carry a concealed weapon? Do you have extensive training not only the basics of using a firearm but using it in a tactical situation? Do you practice tactical shooting on a regular basis?
- Are you in good physical condition? You can't run away from an active shooter if you can barely walk a block without having to stop and catch your breath. You can't hide in certain advantageous places if you can't even squat down in a hidey hole without throwing out your back. Plus, if you need to make a last ditch effort at saving yourself by physically attacking your attacker, the better condition you are in, the slightly better your chances are of being successful at this.
- Always attempt to have multiple layers of security around you. In the same way you want multiple layers of security at your home (a perimeter fence around your property, a couple of dogs in the yard, reinforced doors and locks on your home, an interior and exterior security system in your home, a safe room in your home), you want the same emphasis on multiple layers of security at work if possible (a guarded gate to get into the facility, a secure way to enter and exit the facility itself, securable interior spaces, etc). Obviously this isn't possible in all types of employment scenarios, especially if you work with the public.

The bottom line is that anytime there is a workplace or school shooting, people aren't prepared because, psychologically, no one thinks it will happen to them. Also, due to the randomness of such a situation, there is no step-by-step guide that can be given to you that says "if you follow this plan, you will be able to save yourself." Each active shooter situation will be different necessitating variable responses depending on what is happening on a minute-by-minute basis. A little practice and preparation on your part, however, can only be a positive thing in preparing you for the remote possibility of such an incident occurring at your workplace.

SORRY, TIM, ORDINARILY THERE WOULD HAVE BEEN QUITE THE CROWD UP HERE TO WELCOME YOU...
...BUT YOU WENT AND SAVED THEM ALL!
NORTH SHORE SEARCH RESCUE
©IRICE14

World marks 10 years since Asia tsunami

Source: http://www.aljazeera.com/video/asia-pacific/2014/12/asia-tsunami-anniversary-2014122612932890841.html



Dec 26, 2014 – A decade has passed since the Indian Ocean tsunami killing quarter of a million people and damaged hundreds of thousands of homes.

Memorial services for the lives lost during the disaster are under way in almost all affected countries on Friday.

Al Jazeera's Step Vaessen, reporting from the Indonesian Aceh province, worst affected by the tsunami, said an official ceremony there would would be attended by the vice president.

"There will be prayers, songs and poetry but most importantly most of the survivors will have their own commemoration services. They will have their prayer sessions **in** their villages, sometimes villages very near to the sea where they can remember what happened ten years ago," she said.

Aceh was the closest to the earthquake epicentre. At least 170,000 people were killed there.

2004 Tsunami

A 9.3 earthquake off Indonesia triggered the tsunami that killed at least 220,000 people

- Indonesia: 170,000
- Sri Lanka: 31,000
- India: 16,400
- Thailand: 5,400
- Other Asian countries: 200
- East Africa: 300

Sri Lanka will mark the anniversary with a symbolic ride of a train the tsunami had derailed, killing 1,270 passengers.

The train will be powered by the same locomotive and feature five of the original carriages.

In Thailand, 5,395 people were killed, among them about 2,000 foreign tourists. Almost 3,000 people remain missing.

Al Jazeera's Veronica Pedrosa, reporting from Khao Lak, said the Swedish government is organising a commemoration at the Orchid

resort.

She said "543 Swedes were killed at this resort alone".

© Reuters

"It is indeed a very difficult moment and I think that's what's different about the way it's being commemorated here in Thailand, that so many people from all over the world were here because they were foreign tourists," she said.

Thai commemoration ceremonies will be held in several other locations including Ban Nam Khem, a southern fishing village destroyed by the wave.

Government agencies and several non-governmental organisations responded to the disaster across the region by building houses for the victims and providing fishing gear and trawlers to fishermen. But the help does not seem enough.

Many survivors still struggle and have barely managed to rebuild their lives.

While billions of dollars of aid have poured in, some have regained prosperity but others find their lives still hanging by a thread, and a $400m warning system built to help keep residents safe has been undermined by mismanagement and waste.

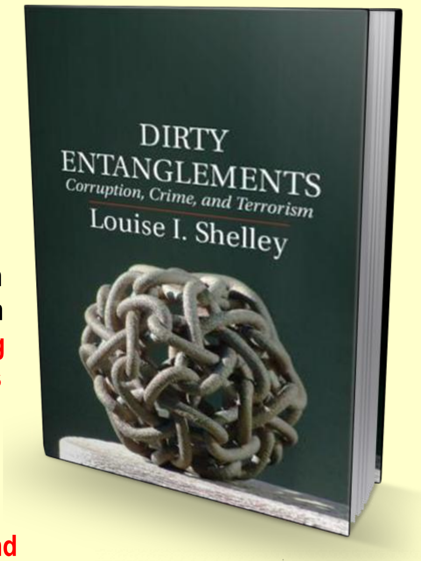
Terrorists use human trafficking to generate revenue, demoralize adversaries, fill the ranks

Source: http://www.homelandsecuritynewswire.com/dr20141231-terrorists-use-human-trafficking-to-generate-revenue-demoralize-adversaries-fill-the-ranks

Dec 31, 2014 – Counterterrorism initiatives tend to target drug trafficking rings operated by militant groups as a way to cut the funding of terror operations. **Terror groups, however, including the Islamic State (ISIS) and Boko Haram, have always diversified their revenue stream by relying on the sale of women and children from captured villages to fund their operations.**

According to the *Daily Beast*, **for as little as $25, a young girl from the minority Yazidi region of Iraq can be purchased**. In his 9 May video, Boko Haram leader Abubakar Shekau threatened to sell the roughly 276 girls kidnapped from a boarding school in Chibok, Borno state. “There is a market for selling humans. Allah says I should sell. He commands me to sell. I will sell women,” Shekau said.

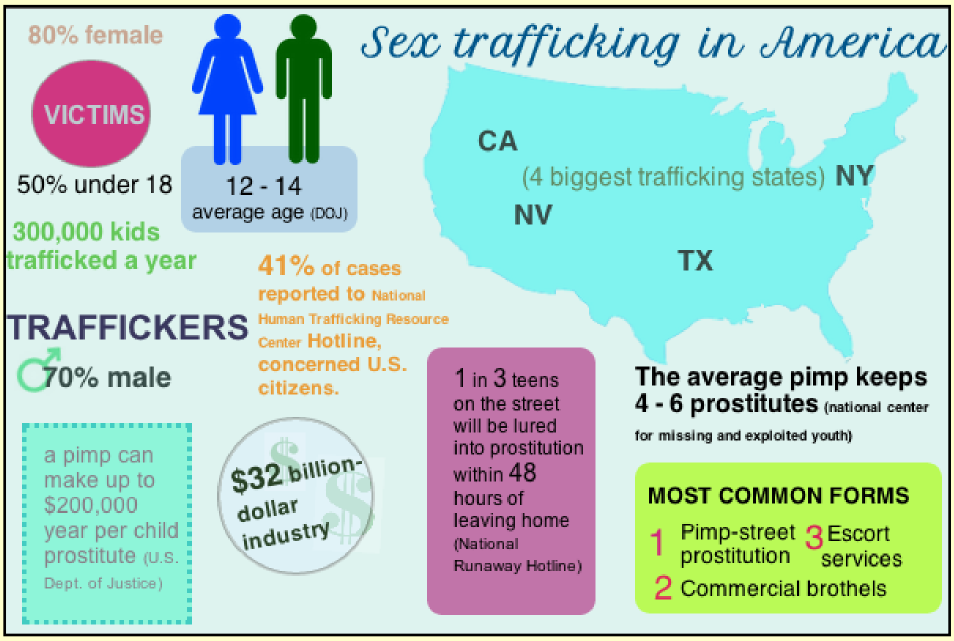
According to UNICEF, more than 1.2 million children become human trafficking victims every year. Organize crime groups make up a significant percent of traffickers, but terrorist groups are making their mark.



Analysts say that counterterrorism officials must begin to pay attention to human trafficking schemes, because in addition to generating revenue, human trafficking helps terror groups demoralize their enemies and supply fighting power. Local officials in northern Nigeria, for example, claim that **Boko Haram is using some of the girls kidnapped earlier this year for suicide bombings**. In **Nepal, Marxist guerrillas traffic girls to India to fund their operations.**

For the United States, human trafficking operations can also become a threat to national security. In Operation White Lace in Los Angeles, women from the former USSR were trafficked into high-end prostitution. Many arrived in the United States as part of sports and religious delegations, but soon obtained visas to remain in the country by posing as students at a language school. **In the book, *Dirty Entanglements: Corruption, Crime and Terrorism*, Louise I. Shelley**, a professor at George Mason University and director of the Terrorism, Transnational Crime, and Corruption Center, reported that **the same language school, which was in actuality a visa mill, also provided student visas to some of the 9/11 hijackers**. Shelley concluded that the language school was a point of intersection of crime and terrorism.

A larger focus on combating human trafficking could not only diminish revenues for terror groups and crime syndicates, but it could help keep terrorists from arriving on U.S. shores. At a 2012 meeting of the President’s Interagency Task Force to Monitor and Combat Trafficking in Persons, then Deputy National Security Adviser and now President Barack Obama’s chief of staff, Denis McDonough, told the administration’s cabinet members in attendance that “human trafficking is at the nexus of organized crime, is a source for funding for international terrorist groups, (and) is a source for funding for transnational terrorist groups. It fundamentally endangers international security.”



Major U.S. cities brace for climate change impacts

Source: http://www.homelandsecuritynewswire.com/dr20141231-major-u-s-cities-brace-for-climate-change-impacts

American cities facing eroding coastlines and greater risk of storm damage are instituting new policies, adopting new approaches, and establishing new practices in order to be better prepared for the impact of climate change in the coming decades. There are different approaches, but 2014 marks a year of major commitments to practices aiming to control and mitigate future climate change impacts on the country’s urban centers.

In major American cities such as San Francisco, New York City, Miami, and Chicago, urban planners and city leaders are factoring in climate change impacts over the next several decades.

As the*Pew Charitable Trusts* reports, American cities facing eroding coastlines and greater risk of storm damage are instituting new policies, adopting new approaches, and establishing new practices in order to be better prepared for the impact of climate change in the coming decades. There are different approaches, but 2014 marks a year of major commitments to practices aiming to control and mitigate future climate change impacts on the country’s urban centers.

In San Francisco, the Capital Planning Committee has decreed that all new construction projects involving city and county agencies must take into account rising sea level trends for the area and offer ways to adapt within building plans.

California wildfires force 4,000 families to evacuate from their homes, "months before such fires normally break out"
-NY Times
CLIMATE CHANGED.
FORECAST THE FACTS

"Our approach is not simply to build a wall and think the problem is solved, but to explore all options, including looking to nature for solutions, like wetlands," said Debbie Raphael, the director of city's Department of the Environment, the organization responsible for much of the new decree's.

Additionally, Governor Jerry Brown has signed legislation allowing for the creation of a Sea Level Rise Database which will collect data and offer solutions for climate change strategies across the state.

New York City has responded in kind as well, having launched a $20 billion initiative to strengthen coastal dunes, upgrade building codes, and protect electrical infrastructure in any flood-prone area, including all major facilities such as hospitals.

Miami and its surrounding metro areas are also working to plan for what is sure to come to low-elevation areas. Palm Beach, Broward, Miami-Dade, and Monroe counties have formed the Southeast Florida Regional Climate Change Compact collectively to plan for an expected sea level rise of as much as two feet by 2060.

Miami Beach has invested $400 million in plans to counteract tidal waters and storms that can flood the city streets. Among these, new plans that detail "minimum elevations" for new sea walls and elevated road ways are only part of the greater effort.

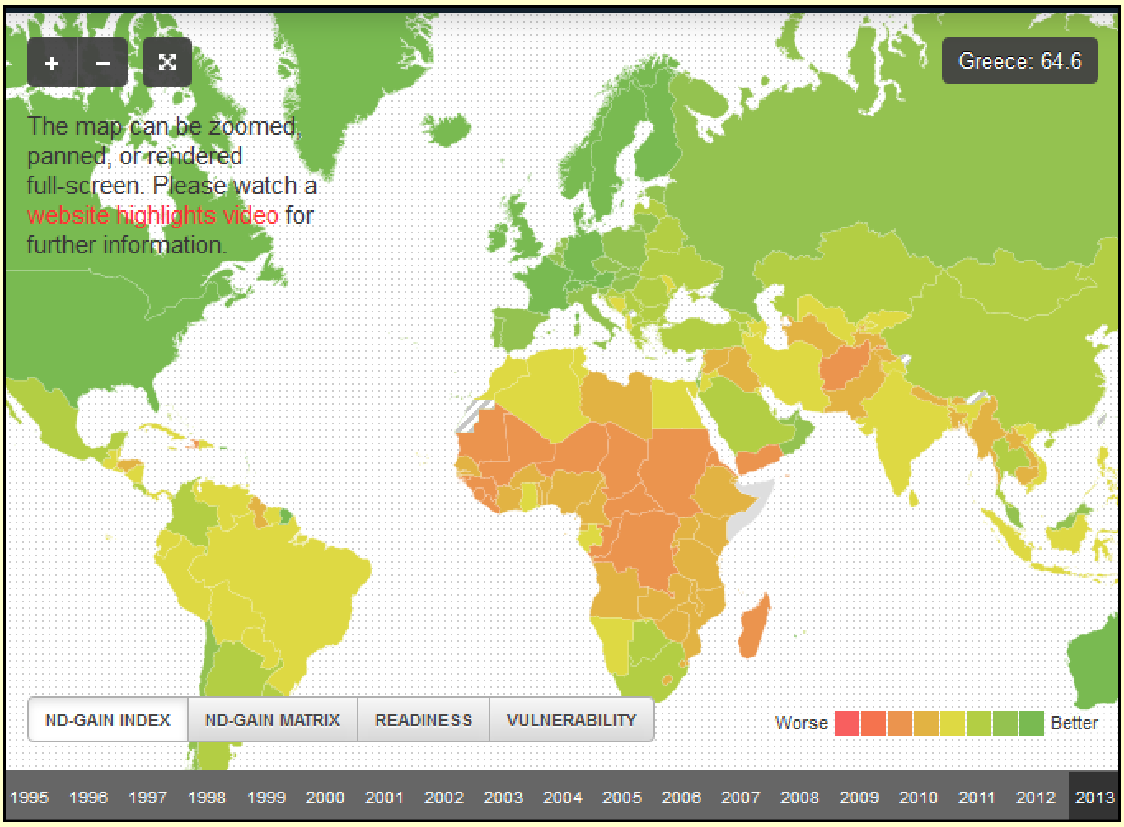
In Chicago, greater emphasis is being placed on "living shorelines" with investment in wetlands and natural landscapes in the hopes that nature can provide a suitable buffer for the city against rising waters. Called greenscapes, these man-made natural lands can reduce storm runoff and flooding while also being cost effective. Currently, transportation departments in the city are evaluating the vulnerability of roadways and how greenscapes can help.

"We've made rapid progress in a short amount of time," said Steve Adams, the climate adaptation director for Sustainable Communities. Speaking on the progress made by cities in 2014, Adams is hopeful, "It's astonishing how clear it is in 2014 that climate change adaptations, or resilience, is really an idea in good standing, where the conversation in 2008 or 2009 was just beginning to emerge."

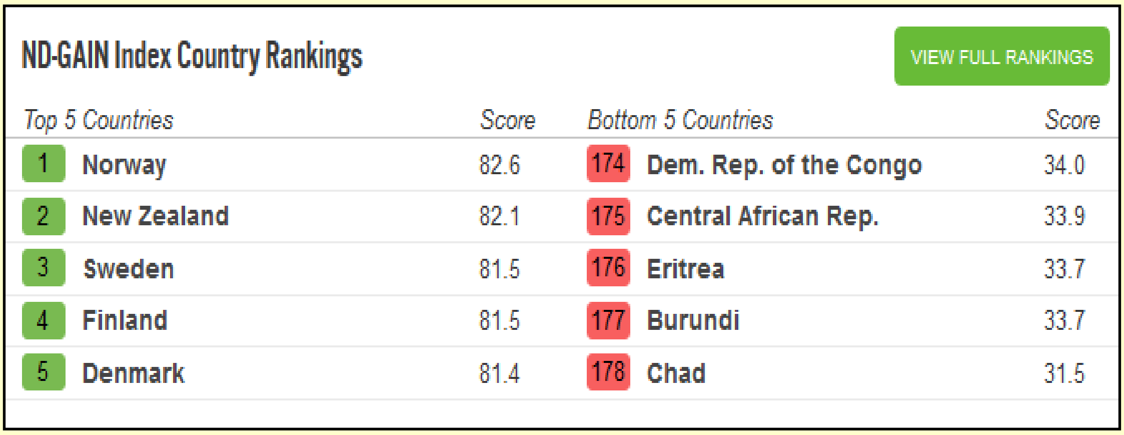
ND-GAIN Index

Source: http://index.gain.org/

The ND-GAIN Index, a project of the University of Notre Dame Global Adaptation Index (ND-GAIN), summarizes a country's vulnerability to climate change and other global challenges in combination with its readiness to improve resilience. It aims to help businesses and the public sector better prioritize investments for a more efficient response to the immediate global challenges ahead. (**NOTE:** Maps are interactive)



The map can be zoomed, panned, or rendered full-screen. Please watch a website highlights video for further information.


VIEW FULL RANKINGS

ND-GAIN Index Country Rankings

	Top 5 Countries	Score		Bottom 5 Countries	Score
1	Norway	82.6	174	Dem. Rep. of the Congo	34.0
2	New Zealand	82.1	175	Central African Rep.	33.9
3	Sweden	81.5	176	Eritrea	33.7
4	Finland	81.5	177	Burundi	33.7
5	Denmark	81.4	178	Chad	31.5

Transnational Asymmetric Armed Conflict under International Humanitarian Law: Key Contemporary Challenges

Institute for National Security Studies, 2015

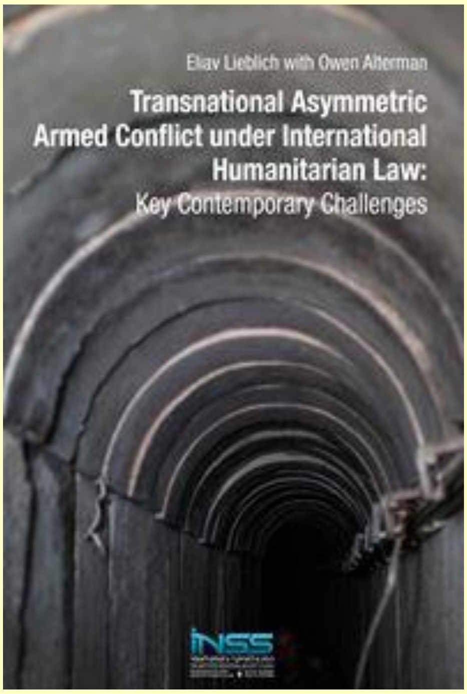
By Eliav Lieblich with, Owen Alterman

Source: http://www.inss.org.il/index.aspx?id=4538&articleid=8532

The change in the nature of armed conflict, from the classic war between sovereign states to the contemporary mode of armed conflict involving non-state actors that at times operate across state borders, raises a new set of legal issues and dilemmas. These legal challenges emanate both from the new nature of warfare and from the increasing emphasis in international legal discourse on the promotion of human rights.

This book addresses some of the major challenges that contemporary conflicts, particularly transnational asymmetric armed conflicts, present in the context of international humanitarian law. Against the growing interface between international humanitarian and human rights law, it discusses the normative framework regulating such conflicts as well as particular issues concerning the law on targeting, such as the application of the principles of distinction and proportionality in scenarios of asymmetric conflict. The book defines the different positions in international discourse regarding these dilemmas and seeks wherever possible to reconcile them, at the same time that it highlights instances where there can be no reconciliation.

The volume attempts to map the approaches toward some of the most pressing issues on the regulation of contemporary armed conflicts. Intended for military commanders, policymakers, lawyers, and the general public, it provides a detailed summary of these dilemmas that can serve decision makers in their formulation and assessment of state action and policy.


Eliav Lieblich with Owen Alterman
Transnational Asymmetric Armed Conflict under International Humanitarian Law:
Key Contemporary Challenges
INSS

Contents

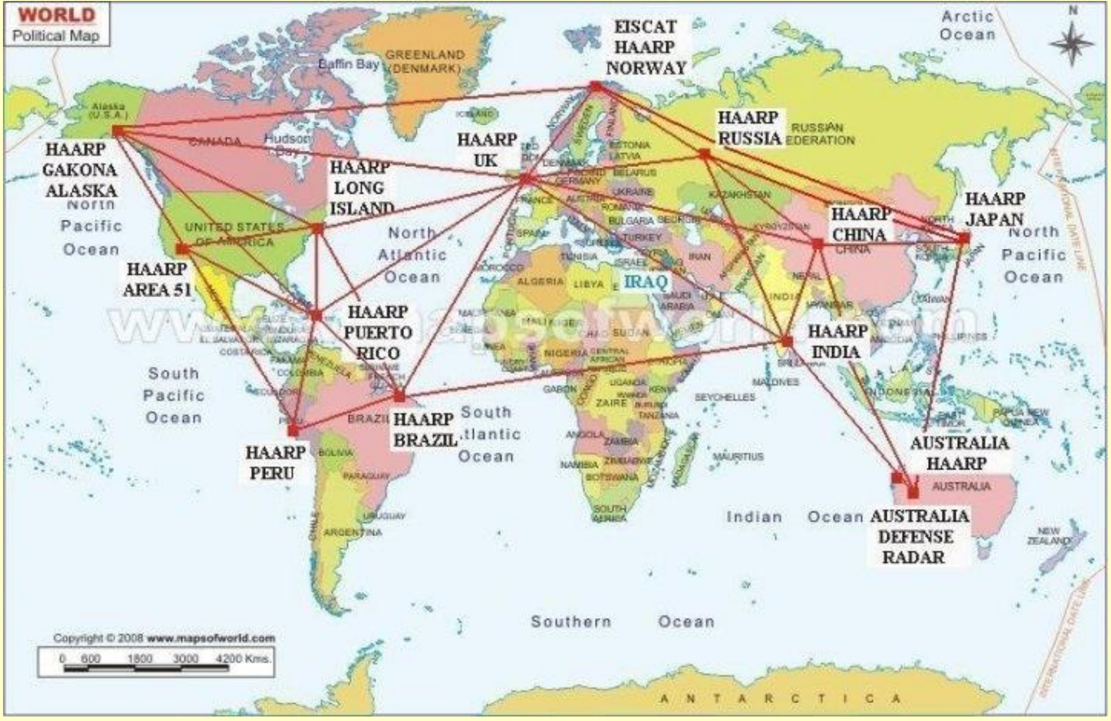
▶ **Read this book at:**
http://www.inss.org.il/uploadImages/systemFiles/Transnational%20Asymmetric_full%20text.pdf

HAARP: Secret Weapon Used For Weather Modification, Electromagnetic Warfare

Source: http://www.globalresearch.ca/haarp-secret-weapon-used-for-weather-modification-electromagnetic-warfare/20407

"It isn't just conspiracy theorists who are concerned about HAARP. The European Union called the project a global concern and passed a resolution calling for more information on its health and environmental risks. Despite those concerns, officials at HAARP insist the project is nothing more sinister than a radio science research facility."
– Quote from a TV documentary on HAARP by the Canadian Broadcasting Corporation (CBC).

Jan 18 – HAARP (High Frequency Active Auroral Research Program) is a little-known, yet critically important U.S. military defense program which has generated quite a bit of controversy over the years in certain circles. Though denied by HAARP officials, some respected researchers allege that secret electromagnetic warfare capabilities of HAARP are designed to forward the US military's stated goal of achieving full-spectrum dominance by the year 2020. Others go so far as to claim that HAARP can and has been used for weather modification, to cause earthquakes and tsunamis, to disrupt global communications systems, and more.



Major aspects of the program are kept secret for alleged reasons of "national security." Yet there is no doubt that HAARP and electromagnetic weapons capable of being used in warfare do exist. According to the official HAARP website, **"HAARP is a scientific endeavor aimed at studying the properties and behavior of the ionosphere, with particular emphasis on being able to understand and use it to enhance communications and surveillance systems for both civilian and defense purposes."**
The ionosphere is the delicate upper layer of our atmosphere which ranges from about 30 miles (50 km) to 600 miles (1,000 km) above the surface of the Earth.

The HAARP website acknowledges that experiments are conducted which use electromagnetic frequencies to fire pulsed, directed energy beams in order to "temporarily excite a limited area of the ionosphere." Some scientists state that purposefully disturbing this sensitive layer could have major and even disastrous consequences. Concerned HAARP researchers like Dr. Michel Chossudovsky of the University of Ottawa and Alaska's Dr. Nick Begich (son of a US Congressman) present evidence suggesting that these disturbances can even cause tsunamis and earthquakes.

Two key major media documentaries, one by Canada's public broadcasting network CBC and the other by the History Channel, reveal the inner workings of HAARP in a most powerful way. The very well researched CBC documentary includes this key quote:

"It isn't just conspiracy theorists who are concerned about HAARP. In January of 1999, the European Union called the project a global concern and passed a resolution calling for more information on its health and environmental risks. Despite those concerns, officials at HAARP insist the project is nothing more sinister than a radio science research facility."

To view the European Union (EU) document which brings HAARP and similar electromagnetic weapons into question, click here. The actual wording at bullet point 24 in this telling document states that the EU "considers HAARP by virtue of its far-reaching impact on the environment to be a global concern and calls for its legal, ecological and ethical implications to be examined by an international independent body before any further research and testing." This reveling document further states that the EU regrets the repeated refusal of the U.S. government to send anyone to give evidence on HAARP.

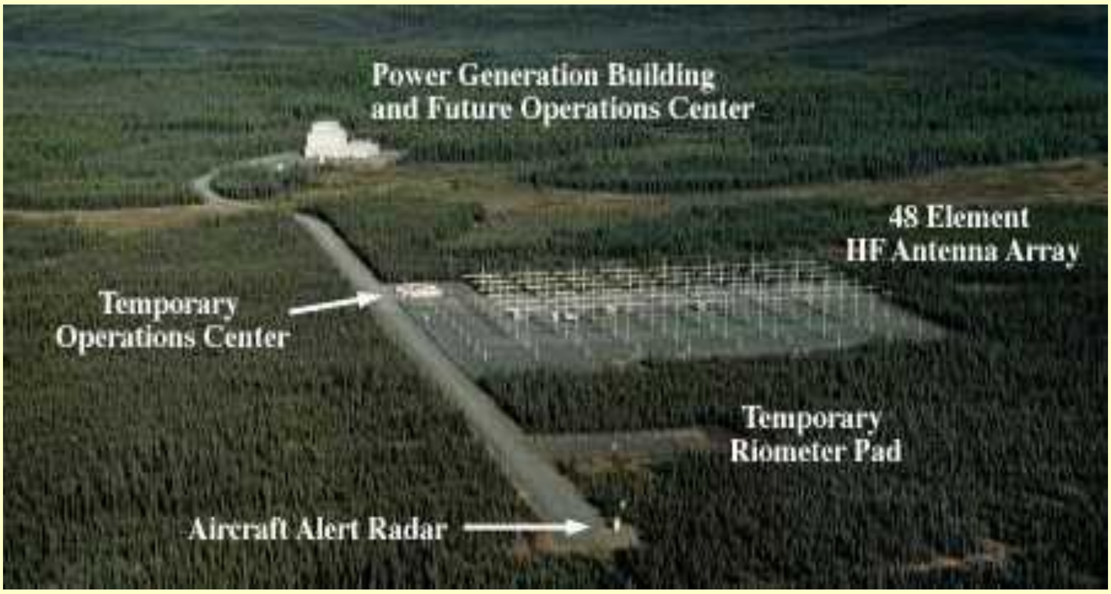
To watch this engaging 15-minute CBC documentary online, click here. For an even more detailed and revealing 45-minute History Channel documentary on HAARP and other secret weapons used for electromagnetic warfare, click here. Below are two quotes from the History Channel documentary:

"Electromagnetic weapons … pack an invisible wallop hundreds of times more powerful than the electrical current in a lightning bolt. One can blast enemy missiles out of the sky, another could be used to blind soldiers on the battlefield, still another to control an unruly crowd by burning the surface of their skin. If detonated over a large city, an electromagnetic weapon could destroy all electronics in seconds. They all use directed energy to create a powerful electromagnetic pulse."

"Directed energy is such a powerful technology it could be used to heat the ionosphere to turn weather into a weapon of war. Imagine using a flood to destroy a city or tornadoes to decimate an approaching army in the desert. The military has spent a huge amount of time on weather modification as a concept for battle environments. If an electromagnetic pulse went off over a city, basically all the electronic things in your home would wink and go out, and they would be permanently destroyed."

For those who still doubt that such devastating secret weapons have been developed, here is an intriguing quote from an article in New Zealand's leading newspaper, the *New Zealand Herald*:

"Top-secret wartime experiments were conducted off the coast of Auckland to perfect a tidal wave bomb, declassified files reveal. United States defence chiefs said that if the project had been completed before the end of the war, it could have played a role as effective as that of the atom bomb. Details of the tsunami bomb, known as Project Seal, are contained in 53-year-old documents released by the Ministry of Foreign Affairs and Trade."

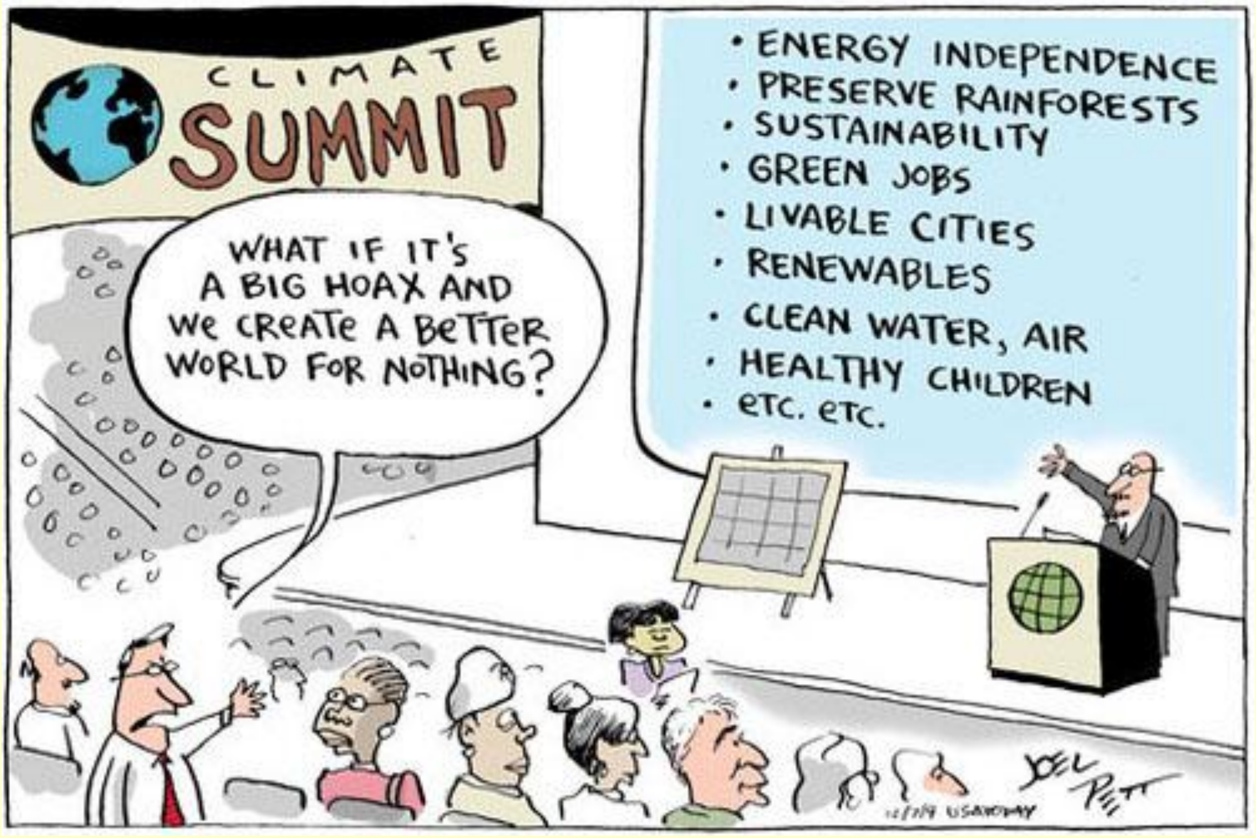


If the military secretly developed a weapon which could cause a tsunami over half a century ago, what kind of advanced deadly weapons might be available now? And why is it that the general public still doesn't know about secret weapons developed over 50 years ago? To understand why the media isn't covering these highly critical issues, click here. Clearly the military has the capability to cause a tsunami and likely to cause earthquakes and hurricanes, as well. It's time for us to take action to spread the word on this vital topic.

Having interpreted to for top generals in my work as a language interpreter with the US Department of State, I learned that military planners are always interested in developing the most devastating weapons possible. Yet these weapons are kept secret as long as possible, allegedly for reasons of national security. The many layers of intense secrecy both in the military and government result in very few people being aware of the gruesome capabilities for death and destruction that have been developed over the years. There are many examples of major defense projects kept successfully out of the public's eyes for years and even decades.

The massive Manhattan Project (development of the first atomic bomb) is one such example. The building of an entire city to support the project in Oak Ridge, Tennessee was successfully kept secret even from the state's governor. The stealth bomber was kept top secret for many years, and the public still has no way of knowing it's full capabilities. It is through the use of the highly organized military and intelligence services that the power elite of our world, working in cooperation with key allies in government and corporate ownership of the media, are able to carry out major cover-ups and secret operations like those involved with HAARP.

Some researchers have raised questions about the possible involvement of HAARP in major disasters like the earthquake in Haiti, Indonesian tsunami, and hurricane Katrina. Could these have been HAARP experiments gone awry? Might they even have been caused by rogue elements which gained control of this devastating technology. Of course disasters like this happen regularly on a natural basis, yet if you begin to research, there is some high strangeness around some of these disasters. The evidence is inconclusive, yet with the known and unknown major destructive capabilities of this weapon, serious questions remain.



Global Risks 2015

Source: http://reports.weforum.org/global-risks-2015/executive-summary/

The 2015 edition of the *Global Risks* report completes a decade of highlighting the most significant long-term risks worldwide, drawing on the perspectives of experts and global decision-makers. Over that time, analysis has moved from risk identification to thinking through risk interconnections and the potentially cascading effects that result. Taking this effort one step further, this year's report underscores potential causes as well as solutions to global risks. Not only do we set out a view on 28 global risks in the report's traditional categories (economic, environmental, societal, geopolitical and technological) but also we consider the drivers of those risks in the form of 13 trends. In addition, we have selected initiatives for addressing significant challenges, which we hope will inspire collaboration among business, government and civil society communities.

Mapping Global Risks in 2015

The Global Risks Landscape, a map of the most likely and impactful global risks, puts forward that, 25 years after the fall of the Berlin Wall, "interstate conflict" is once again a foremost concern (see Table 1). However, 2015 differs markedly from the past, with rising technological risks, notably cyber attacks, and new economic realities, which remind us that geopolitical tensions present themselves in a very different world from before. Information flows instantly around the globe and emerging technologies have boosted the influence of new players and new types of warfare. At the same time, past warnings of potential environmental catastrophes have begun to be borne out, yet insufficient progress has been made – as reflected in the high concerns about failure of climate-change adaptation and looming water crises in this year's report.

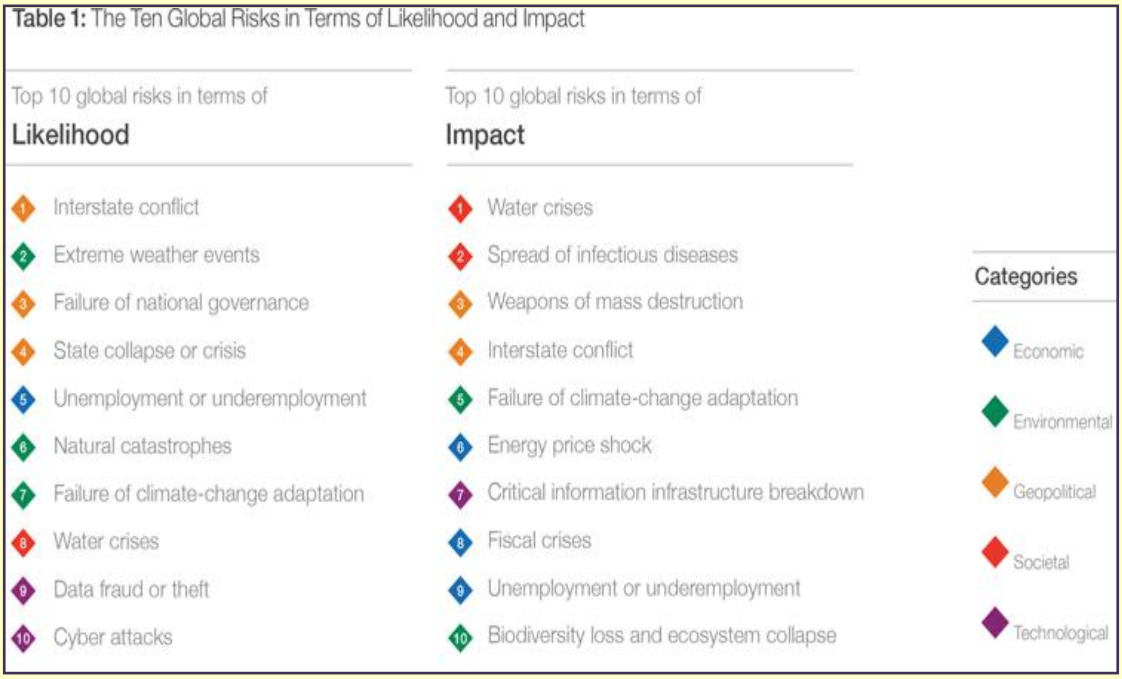


Table 1: The Ten Global Risks in Terms of Likelihood and Impact

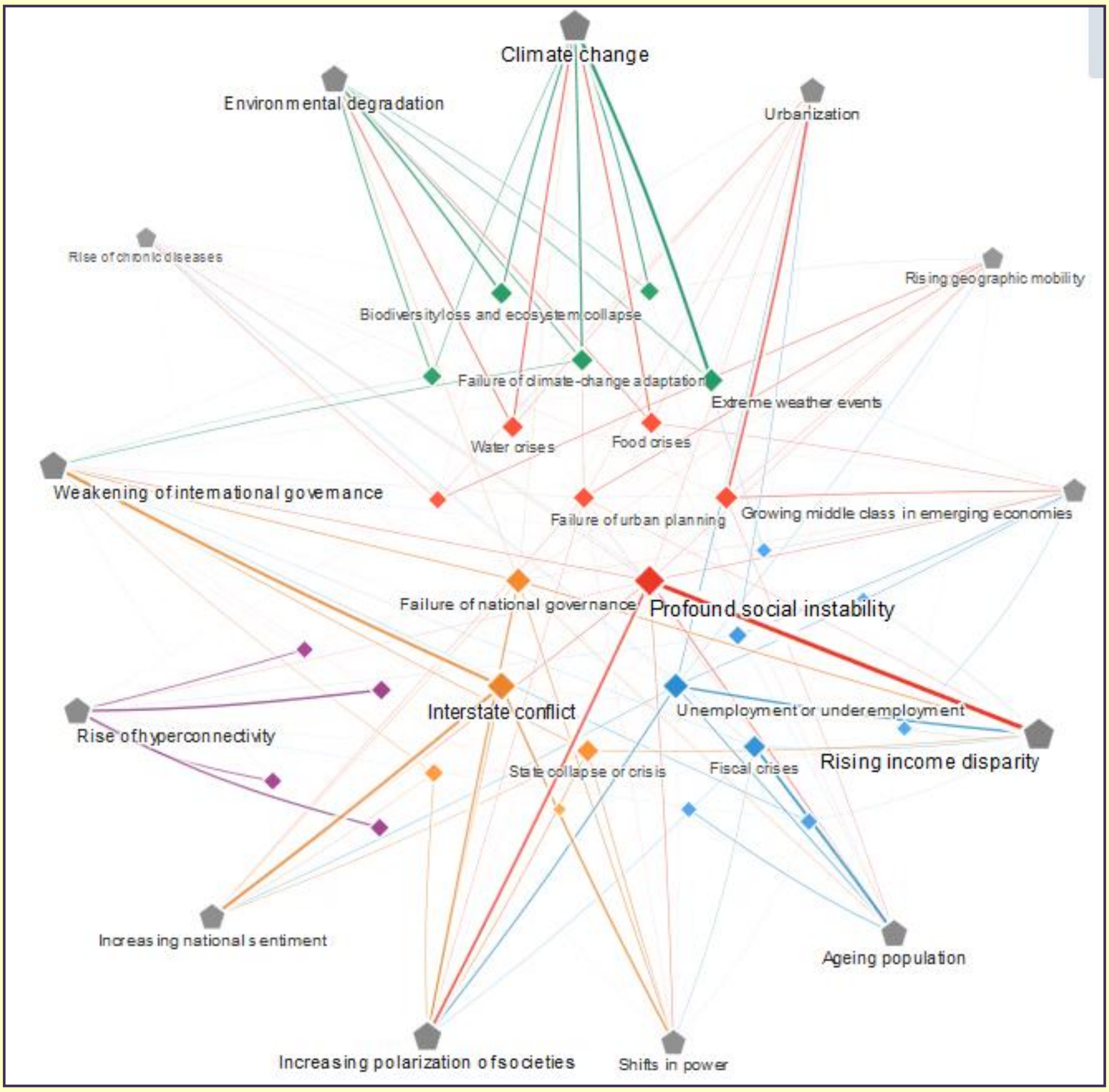
	Top 10 global risks in terms of Likelihood		Top 10 global risks in terms of Impact
1	Interstate conflict	1	Water crises
2	Extreme weather events	2	Spread of infectious diseases
3	Failure of national governance	3	Weapons of mass destruction
4	State collapse or crisis	4	Interstate conflict
5	Unemployment or underemployment	5	Failure of climate-change adaptation
6	Natural catastrophes	6	Energy price shock
7	Failure of climate-change adaptation	7	Critical information infrastructure breakdown
8	Water crises	8	Fiscal crises
9	Data fraud or theft	9	Unemployment or underemployment
10	Cyber attacks	10	Biodiversity loss and ecosystem collapse

Categories

- ◆ Economic
- ◆ Environmental
- ◆ Geopolitical
- ◆ Societal
- ◆ Technological

These multiple cross-cutting challenges can threaten social stability, perceived to be the issue most interconnected with other risks in 2015, and additionally aggravated by the legacy of the global economic crisis in the form of strained public finances and persistent unemployment. The central theme of profound social instability highlights an important paradox that has been smouldering since the crisis but surfaces prominently in this year's report. Global risks transcend borders and spheres of influence and require stakeholders to work together, yet these risks also threaten to undermine the trust and collaboration needed to adapt to the challenges of the new global context.

The world is, however, insufficiently prepared for an increasingly complex risk environment. For the first time, the report provides insights on this at the regional level: social instability features among the three global risks that Europe, Latin America and the Caribbean, and the Middle East and North Africa are least prepared for. Other societal risks, ranging from the failure of urban planning in South Asia to water crises in the Middle East and North Africa, are also prominent. And capacity to tackle persistent unemployment – an important risk connected with social instability – is a major concern in Europe and sub-Saharan Africa.


Climate change
Environmental degradation
Urbanization
Rise of chronic diseases
Rising geographic mobility
Biodiversity loss and ecosystem collapse
Failure of climate-change adaptation
Extreme weather events
Water crises
Food crises
Weakening of international governance
Failure of urban planning
Growing middle class in emerging economies
Failure of national governance
Profound social instability
Interstate conflict
Unemployment or underemployment
Rise of hyperconnectivity
State collapse or crisis
Fiscal crises
Rising income disparity
Increasing national sentiment
Ageing population
Increasing polarization of societies
Shifts in power

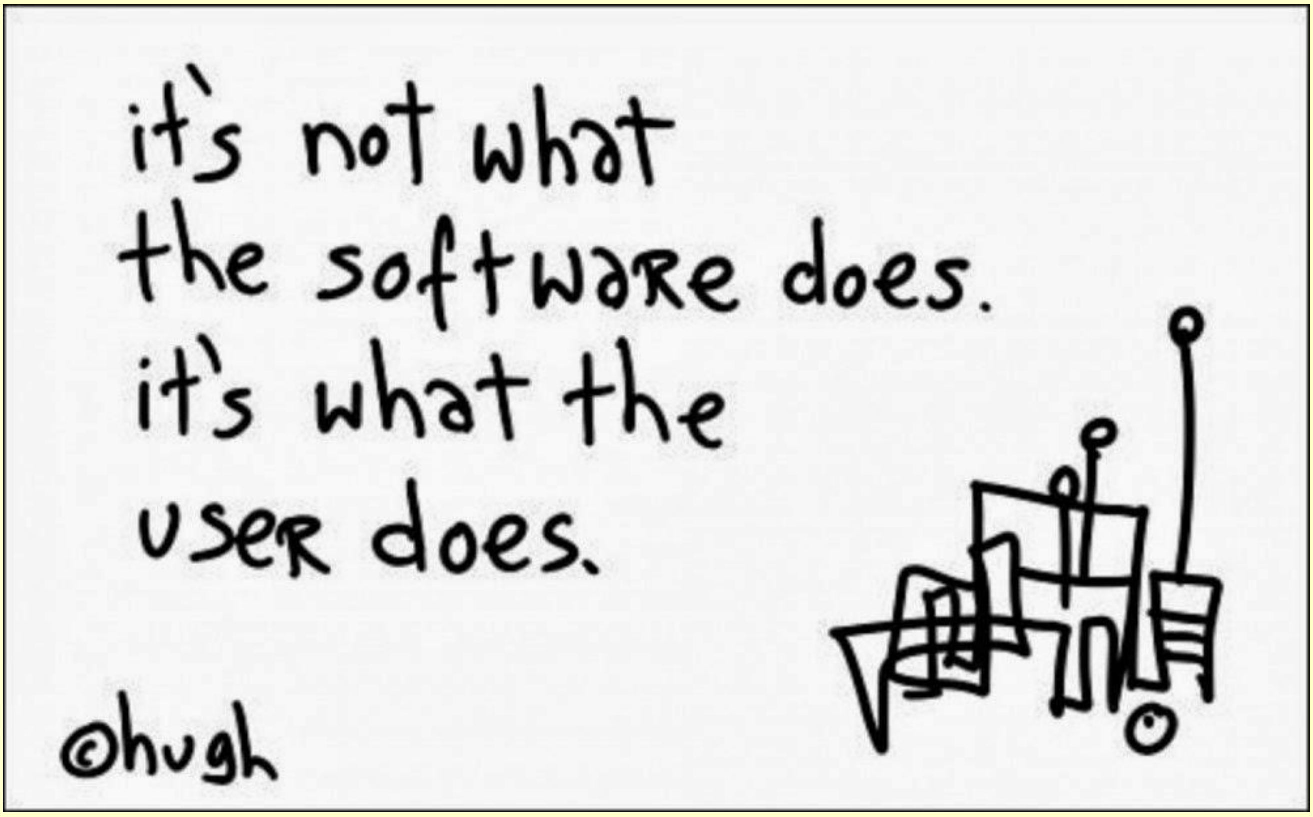
As in previous years, Part 2 explores three risk constellations that bear on the survey findings. In 2015, these are:

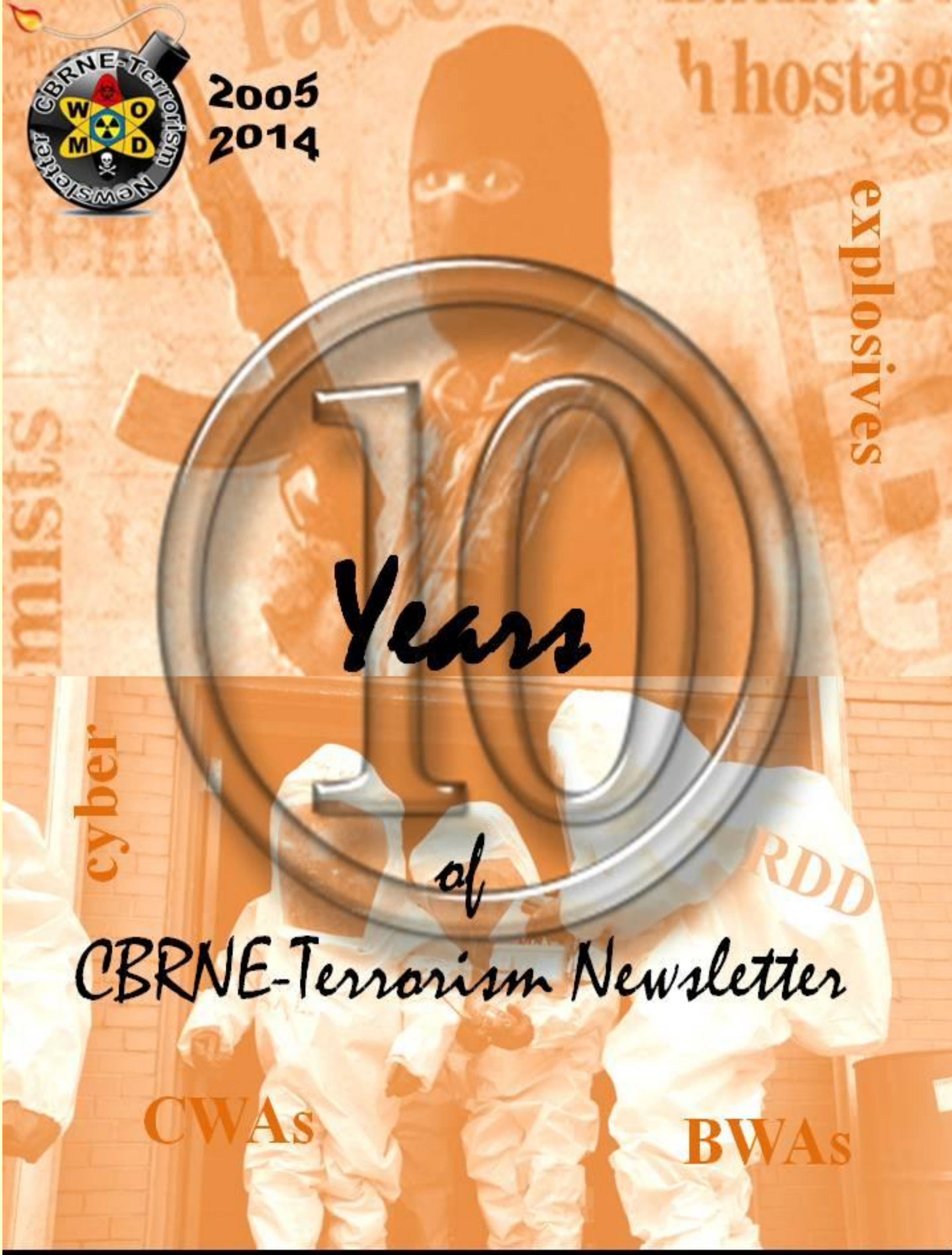
- **Interplay between geopolitics and economics:** The interconnections between geopolitics and economics are intensifying because states are making greater use of economic tools, from regional integration and trade treaties to protectionist policies and cross-border investments, to establish relative geopolitical power. This threatens to undermine the logic of global economic cooperation and potentially the entire international rule-based system.
- **Urbanization in developing countries:** The world is in the middle of a major transition from predominantly rural to urban living, with cities growing most rapidly in Asia and Africa. If managed well, this will help to incubate innovation and drive economic growth. However, our ability to address a range of global risks – including climate change, pandemics, social unrest, cyber threats and infrastructure development – will largely be determined by how well cities are governed.

- **Governance of emerging technologies:** The pace of technological change is faster than ever. Disciplines such as synthetic biology and artificial intelligence are creating new fundamental capabilities, which offer tremendous potential for solving the world's most pressing problems. At the same time, they present hard-to-foresee risks. Oversight mechanisms need to more effectively balance likely benefits and commercial demands with a deeper consideration of ethical questions and medium to long-term risks – ranging from economic to environmental and societal.

Mitigating, preparing for and building resilience against global risks is long and complex, something often recognized in theory but difficult in practice. Against this backdrop, Part 3 features three proven or promising initiatives that were instituted in response to extreme weather events and climate-change adaptation. The modelling of the Murray-Darling Basin river system in Australia has pioneered innovative methods of water management that are now being adapted for use elsewhere in the world. The Resilient America Roundtable is currently helping selected local communities across the United States to understand how they might be affected by different risks and then design resilience strategies. ZÜRS Public, part of an extensive flood management programme in Germany, is a public-private collaboration that for several years now has been a tool for communicating with homeowners and businesses about their exposure to flood risk.

Over the past 10 years, the *Global Risks* report has raised awareness of the dangers from the interconnected nature of global risks and has persistently called for multistakeholder collaboration to address them. By offering a broad-ranging overview from risk identification and evaluation to practices – from the "what" to the "how" – this year's report aims to provide the most comprehensive set of insights yet for decision-makers in its decade-long history.





2005
2014

10 Years of CBRNE-Terrorism Newsletter

WE have to be lucky all the time. THEY have to be lucky only once!