10 years

April 2015

CBRNE
NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

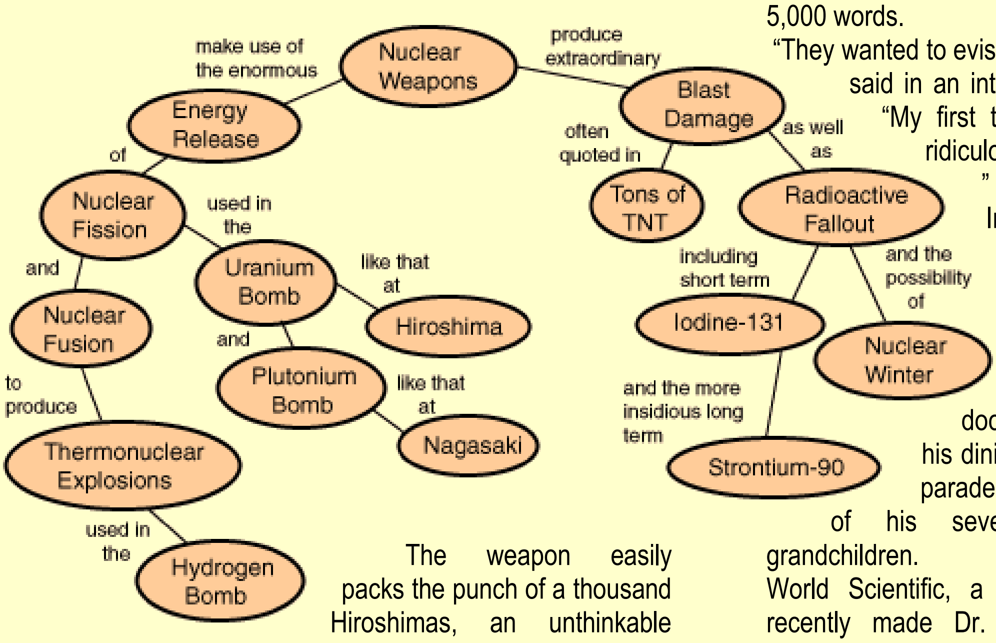
The other face of terrorism...

www.cbrne-terrorism-newsletter.com

Hydrogen Bomb Physicist's Book Runs Afoul of Energy Department

Source: http://www.nytimes.com/2015/03/24/science/hydrogen-bomb-physicists-book-runs-afoul-of-energy-department.html

For all its horrific power, the atom bomb — leveler of Hiroshima and instant killer of some 80,000 people — is but a pale cousin compared to another product of American ingenuity: the hydrogen bomb.



The weapon easily packs the punch of a thousand Hiroshimas, an unthinkable range of destruction that lay behind the Cold War's fear of mutual annihilation. It was developed in great secrecy, and Washington for decades has done everything in its power to keep the details of its design out of the public domain.

Now, a physicist who helped devise the weapon more than half a century ago has defied a federal order to cut from his new book material that the government says teems with thermonuclear secrets.

The author, Kenneth W. Ford, 88, spent his career in academia and has not worked on weapons since 1953. His memoir, "Building the H Bomb: A Personal History," is his 10th book. The others are physics texts, elucidations of popular science and a reminiscence on flying small planes.

He said he included the disputed material because it had already been disclosed elsewhere and helped him paint a fuller picture of an important chapter of American history. But after he volunteered the manuscript for a security review, federal officials told him to remove about 10 percent of the text, or roughly 5,000 words.

"They wanted to eviscerate the book," Dr. Ford said in an interview at his home here. "My first thought was, 'This is so ridiculous I won't even respond.' "

Instead, he talked with federal officials for half a year before reaching an impasse in late January, a narrative he backs up with many documents laid out neatly on his dining room table, beneath a parade of photographs of some of his seven children and 13 grandchildren.

World Scientific, a publisher in Singapore, recently made Dr. Ford's book public in electronic form, with print versions to follow. Reporters and book review editors have received page proofs.

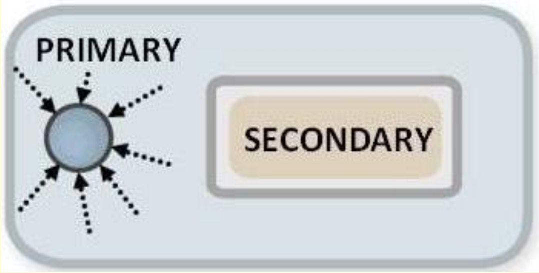
The Department of Energy, the keeper of the nation's nuclear secrets, declined to comment on the book's publication.

But in an email to Dr. Ford last year, Michael Kolbay, a classification officer at the agency, warned that the book's discussion of the "design nuances of a successful thermonuclear weapons program" would "encourage emerging proliferant programs," a euphemism for aspiring nuclear powers.

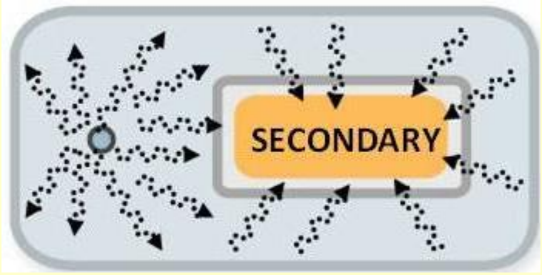
In theory, Washington can severely punish leakers. Anyone who comes in contact with classified atomic matters must sign a nondisclosure agreement that warns of criminal penalties and the government's right to "all royalties, remunerations and emoluments" that result from the disclosure of secret information.

Inside an H-Bomb

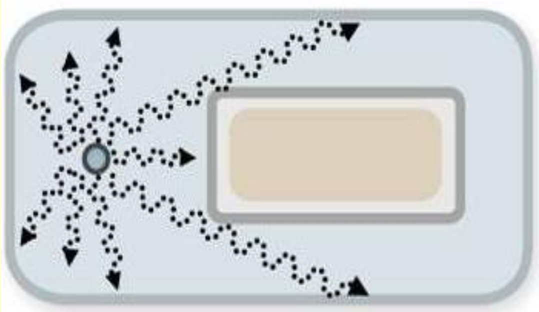
At its simplest, a hydrogen bomb uses an atomic primary stage to trigger a more powerful thermonuclear stage.



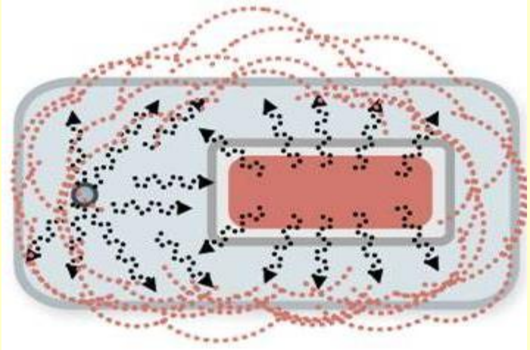
Conventional explosives compress plutonium in the primary, creating a critical mass in which atoms begin to split apart and release nuclear energy.



The radiation vaporizes the lining of the casing and radiates back toward the secondary, compressing it and heating it to fusion temperature.



Radiation from the primary flows down the length of the bomb casing ahead of the primary blast.



Thermonuclear fusion releases huge amounts of energy, and the fireball bursts out of the casing.

Source: "Dark Sun: The Making of the Hydrogen Bomb," by Richard Rhodes (The New York Times)

But the reality is that atomic pioneers and other insiders — in talks, books, articles and television shows — have divulged many nuclear secrets over the decades and have rarely faced any consequences.

The result is a twilight zone of sensitive but never formally declassified public information. The policy of the Energy Department is never to acknowledge the existence of such open atomic secrets, a stance it calls its "no comment" rule.

Yet in preparing his book, Dr. Ford deeply mined this shadowy world of public information. For instance, the federal agency wanted him to strike a reference to the size of the first hydrogen test device — its base was seven feet wide and 20 feet high. Dr. Ford responded that public photographs of the device, with men, jeeps and a forklift nearby, gave a scale of comparison that clearly revealed its overall dimensions.

Kenneth W. Ford at home in Philadelphia. He recently wrote his memoir: "Building the H Bomb: A Personal History." Credit Mark Makela for The New York Times

Steven Aftergood, director of the Project on Government Secrecy for the Federation of American Scientists, a private group in Washington, said he had received page proofs of Dr. Ford's book and expected that many of its details had run afoul of what he characterized as the agency's classification whims.

"There are probably real issues intertwined with spurious bureaucratic nonsense," Mr. Aftergood said.

He added that it would not be surprising if the Department of Energy did nothing in response to the book's publication. "Any action," Mr. Aftergood said, "is only going to magnify interest."

In 1979, the department learned that the hard way when it tried to block a magazine's release of H-bomb secrets; its failure gave the article a rush of free publicity.

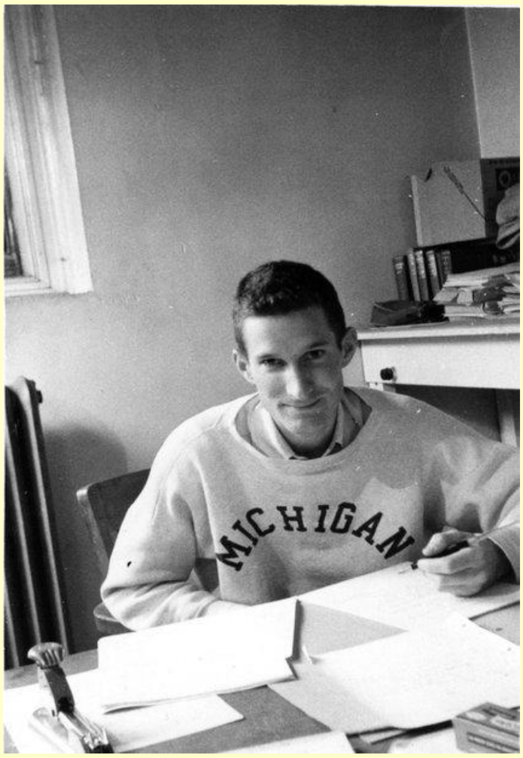
A main architect of the hydrogen bomb, Richard L. Garwin, whom Dr. Ford interviewed for the book, describes the memoir in its so-called front matter as "accurate as well as entertaining."

In an interview, Dr. Garwin said he recalled nothing in the book's telling of hydrogen bomb history that, in terms of public information, "hasn't been reasonably authoritatively stated." Still, he said, his benign view of the book "doesn't mean I encourage people to talk about such things."

Hydrogen bombs are the world's deadliest weapons. The first test of one, in November 1952, turned the Pacific isle of Elugelab, a mile in diameter, into a boiling mushroom cloud.

Today, Britain, China, France, Russia and the United States are the only declared members of the thermonuclear club, each possessing hundreds or thousands of hydrogen bombs. Military experts suspect that Israel has dozens of them. India, Pakistan and North Korea are seen as interested in acquiring the potent weapon.

Though difficult to make, hydrogen bombs are attractive to nations and militaries because their fuel is relatively cheap. Inside a thick metal casing, the weapon relies on a small atom bomb that works like a match to ignite the hydrogen fuel.



Dr. Ford at Princeton in 1952. His work on the development of the hydrogen bomb involved calculating the likelihood that the compressed fuel would burn thoroughly and estimating the bomb's explosive power.

Dr. Ford entered this world by virtue of elite schooling. He graduated from Phillips Exeter Academy in 1944 and Harvard in 1948. While working on his Ph.D. at Princeton, he was drawn into the nation's hydrogen bomb push by his mentor, John A. Wheeler, a star of modern science.

Dr. Ford worked in the shadow of Edward Teller and Stanislaw Ulam, bomb designers at the Los Alamos lab in New Mexico. Early in 1951, they hit on a breakthrough idea: using radiation from the exploding atom bomb to generate vast forces that would compress and heat the hydrogen fuel to the point of thermonuclear ignition.

From 1950 to 1952, Dr. Ford worked on the project, first at Los Alamos and then back at Princeton. Among other things, he calculated the likelihood that the compressed fuel would burn thoroughly and estimated the bomb's explosive power.

He received his doctorate in 1953, and remained in academia, teaching at such schools as Brandeis; the University of California, Irvine; and the University of Massachusetts Boston.

In the interview at his home, he said he was researching his H-bomb memoir when a historian at the Department of Energy suggested that he submit the manuscript for classification review. He did so, and in August, the agency responded.

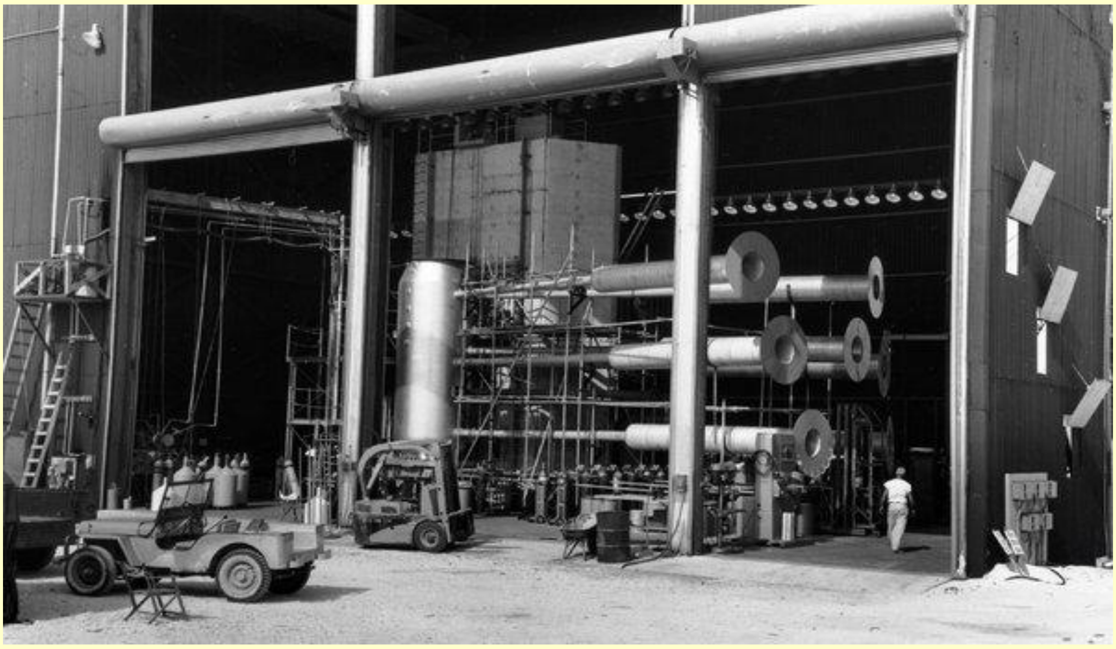
"Our team is quite taken with your manuscript," an official wrote. "However, some concerns have been identified."

In late September, Dr. Ford met with agency officials. Afterward, in an email, he told them that he remained convinced the book "contains nothing whatsoever whose dissemination could, by any stretch of the imagination, damage the United States or help a country that is trying to build a hydrogen bomb."

On Nov. 3, Andrew P. Weston-Dawkes, director of the agency's office of classification, wrote Dr. Ford to say that the review had "identified portions that must be removed prior to publication."

The ordered cuts, 60 in all, ranged from a single sentence to multiple paragraphs, and included endnotes and illustrations.

The first hydrogen bomb in its construction shed on Elugelab, which was later vaporized by the bomb’s blast in 1952. Credit Los Alamos National Laboratory



The Happy Hydrogen Bomb was shown in: The Adventurous Type at the Hyde Park Art Centre in Chicago Illinois.

“Were I to follow all — or even most — of your suggestions,” Dr. Ford wrote in reply, “it would destroy the book.”

In December, he told the department he would make a few minor revisions. For instance, in two cases he would change language describing the explosive yields of bomb tests from “in fact” to “reportedly.” After much back and forth, the conversation ended in January with no resolution, and the book’s publisher pressed on.

The government's main concern seems to center on deep science that Dr. Ford articulates with clarity. Over and over, the book discusses thermal equilibrium, the discovery that the temperature of the hydrogen fuel and the radiation could match each other during the explosion. Originally, the perceived lack of such an effect had seemed to doom the proposed weapon.

The breakthrough has apparently been discussed openly for years. For instance, the National Academy of Sciences in 2009 published a biographical memoir of Dr. Teller, written by Freeman J. Dyson, a noted physicist with the Institute for Advanced Study in Princeton, N.J. It details the thermal equilibrium advance in relation to the hydrogen bomb.

At his home, Dr. Ford said he considered himself a victim of overzealous classification and wondered what would have happened if he had never submitted his manuscript for review.

"I was dumbfounded," he said of the agency's reaction to it.

Dr. Ford said he never intended to make a point about openness and nuclear secrecy — or do anything other than to give his own account of a remarkable time in American history.

"I don't want to strike a blow for humankind," he said. "I just want to get my book published."

US Declassifies Document Revealing Israel's Nuclear Program

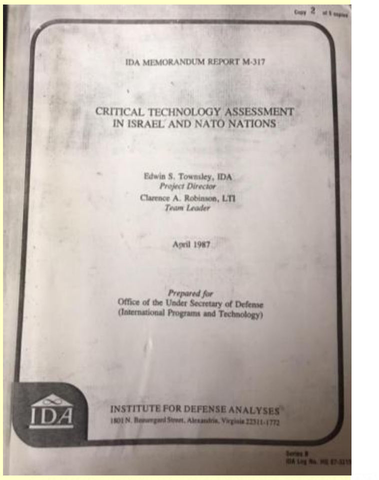
Source: http://www.israelnationalnews.com/News/News.aspx/193175#.VRZGUeGTLz4

Dimona nuclear reactor circa 1960s – National Security Archive/Flash 90

March 25 – In a development that has largely been missed by mainstream media, **the Pentagon early last month quietly declassified a Department of Defense top-secret document detailing Israel's nuclear program**, a highly covert topic that Israel has never formally announced to avoid a regional nuclear arms race, and which the US until now has respected by remaining silent.

But by publishing the declassified document from 1987, the US reportedly breached the silent agreement to keep quiet on Israel's nuclear powers for the first time ever, detailing the nuclear program in great depth.

The timing of the revelation is highly suspect, given that it came as tensions spiraled out of control between Prime Minister Binyamin Netanyahu and US President Barack Obama ahead of Netanyahu's March 3 address in Congress, in which he warned against the dangers of Iran's nuclear program and how the deal being formed on that program leaves the Islamic regime with nuclear breakout capabilities.



Copy 2 of 5 copies

IDA MEMORANDUM REPORT M-317

CRITICAL TECHNOLOGY ASSESSMENT
IN ISRAEL AND NATO NATIONS

Edwin S. Townsley, IDA
Project Director
Clarence A. Robinson, LTI
Team Leader

April 1987

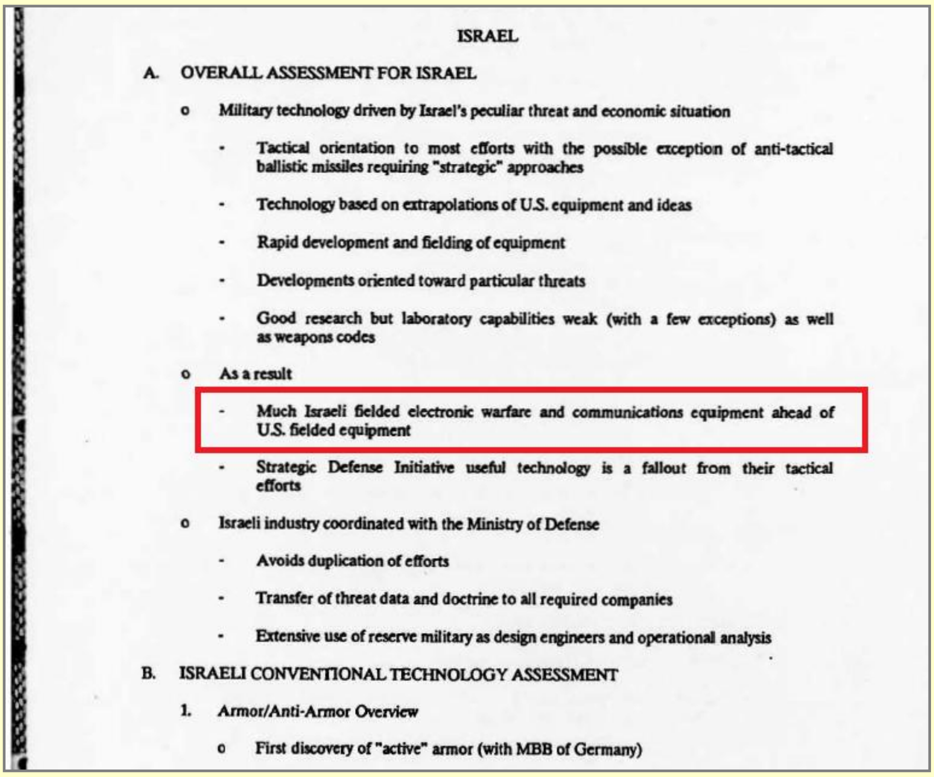
Prepared for
Office of the Under Secretary of Defense
(International Programs and Technology)

IDA
INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

Series B
IDA Log No. HQ 87-32

Another highly suspicious aspect of the document is that while the Pentagon saw fit to declassify sections on Israel's sensitive nuclear program, **it kept sections on Italy, France, West Germany and other NATO countries classified, with those sections blocked out in the document.**

The 386-page report entitled **"Critical Technological Assessment in Israel and NATO Nations"** gives a detailed description of how Israel advanced its military technology and developed its nuclear infrastructure and research in the 1970s and 1980s.



ISRAEL

A. OVERALL ASSESSMENT FOR ISRAEL

o Military technology driven by Israel's peculiar threat and economic situation

- Tactical orientation to most efforts with the possible exception of anti-tactical ballistic missiles requiring "strategic" approaches
- Technology based on extrapolations of U.S. equipment and ideas
- Rapid development and fielding of equipment
- Developments oriented toward particular threats
- Good research but laboratory capabilities weak (with a few exceptions) as well as weapons codes

o As a result

- Much Israeli fielded electronic warfare and communications equipment ahead of U.S. fielded equipment
- Strategic Defense Initiative useful technology is a fallout from their tactical efforts

o Israeli industry coordinated with the Ministry of Defense

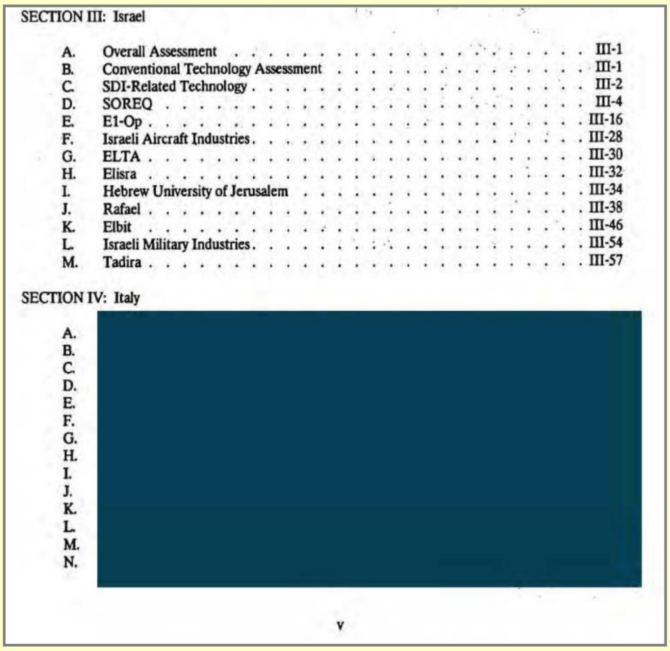
- Avoids duplication of efforts
- Transfer of threat data and doctrine to all required companies
- Extensive use of reserve military as design engineers and operational analysis

B. ISRAELI CONVENTIONAL TECHNOLOGY ASSESSMENT

1. Armor/Anti-Armor Overview

o First discovery of "active" armor (with MBB of Germany)

Israel is "developing the kind of codes which will enable them to make hydrogen bombs. That is, codes which detail fission and fusion processes on a microscopic and macroscopic level," reveals the report, stating that in the 1980s Israelis were reaching the ability to create bombs considered a thousand times more powerful than atom bombs.



SECTION III: Israel

[redacted]

v

The revelation marks a first in which the US published in a document a description of how Israel attained hydrogen bombs. **The report also notes research laboratories in Israel "are equivalent to our Los Alamos, Lawrence Livermore and Oak Ridge National Laboratories,"** the key labs in developing America's nuclear arsenal. Israel's nuclear infrastructure is "an almost exact parallel of the capability currently existing at our National Laboratories," it adds.

"As far as nuclear technology is concerned the Israelis are roughly where the U.S. was in the fission weapon field in about 1955 to 1960," the report reveals, noting a time frame just after America tested its first hydrogen bomb.

Institute for Defense Analysis, a federally funded agency operating under the Pentagon, penned the report back in 1987.

Aside from nuclear capabilities, the report revealed Israel at the time had "a totally integrated effort in systems development throughout the nation," with electronic combat all in one "integrated system, not separated systems for the Army, Navy and Air Force." **It even acknowledged that in some cases, Israeli military technology "is more advanced than in the U.S."**

Declassifying the report comes at a sensitive timing as noted above, and given that the process to have it published was started three years ago, that timing is seen as having been the choice of the American government.

US journalist Grant Smith petitioned to have the report published based on the Freedom of Information Act. Initially the Pentagon took its time answering, leading Smith to sue, and a District Court judge to order the Pentagon to respond to the request.

Smith, who heads the Institute for Research: Middle East Policy, reportedly said he thinks this is the first time the US government has officially confirmed that Israel is a nuclear power, a status that Israel has long been widely known to have despite being undeclared.

Today – Negev Nuclear Research Center near Dimona, Israel.

Nuclear forensicsImproving plutonium identification

Source: http://www.homelandsecuritynewswire.com/dr20150330-improving-plutonium-identification

Researchers have developed a new kind of sensor that can be used to investigate the telltale isotopic composition of plutonium samples — a critical measurement for nuclear non-proliferation efforts and related forensics, as well as environmental monitoring, medical assays, and industrial safety. The novel device, based on "transition edge" sensor technology developed at NIST, is capable of ten times better resolution than all but the most expensive and time-consuming of current methods, and reduces the time needed for sample analysis from several days to one day.

A collaboration between NIST scientists and colleagues at Los Alamos National Laboratory (LANL) has resulted in a new kind of sensor that can be used to investigate the telltale isotopic composition of plutonium samples — a critical measurement for nuclear non-proliferation efforts and related forensics, as well as environmental monitoring, medical assays, and industrial safety.

The novel device, based on "transition edge" sensor technology developed at NIST (TESs are used in a variety of applications —see, for example, New High-Resolution X-ray Spectrometer for Beam Lines, and Adding Up Photons with a TES), is capable of ten times better resolution than all but the most expensive and time-consuming of current methods, and reduces the time needed for sample analysis from several days to one day. Researchers from NIST and LANL describe the new design and its results in the journal *Analytical Chemistry*.

NIST says that plutonium (Pu), highly radioactive and extensively employed in nuclear weapons and reactors, has many isotopes, and any trace sample contains slightly different proportions. **Pu-239 is the main constituent of both weapons-grade and power reactor-grade plutonium; Pu-240 is the principal minority isotope (Pu-240 is present in low concentrations in nuclear weapons owing to its tendency to fission spontaneously.** Concentrations are higher in reactor fuel and other uses).

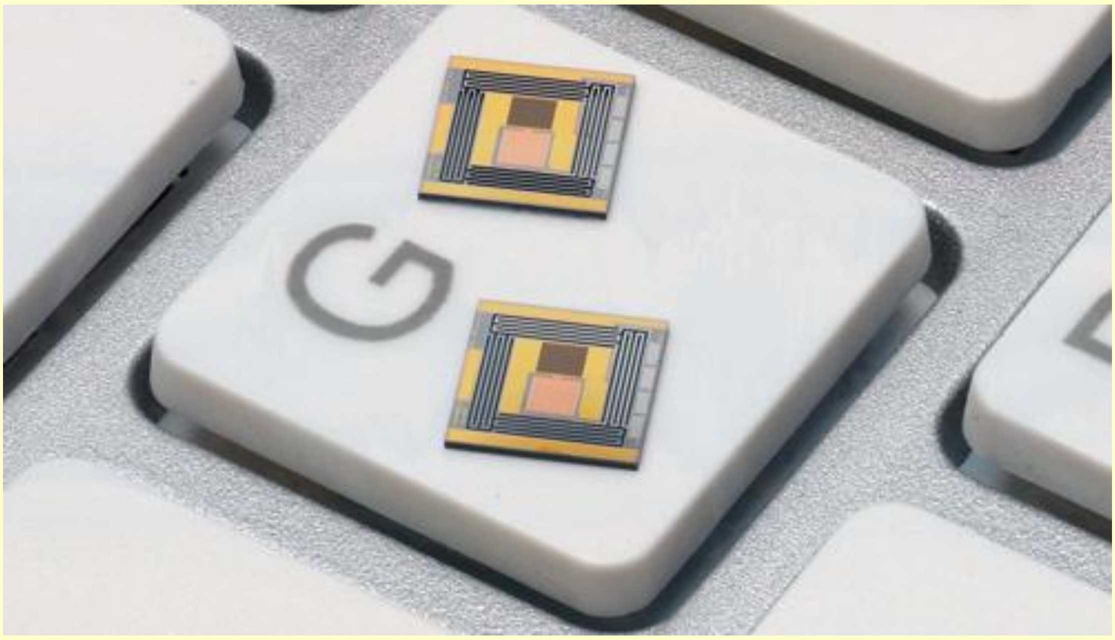
Analyzing the exact mass ratio of the two in a sample reveals important information about the material's origin, processing history, safety, and possible intended use. A key potential application in nuclear forensics is the attribution of a radiological event.

Until now, high-resolution mass-ratio results have only been possible by using mass spectrometry, a complicated procedure in which atoms of different masses travel different trajectories through a magnetic field. The more common, but less precise, method is to use solid-state detectors which absorb the alpha particles (when plutonium breaks down by fission into lighter elements, it emits alpha particles [two neutrons and two protons bound together, equivalent to a helium nucleus] as well as electrons and radiation) emitted by the radioactive sample and record their energy. Each isotope emits alphas with slightly different specific energies. So measuring the number of alpha particles at each energy level reveals the content of the sample.

"That sounds simple, but the issue is complicated by the fact that each isotope can have multiple decay modes that can lead to two, three, even four or more alpha particle energies per isotope," says Joel Ullom, leader of NIST's Quantum Sensors Project. "Even the best solid-state detectors cannot fully resolve all of the alpha particle energies, so the analysis of data from solid-state detectors relies on extensive knowledge of all of the overlapping alpha particle energy lines."

The TES-based design has better intrinsic energy resolving power than solid-state sensors. This is not the only advantage, however. "Since the TES is a thermal sensor, we can incorporate the radiological material directly into the sensor," says NIST project scientist Dan Schmidt. "The TES sensor can measure the total energy produced by each decay. This eliminates all of multiple alpha particle energies per isotope seen by conventional solid-state detectors, potentially greatly simplifying the analysis."

Transition-edge sensors (TES) are very small superconducting devices through which a trickle of current runs without resistance as long as the device stays below a critical temperature. Above that temperature, the sensor loses its superconductivity and reverts to normal electrical resistance. The device is cooled to the point at which it is on the edge of the transition between those two conditions.



Two of the TES-based devices sitting on one key of a computer keyboard. The brown rectangle at the top is the mount upon which the gold-and-plutonium sample is placed. It is connected to the TES (pink lower rectangle).

When a photon or particle deposits energy into the TES (or a surface attached to it), it raises the temperature of the device, superconductivity ceases, and the sudden onset of electrical resistance registers as an electrical signal.

NIST notes that to use the new sensor design, the LANL researchers dissolved plutonium samples in solvent and placed a few drops on a piece of gold foil about one-sixth the thickness of a human hair. The solvent evaporates, and the foil is folded up so that all the Pu is enclosed. The folded foil is then squeezed about 100 times until the particle size of the solvent residue is minimized and the Pu and gold are thoroughly mixed. As a result, the gold will absorb nearly 100 percent of all the energy of radiation and convert it to heat.

The gold-Pu mix is then pressed onto a mount pad attached to a TES sensor. The NIST team had to design a new kind of TES that was mechanically robust enough to withstand the bonding force. Previous TES sensors used delicate membranes; the new sensors employ silicon mechanical beams for structural support.

Alpha particles emitted by Pu-239 raise the gold mix to one temperature; those from Pu-240 raise it to a different temperature. The highly sensitive TES detects the difference and the associated electronics records the number of each type. After 21.4 hours of data at approximately one emission detection per second, plots of the data points showed two distinct energy peaks, one for each isotope, with almost no overlap.

The scientists tested their TES results against mass spectrometer analysis of the same sample material and found the results to be in good agreement.

"Obtaining high quality results on much faster time scales than mass spectrometry is extremely important," says NIST project scientist Dan Swetz. "If a radiological event occurs, the forensics will need to be completed as quickly as possible."

The new sensor design is only the latest in a long series of TES accomplishments at NIST's Physical Measurement Laboratory. "We have spent the last two decades developing transition edge sensors and their superconducting electronics," says Dave Rudman, leader of the Quantum Devices Group. "The broad uses of these sensors include telescopes studying the remnants of the Big Bang, optical photon detectors for quantum communication, X-ray spectrometers conducting applied and basic materials research, and gamma-ray spectrometers for analyzing spent nuclear fuel. While these and the new plutonium device span many orders of magnitude in energy, the underlying fundamental measurement principle is the same."

— Read more in Andrew S. Hoover et al., "Measurement of the 240Pu/239Pu Mass Ratio Using a Transition-Edge-Sensor Microcalorimeter for Total Decay Energy Spectroscopy," Analytical Chemistry, *Article ASAP (27 February 2015)*

Nuclear War in Ancient Times

If you are interesting to read more visit the following introductory articles:

http://www.zengardner.com/evidence-ancient-nuclear-war-earth/

http://ancientnuclearwar.com/

Automated Radiation Measurement Station Now Operational at Virginia Department of Health Building

Source:http://www.domesticpreparedness.com/Industry/Industry_Updates/Automated_Radiation_Measurement_Station_Now_Operational_at_Virginia_Department_of_Health_Building/

Boulder, CO - Apogee Communications Group announces NukAlert's Automated Radiation Measurement Station (ARMS) is now sending real time radiation reports from the Virginia Department of Health's building in Richmond to FEMA's RadReponder Network. The ARMS provides 24/7 radiation monitoring and can initiate shutoff of air intake to a building's HVAC system when a user defined radiation level is reached. The ARMS can also notify multiple users, by text and email, of radiation alerts.

Apogee distributes NukAlert's radiation detection devices to government and corporate accounts. The NukAlert's radiation equipment has been tested by Oak Ridge National Laboratory and reports radiation from 1μR/hr to 700R/hr with no saturation below 1,000R/hr.

The RadResponder Network collects real time radiation reports from local, state, and federal agencies. The network reports live data needed to characterize the incident and support lifesaving decisions.

P5+1, Iran agree on parameters of an agreement over Iran's nuclear program

Source: http://www.homelandsecuritynewswire.com/dr20150403-p5-1-iran-agree-on-parameters-of-an-agreement-over-irans-nuclear-program

April 03 – A couple of hours ago, the P5+1 and Iran announced the parameters of a Joint Comprehensive Plan of Action (JCPOA) regarding Iran's nuclear program. The parameters were decided in Lausanne, Switzerland, during marathon negotiation sessions which occupied most of the week.

These U.S. Department of State says that these elements form the foundation upon which the final text of the JCPOA will be written between now and 30 June, and that they "reflect the significant progress" which has been made in discussions between the P5+1, the European Union, and Iran. Many important implementation details are still to be negotiated, and State stressed that "nothing is agreed until everything is agreed."

The main elements of the parameters agreed to in Lausanne:

Enrichment

- Iran has agreed to reduce by approximately two-thirds its installed centrifuges. Iran will go from having about 19,000 installed today to 6,104 installed under the deal, with only 5,060 of these enriching uranium for ten years. All 6,104 centrifuges will be IR-1s, Iran's first-generation centrifuge.
- Iran has agreed to not enrich uranium over 3.67 percent for at least fifteen years.
- Iran has agreed to reduce its current stockpile of about 10,000 kg of low-enriched uranium (LEU) to 300 kg of 3.67 percent LEU for fifteen years.
- All excess centrifuges and enrichment infrastructure will be placed in IAEA monitored storage and will be used only as replacements for operating centrifuges and equipment.
- Iran has agreed not to build any new facilities for the purpose of enriching uranium for fifteen years.
- Iran's breakout timeline — the time that it would take for Iran to acquire enough fissile material for one weapon — is currently assessed to be two to three

months. That timeline will be extended to at least one year, for a duration of at least ten years, under this framework.

Iran will convert its facility at Fordow so that it is no longer used to enrich uranium

- Iran has agreed to not enrich uranium at its Fordow facility for at least fifteen years.
- Iran has agreed to convert its Fordow facility so that it is used for peaceful purposes only — into a nuclear, physics, technology, research center.
- Iran has agreed not to conduct research and development associated with uranium enrichment at Fordow for fifteen years.
- Iran will not have any fissile material at Fordow for fifteen years.
- Almost two-thirds of Fordow's centrifuges and infrastructure will be removed. The remaining centrifuges will not enrich uranium. All centrifuges and related infrastructure will be placed under IAEA monitoring.

Iran will only enrich uranium at the Natanz facility, with only 5,060 IR-1 first-generation centrifuges for ten years

- Iran has agreed to only enrich uranium using its first generation (IR-1 models) centrifuges at Natanz for ten years, removing its more advanced centrifuges.
- Iran will remove the 1,000 IR-2M centrifuges currently installed at Natanz and place them in IAEA monitored storage for ten years.
- Iran will not use its IR-2, IR-4, IR-5, IR-6, or IR-8 models to produce enriched uranium for at least ten years. Iran will engage in limited research and development with its advanced centrifuges, according to a schedule and parameters which have been agreed to by the P5+1.
- For ten years, enrichment and enrichment research and development will be limited to ensure a breakout timeline of at least one year. Beyond ten years, Iran will abide by its enrichment and enrichment R&D plan submitted to the IAEA, and pursuant to the JCPOA, under the Additional Protocol resulting in certain limitations on enrichment capacity.

Inspections and transparency

- The IAEA will have regular access to all of Iran's nuclear facilities, including to Iran's enrichment facility at Natanz and its former enrichment facility at Fordow, and including the use of the most up-to-date, modern monitoring technologies.
- Inspectors will have access to the supply chain that supports Iran's nuclear program. The new transparency and inspections mechanisms will closely monitor materials and/or components to prevent diversion to a secret program.
- Inspectors will have access to uranium mines and continuous surveillance at uranium mills, where Iran produces yellowcake, for twenty-five years.
- Inspectors will have continuous surveillance of Iran's centrifuge rotors and bellows production and storage facilities for twenty years. Iran's centrifuge manufacturing base will be frozen and under continuous surveillance.
- All centrifuges and enrichment infrastructure removed from Fordow and Natanz will be placed under continuous monitoring by the IAEA.
- A dedicated procurement channel for Iran's nuclear program will be established to monitor and approve, on a case by case basis, the supply, sale, or transfer to Iran of certain nuclear-related and dual use materials and technology — an additional transparency measure.
- Iran has agreed to implement the Additional Protocol of the IAEA, providing the IAEA much greater access and information regarding Iran's nuclear program, including both declared and undeclared facilities.
- Iran will be required to grant access to the IAEA to investigate suspicious sites or allegations of a covert enrichment facility, conversion facility, centrifuge production facility, or yellowcake production facility anywhere in the country.
- Iran has agreed to implement Modified Code 3.1 requiring early notification of construction of new facilities.
- Iran will implement an agreed set of measures to address the IAEA's concerns regarding the Possible Military Dimensions (PMD) of its program.

Reactors and reprocessing

- Iran has agreed to redesign and rebuild a heavy water research reactor in Arak, based on a design that is agreed to by the P5+1, which will not produce weapons grade plutonium, and which will support peaceful nuclear research and radioisotope production.
- The original core of the reactor, which would have enabled the production of significant quantities of weapons-grade plutonium, will be destroyed or removed from the country.
- Iran will ship all of its spent fuel from the reactor out of the country for the reactor's lifetime.
- Iran has committed indefinitely to not conduct reprocessing or reprocessing research and development on spent nuclear fuel.
- Iran will not accumulate heavy water in excess of the needs of the modified Arak reactor, and will sell any remaining heavy water on the international market for fifteen years.
- Iran will not build any additional heavy water reactors for fifteen years.

Sanctions

- Iran will receive sanctions relief, if it verifiably abides by its commitments.
- U.S. and E.U. nuclear-related sanctions will be suspended after the IAEA has verified that Iran has taken all of its key nuclear-related steps. If at any time Iran fails to fulfill its commitments, these sanctions will snap back into place.
- The architecture of U.S. nuclear-related sanctions on Iran will be retained for much of the duration of the deal and allow for snap-back of sanctions in the event of significant non-performance.
- All past UN Security Council resolutions on the Iran nuclear issue will be lifted simultaneous with the completion, by Iran, of nuclear-related actions addressing all key concerns (enrichment, Fordow, Arak, PMD, and transparency).
- However, core provisions in the UN Security Council resolutions — those that deal with transfers of sensitive technologies and activities — will be re-established by a new UN Security Council resolution that will endorse the JCPOA and urge its full implementation.
- It will also create the procurement channel mentioned above, which will serve as a key transparency measure. Important restrictions on conventional arms and ballistic missiles, as well as provisions that allow for related cargo inspections and asset freezes, will also be incorporated by this new resolution.
- A dispute resolution process will be specified, which enables any JCPOA participant, to seek to resolve disagreements about the performance of JCPOA commitments.
- If an issue of significant non-performance cannot be resolved through that process, then all previous UN sanctions could be re-imposed.
- U.S. sanctions on Iran for terrorism, human rights abuses, and ballistic missiles will remain in place under the deal.

Phasing

- For ten years, Iran will limit domestic enrichment capacity and research and development — ensuring a breakout timeline of at least one year. Beyond that, Iran will be bound by its longer-term enrichment and enrichment research and development plan it shared with the P5+1.
- For fifteen years, Iran will limit additional elements of its program. For instance, Iran will not build new enrichment facilities or heavy water reactors and will limit its stockpile of enriched uranium and accept enhanced transparency procedures.
- Important inspections and transparency measures will continue well beyond fifteen years. Iran's adherence to the Additional Protocol of the IAEA is permanent, including its significant access and transparency obligations. The robust inspections of Iran's uranium supply chain will last for 25 years.
- Even after the period of the most stringent limitations on Iran's nuclear program, Iran will remain a party to the Nuclear Non-Proliferation Treaty (NPT), which prohibits Iran's development or acquisition of nuclear weapons and requires IAEA safeguards on its nuclear program.

Thousands attend anti-Trident rally in Glasgow

Source: http://www.heraldscotland.com/politics/scottish-politics/thousands-attend-anti-trident-rally-in-glasgow.1428156845

14

Apr 04 – **Thousands of anti-nuclear protesters have come together in a major rally calling on politicians to scrap Trident.**

Inverness
Aberdeen
Faslane Base
Dundee
Edinburgh
Glasgow
Belfast
UNITED KINGDOM
Leeds
Kingston upon Hull
Dublin
Liverpool
IRELAND
Stoke-on-Trent
Birmingham
London
Bristol
Poole
Channel
3D

Speaker Nicola Sturgeon told the crowd at the Bairns Not Bombs demonstration in Glasgow she thought it the largest of its kind ever staged in the city.

With just over a month until the General Election, campaigners marched through the city centre before filling George Square with a sea of placards and banners.

The rally, organised by the **Scrap Trident group**, will be followed on April 13 by a blockade of **Faslane naval base**, home of the UK's nuclear deterrent.

The action is geared towards piling pressure on Westminster candidates to block the renewal of the nuclear weapon system and invest in public services.

The First Minister said: "One of the biggest decisions that MPs will take in the next Parliament is whether **to waste £100 billion on renewing these morally obscene weapons.**

"Broken down, that'll be around £3 billion a year, peaking at an eye-watering £4 billion in the 2020s.

"We all know that Trident is morally unjustifiable, but at a time when the Westminster parties are all committed to forcing yet more austerity on us after the election Trident is economically indefensible.

"Just think of what could be achieved with this money for the NHS, education or other public services - not just in Scotland, but across the UK."

A police estimate suggests around 2,500 people attended the rally, while organisers said the figure was closer to 4,000.

Scottish Green party co-convenor Patrick Harvie told the crowd: "There's a wave of anger up and down Scotland and throughout these islands at the idea of cutting billions from the budget that support the most vulnerable people in society, while spending even more billions on a new generation of weapons of mass destruction.

"Your job over the coming weeks is to make sure people hear the alternative voice.

"You need to take the message out day after day, to friends, family, your colleagues, your neighbours, make sure they bring the issue of Trident to the top of the political agenda when they decide how they will cast their vote.

"Let's convince everybody in this country to vote no to Trident."

Ms Sturgeon said: "All of us must put the question of Trident renewal at the top of the agenda over the next few weeks.

"The MPs you elect next month will decide whether we renew Trident.

"The choice could not be clearer. You can vote to spend £100 billion on a new generation of weapons of mass destruction.

"Or you can vote to spend £100 billion on building a fairer and more prosperous society.

"Future generations will never forgive us if we make the wrong choice."

Labour's North Ayrshire candidate Katy Clark also addressed the rally, along with Cat Boyd from the Radical Independence Campaign and Ann Henderson of the STUC.

EDITOR'S COMMENT: Some simple easy/difficult questions arose here: Nuclear missiles or jobs, food, health insurance? Is there a real threat justifying nukes? Is UK a super-power or not? Does UK really need strong Armed Forces? Do protesters and rally organizers really believe what they protest for? Is it enough to scrap your own nukes when other have them or planning to aquire them? Will opposition scrap nukes if becomes the ruling party? And many more! It would be nice to eliminate all weapons fo mass destruction and spend money to the people and for the people. But we all know that this will not happen – at least not in this life time! Same with conventional weapons – it would be great if Greece did not have to spend billions on weaponry and instead pay back its depts and invest in progress. Recently there was a debate about spending 500 mil euro for the renovation of five P3 Orion aircrafts (expanding their operational life by 20 years) when only 200 mil euro where given for the ongoing humanitarian crisis in Greece. At the same time hundreds of national air space violations (on daily basis) from Turkish Air Force evaporate every thought of reducing defense expenses in favor to the people. Life could be a "beach" but for the time being is only a "bitch" and we have to live with it.

New START Treaty Count: Russia Dips Below US Again

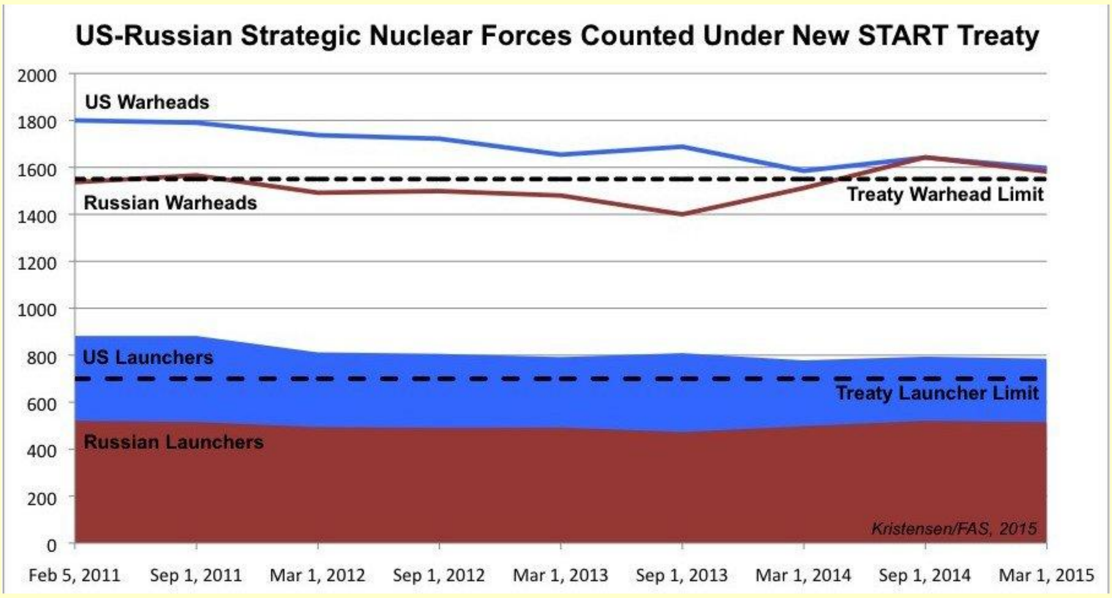
Source: http://fas.org/blogs/security/2015/04/newstart2015/

Russian deployed strategic warheads counted by the New START Treaty once again slipped below the U.S. force level, according to the latest fact sheet released by the State Department.

The so-called aggregate numbers show that Russia as of March 1, 2015 deployed 1,582 warheads on 515 strategic launchers. The U.S. count was 1,597 warheads on 785 launchers.

Back in September 2014, the Russian warhead count for the first time in the treaty's history moved above the U.S. warhead count. The event caused U.S. defense hawks to say it showed Russia was increasing it nuclear arsenal and blamed the Obama administration. Russian news media gloated Russia had achieved "parity" with the United States for the first time.

Of course, none of that was true. The ups and downs in the aggregate data counts are fluctuations caused by launchers moving in an out of overhaul and new types being deployed while old types are being retired. The fact is that both Russia and the United States are slowly – very slowly – reducing their deployed forces to meet the treaty limits by February 2018.

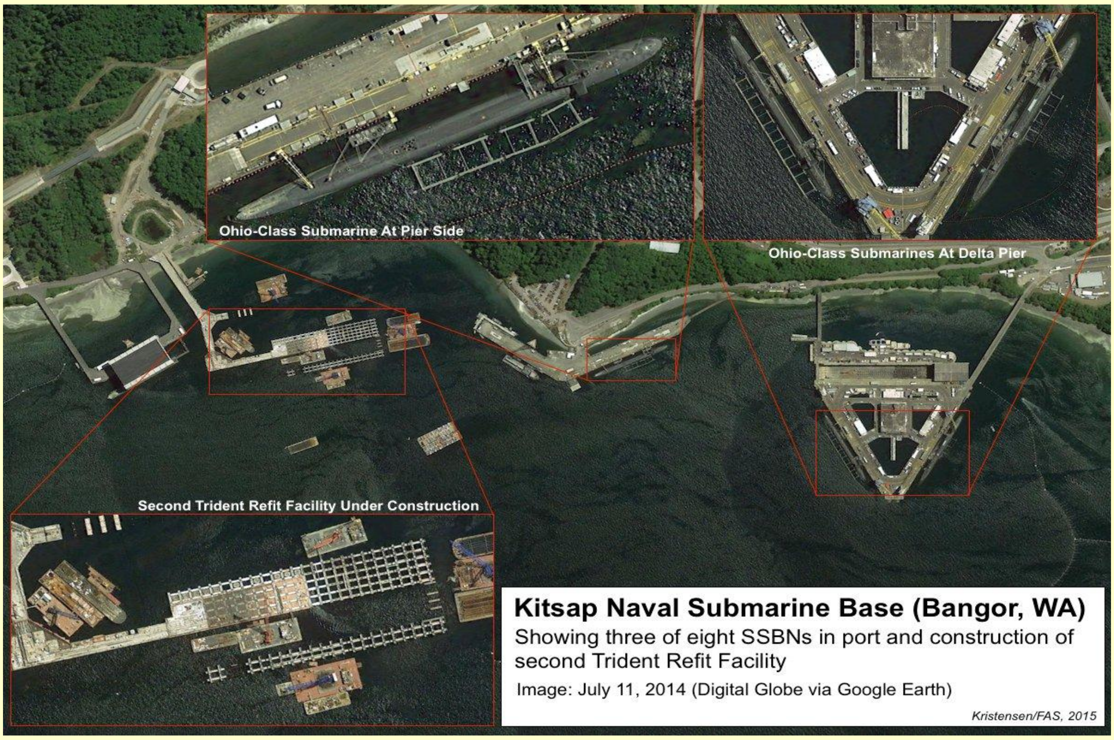


New START Count, Not Total Arsenals

And no, the New START data does now show the total nuclear arsenals of Russia and the United States, only the portion of them that is counted by the treaty.

While New START counts 1,582 Russian deployed strategic warheads, the country's total warhead inventory is much higher: an estimated 7,500 warheads, of which 4,500 are in the military stockpile (the rest are awaiting dismantlement).

The United States is listed with 1,597 deployed strategic warheads, but actually possess an estimated 7,100 warheads, of which about 4,760 are in the military stockpile (the rest are awaiting dismantlement).

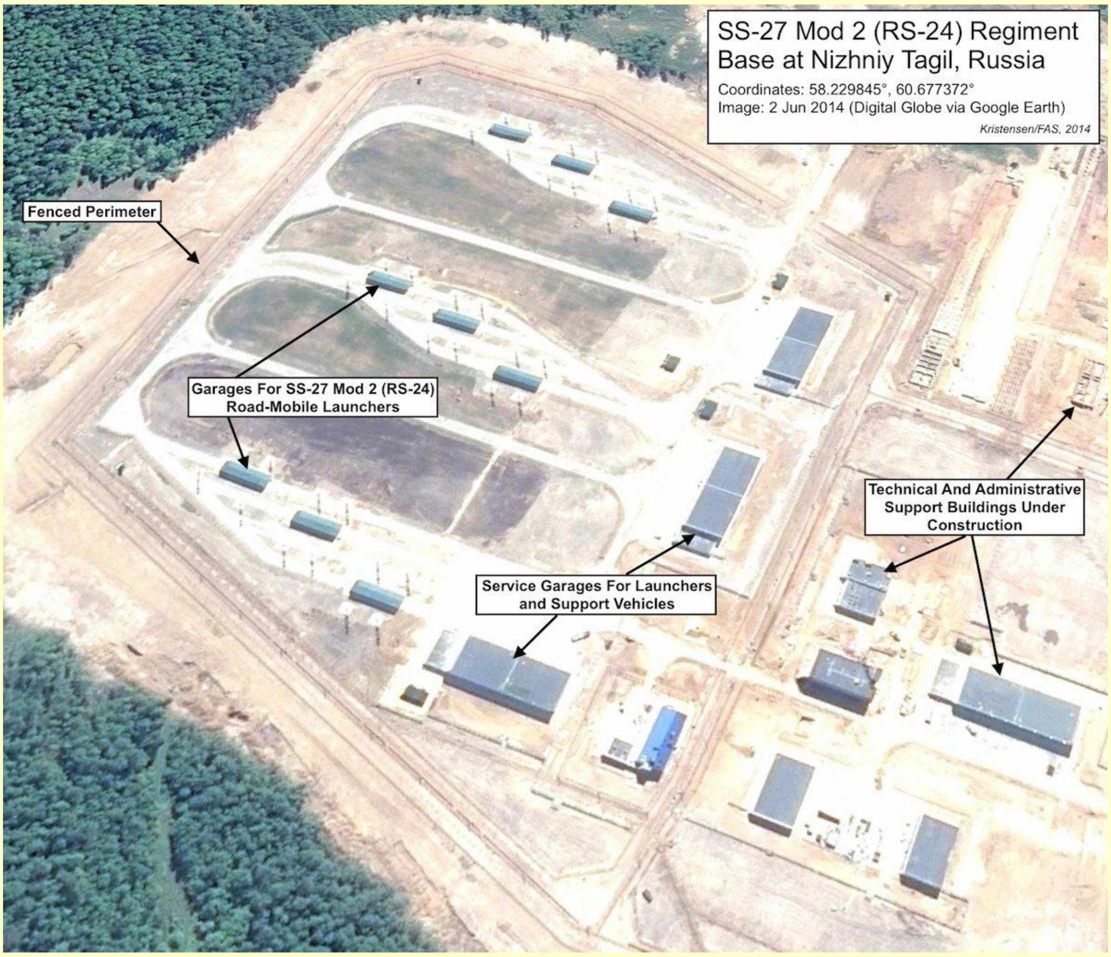

Ohio-Class Submarine At Pier Side
Ohio-Class Submarines At Delta Pier
Second Trident Refit Facility Under Construction
Kitsap Naval Submarine Base (Bangor, WA)
Showing three of eight SSBNs in port and construction of second Trident Refit Facility
Image: July 11, 2014 (Digital Globe via Google Earth)
Kristensen/FAS, 2015

In 2015 the U.S. Navy will begin reducing the number of missile tubes from 24 to 20 on each SSBN, three of which are seen in this July 2014 photo at Kitsap Naval Submarine Base at Bangor (WA). The image also shows construction underway of a second Trident Refit Facility (coordinates: 47.7469°, -122.7291°).

The two countries only have to make minor adjustments to their forces to meet the treaty limit of 1,550 deployed strategic warheads by February 2018.

Launcher Disparity

The launchers (ballistic missiles and heavy bombers) are a different matter. Russia has been far below the treaty limit of 700 deployed launchers since before the treaty entered into effect in 2011. Despite the nuclear "build-up" alleged by some, Russia is currently counted as deploying 515 launchers – 185 launchers below the treaty limit.


SS-27 Mod 2 (RS-24) Regiment
Base at Nizhniy Tagil, Russia
Coordinates: 58.229845°, 60.677372°
Image: 2 Jun 2014 (Digital Globe via Google Earth)
Kristensen/FAS, 2014
Fenced Perimeter
Garages For SS-27 Mod 2 (RS-24) Road-Mobile Launchers
Technical And Administrative Support Buildings Under Construction
Service Garages For Launchers and Support Vehicles

Modernization of mobile ICBM garrison base at Nizhniy Tagil in the Sverdlovsk province in Central Russia. The garrison is upgrading from SS-25 to SS-27 Mod 2 (RS-24) (coordinates: 58.2289°, 60.6773°).

In other words, Russia doesn't have to reduce any more launchers under New START. In fact, it could deploy an additional 185 nuclear missiles over the next three years and still be in compliance with the treaty.

The United States is counted as deploying 785 launchers, 270 more than Russia. The U.S. has a surplus in all three legs of its strategic triad: bombers, ICBMs, and SLBMs. To get down to the 700 launchers, the U.S. Air Force will have to destroy empty ICBM silos, dismantle nuclear equipment from excess B-52H bombers, and the U.S. Navy will reduce the number of launch tubes on each ballistic missile submarine from 24 to 20.

Even when the treaty enters into force in 2018, a considerable launcher disparity will remain. The United States plans to have the full 700 deployed launchers. Russia's plans are less certain but appear to involve fewer than 500 deployed launchers.

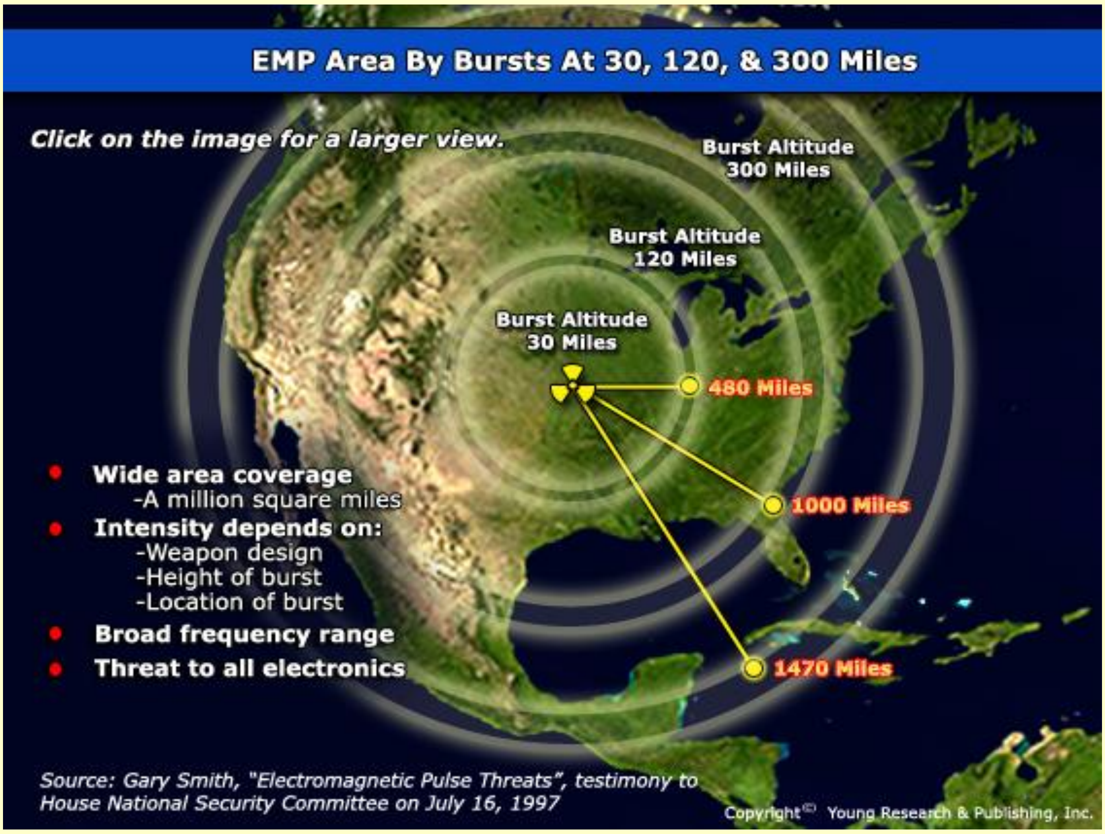
Russia is compensating for this disparity by transitioning to a posture with a greater share of the ICBM force consisting of MIRVed missiles on mobile launchers. This is bad for strategic stability because a smaller force with more warheads on mobile launchers would have to deploy earlier in a crisis to survive. Russia has already begun to lengthen the time mobile ICBM units deploy away from their garrisons.

It seems obvious that the United States and Russia will have to do more to cut excess capacity and reduce disparity in their nuclear arsenals.

EDITOR'S COMMENT: Perhaps this article might provide some answers posed after the previous article ("Scrap Trident").

Iranian plan for EMP attack on the US

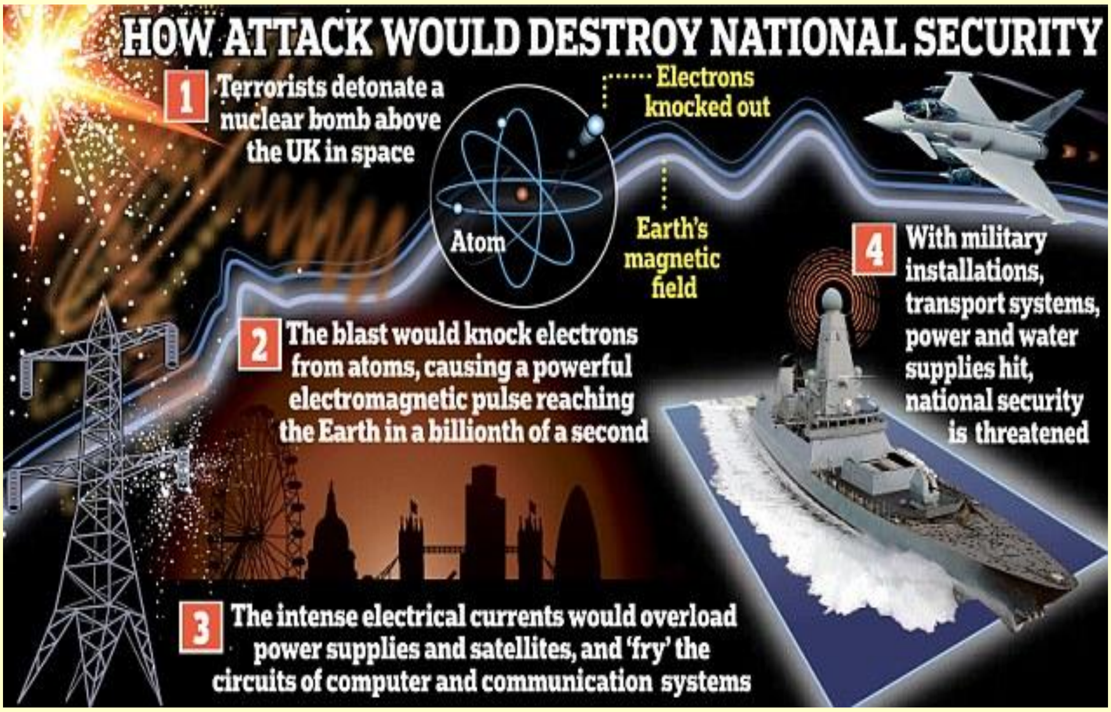
Source: http://i-hls.com/2015/04/iranian-plan-for-emp-attack-on-the-us


EMP Area By Bursts At 30, 120, & 300 Miles
Click on the image for a larger view.
Burst Altitude 300 Miles
Burst Altitude 120 Miles
Burst Altitude 30 Miles
480 Miles
1000 Miles
1470 Miles
Wide area coverage
-A million square miles
Intensity depends on:
-Weapon design
-Height of burst
-Location of burst
Broad frequency range
Threat to all electronics
Source: Gary Smith, "Electromagnetic Pulse Threats", testimony to House National Security Committee on July 16, 1997
Copyright© Young Research & Publishing, Inc.

Apr 07 – **According to *WND* news site a "secret" Iranian military handbook confirms that Iran is including among its arsenal of plans, to launch a nuclear electromagnetic pulse (EMP) attack on the US.** An EMP attack is an attack brought about by a high altitude nuclear explosion that has a devastating effect on the electrical grid and other life supporting infrastructures on the ground. It could, potentially, black out a country for weeks and even months. Carrying out such an attack would require Iran to have not only the missiles to launch such a device but the technology to produce a nuclear explosion.

The revelation comes as the United States, along with the countries comprising the United Nations Security Council, have finalized a deal regarding Iran's nuclear development program. Concerns have been raised regarding Iran continuing with its plan to produce nuclear weapons and about the agreement just signed not doing enough to prevent this from taking place.

The *WND* has been reporting about this topic as far back as 2005, when intelligence sources were quoted as saying: "Iran is not only covertly developing nuclear weapons, it is already testing ballistic missiles specifically designed to destroy America's technical infrastructure, effectively neutralizing" the US.


HOW ATTACK WOULD DESTROY NATIONAL SECURITY
1 Terrorists detonate a nuclear bomb above the UK in space
Electrons knocked out
Atom
Earth's magnetic field
2 The blast would knock electrons from atoms, causing a powerful electromagnetic pulse reaching the Earth in a billionth of a second
4 With military installations, transport systems, power and water supplies hit, national security is threatened
3 The intense electrical currents would overload power supplies and satellites, and 'fry' the circuits of computer and communication systems

Dr. Vincent Pry, a US expert on Nuclear Strategy and the use of Electromagnetic pulse has written in a recent column in Israeli news site *Aruz Sheva*, **that not only do "Iranian military documents describe such a scenario… a recently translated Iranian military textbook endorses nuclear EMP attacks against the United States."**

An Iranian EMP attack, using only a small number of nuclear missiles or even one, can threaten the existence of modernity and be the death knell of Western principles of international law, humanism and freedom," Pry wrote.

"They could put a weapon on a boat or freighter, and if Iran has ballistic missiles it could put it anywhere on the U.S. coast," said John Bolton, former U.S. ambassador to the United Nations and a senior fellow at the Washington-based American Enterprise Institute.

According to sources, the Iranian military handbook refers to an EMP attack on some 20 locations in the United States.

The structure that will protect Chernobyl's reactor 4 enters final phase

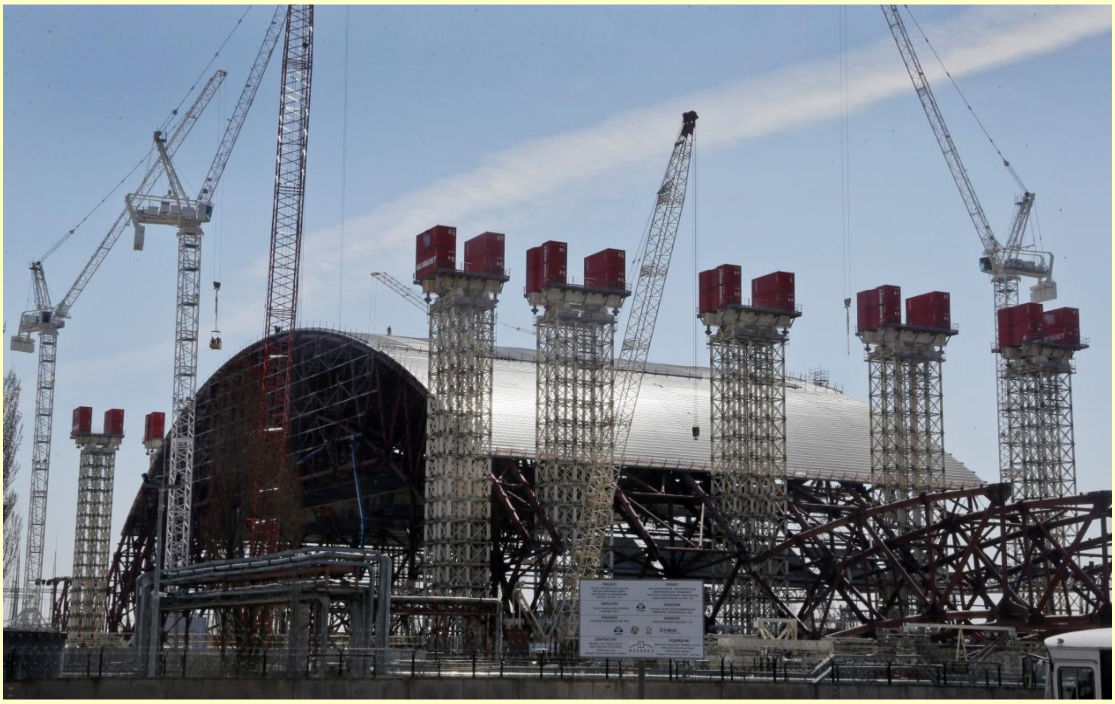
Source: http://it.euronews.com/2015/03/18/chernobyl-la-struttura-che-proteggera-il-reattore-4-entra-nella-fase-finale/

The construction of the immense structure that will protect the reactor number four of the Chernobyl nuclear power plant disaster enters the final phase.

The flaps of this arc composed from 32 thousand tons of steel and concrete will be merged in April. Once dropped on the reactor and the old sarcophagus that covers it, it will trap radioactive emissions caused by the accident of 26 April 1986.

"The area of exclusion will never be free from radioactive waste," says Vince Novak, responsible for nuclear safety of the Bank for Reconstruction and Development, who adds: "The intention is to permanently maintain an area for storage and treatment of waste."

Designers stressed that so ambitious project has never been made before. Operational from 2017, will last at least a hundred years.



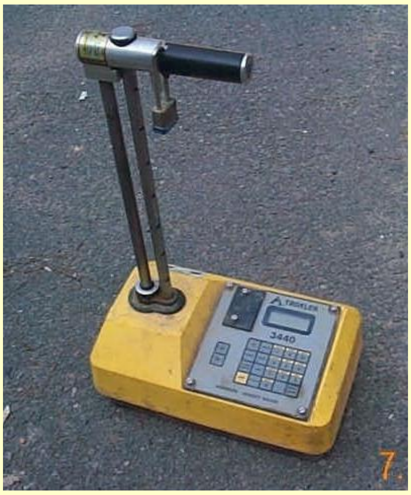
"This arc will protect the sarcophagus where today all radioactive material is contained- says engineer Volodymyr Verbytskyi - Around here, you can not live until at least ten other half lives, that is for another 300 years."

The shelter will be 105 meters high and 257 meters wide. The cost is around 2.15 billion euro, financed, among others, by the European Union, the members of the G7 and Russia.

But waste disposal poses many challenges, as explained by the envoy euronews, Sergio Cantone: "The realization of the protective structure proceeds and will be delivered on time. However, much remains to be done. And the scientific solutions are far: as you take away all those elements will radiation still be present in the reactor number four? ".

Radioactive Gauge Stolen from Pulaski Co. Construction

Source: http://www.arkansasmatters.com/story/d/story/radioactive-gauge-stolen-from-pulaski-co-construct/20797/XxtVK6NaLk6HJQq3BVzBQg



March 30 – The Arkansas Department of Health, Radiation Control Program received notification today that a gauge containing radioactive material has been stolen from a construction site near I-40 West in Northwest Pulaski County, Arkansas.

The device contains shielding and is not dangerous if it remains intact. However, the device could present a radiation hazard if it was damaged and the radioactive sources were exposed or removed from their sealed container.

The gauge transport case is about the size and shape of a trunk and is made of a hard, yellow plastic with handles on each end and the top. The gauge itself is also yellow with a rectangular base and a foot-long handle on top (photographs are attached). Both are clearly labeled as radioactive. The gauge and transport case weighs approximately 85 to 95 pounds.

The gauge contains approximately 8 millicuries of cesium-137 and 40 millicuries of americium-241. It is used to take moisture and density measurements by projecting radiation from the two radioactive sources into the ground and then displaying the amount of radiation reflected back to the gauge. The gauge is described as a Troxler Electronic Laboratories Model 3440, Serial Number 25959. State police, local government officials and law enforcement agencies, the United States Nuclear Regulatory Commission and the Arkansas Department of Emergency Management have also been notified.

Although the gauge poses a potential public health risk, it does not contain sufficient material to be used for any explosive device.

UPDATE (April 8, 2015)

The radioactive gauge has been found. According to the Arkansas Department of Health it was recovered near the Marche community in Pulaski County. There is no evidence that the gauge posed a health risk to anyone during its absence. The gauge does not appear to be damaged, and has been taken to a permanent storage location.

Each Of These Radioactive Vases Is Made From The Toxic Sludge Byproduct Of Your Phone, Computer, Car

Source: http://www.fastcocreate.com/3044979/each-of-these-radioactive-vases-is-made-from-the-toxic-sludge-byproduct-of-your-phone-comput

3 finished vases, conceived by Unknown Fields Division and produced with Kevin Callaghan, a ceramics artist, will be on display in the V and A Gallery.Photo: Toby Smith, courtesy of Unknown Fields.

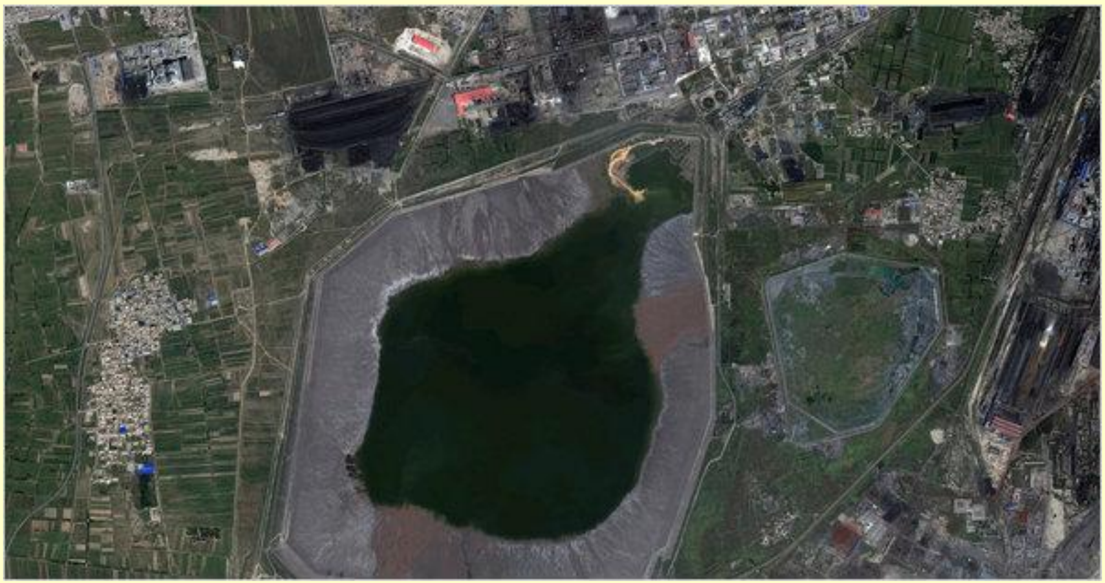
Ceramic vases made from toxic mud created in the production of must-have products such as laptops and smartphones will present a markedly different perspective on consumer technology when they go on show at London's Victoria & Albert Museum later this month.

The mud was collected from a toxic lake in Inner Mongolia into which thick, black chemical waste is pumped from neighboring refineries in and around Baotou, the region's largest industrial city.

China produces an estimated 95% of the world's supply of "rare earth" elements.

MONGOLIA
Baotou
Beijing
Shanghai
CHINA

Baotou is one of the world's biggest suppliers of the materials—elements found in anything from magnets and wind turbines and electric car motors to the electronic guts of smart phones and flat screen TVs.



This lake outside of Baotou, China, contains sludge laced with toxic chemical compounds from rare earth processing.

The ceramics were produced by The Unknown Fields Division, a self-declared "nomadic design studio" headed by Liam Young and Kate Davies and developed within the Architectural Association in London, whose aim is to reflect the shadows luxury products cast across the planet.

"The vases are a way to talk about ideas around luxury and desire. How both are culturally constructed collective sets of values that are fleeting and particular to our time," says Davies.

"These three 'rare earthenware' vessels are the physical embodiment of a contemporary global supply network that displaces earth and weaves matter across the planet."

Adds Young: "The dominant media narrative about our technologies is based on lightness and thinness. Terms like 'cloud' of 'Macbook Air' imply that our gadgets are just ephemeral objects—and this is the story we all want to believe.

"In reality, our technologies should really be thought of as geological artefacts that are carved out of the earth and produced by a planetary-scaled factory."

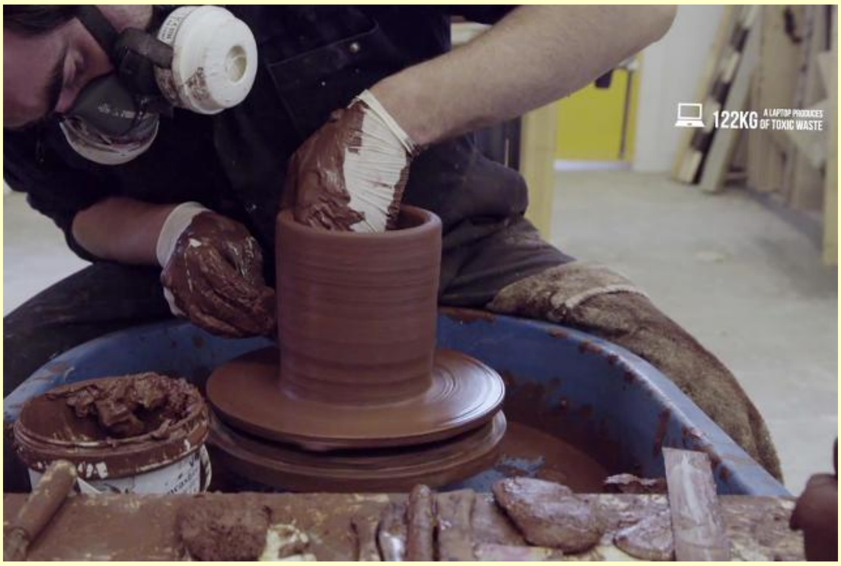
Unknown Fields travels the world to explore landscapes and infrastructures critical to the production of contemporary cities and the technologies they contain – often forgotten landscapes scarred by consumer demand.

With an approach that's part design-focused, part investigative journalism the studio uses techniques such as film, animation and fiction

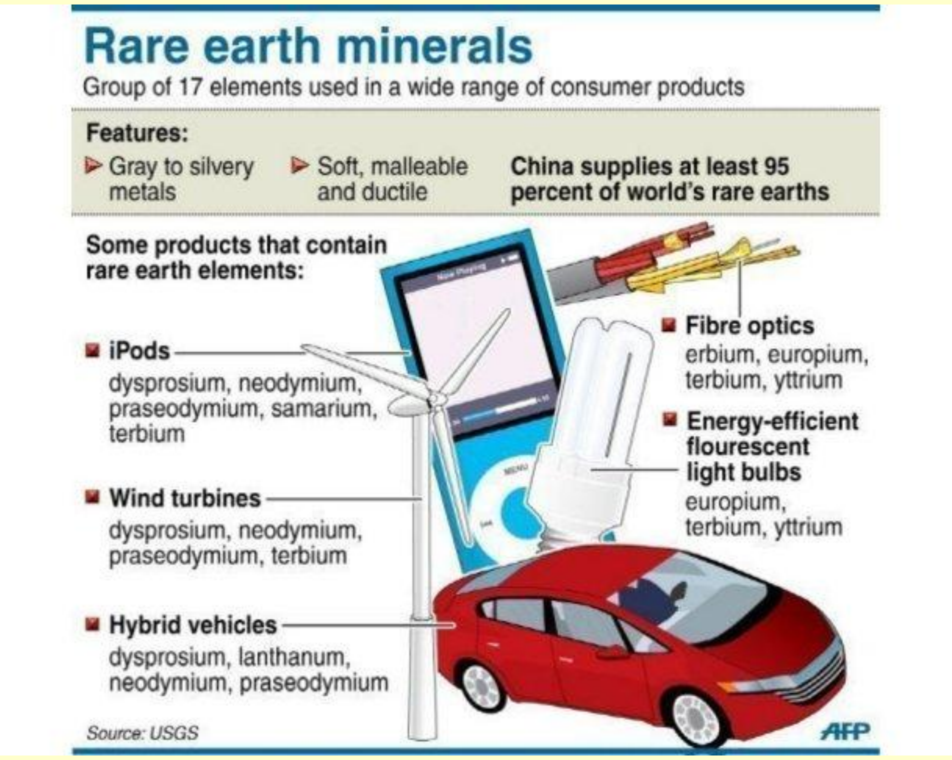
to develop what they call 'counter narratives' that encourage an audience to consider how we might relate to these sites in different ways.

The "rare earthenware" project evolved out of a trip Unknown Fields organized last summer taking around 20 creatives from a mix of disciplines to visit Baotou's toxic lake. The V&A was already keen to work with the studio, and commissioned the ceramics to feature in its What is Luxury? Exhibition opening on April 25.

The expedition traced the supply lines of contemporary technologies from the high street in London back through container ships and industrial ports in Asia to the factories of China and the refineries and mining pits of Inner Mongolia.



The team was accompanied by photographer Toby Smith who documented the trip during which toxic mud was gathered. Also involved was ceramicist Kevin Callaghan who produced the vases.


Rare earth minerals
Group of 17 elements used in a wide range of consumer products
Features:
Gray to silvery metals
Soft, malleable and ductile
China supplies at least 95 percent of world's rare earths
Some products that contain rare earth elements:
iPods
dysprosium, neodymium, praseodymium, samarium, terbium
Wind turbines
dysprosium, neodymium, praseodymium, terbium
Hybrid vehicles
dysprosium, lanthanum, neodymium, praseodymium
Fibre optics
erbium, europium, terbium, yttrium
Energy-efficient flourescent light bulbs
europium, terbium, yttrium
Source: USGS
AFP

The ceramic vessels are made from the amount of toxic mud that is generated in the production of each of the objects of technology Unknown Fields chose them to represent: the smartphone, the flat screen computer, and the electric car.

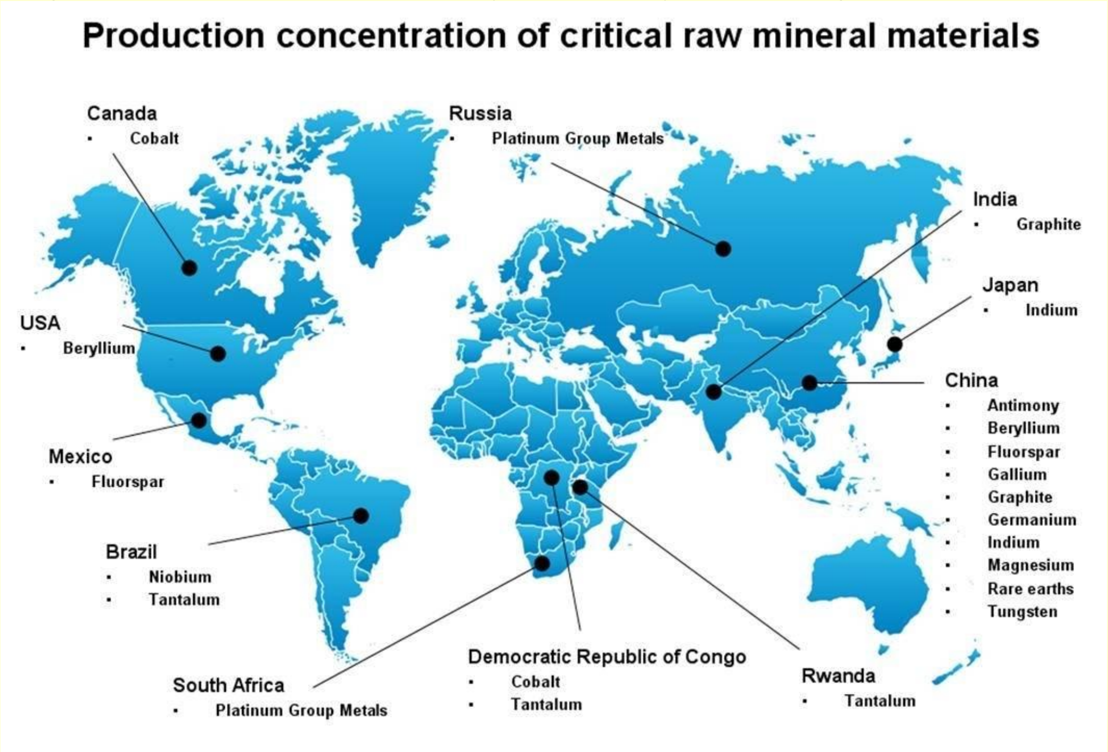
"The size of each vase is a direct result from how much toxic waste each of these single objects generates in its production," says Young.

"The surface finish of the vase also comes from the toxic material used. Because the heavy metals of the lake mud is so incredibly high, when it is fired in a pottery kiln those metals melt and create their own glistening glaze on the surface of the vase."

In silhouette they echo highly valuable Ming dynasty porcelain 'Tongping' or 'Sleeve' vases, Davies adds. "Vases are traditionally objects of value and display wealth," she continues. "Ming vases are particularly iconic objects of high value as well as being artefacts of international trade."

Due to the mud's toxicity, everyone involved had to wear dust masks, gloves, goggles and protective suits when handling the material at each stage of the production process and any waste was disposed of via hazardous material routes.

"An entire city is built beside this toxic lake in Inner Mongolia, yet



for us to be safe when handling this material and get past the museum's health and safety team we all needed fully body protection," Young adds.

An important part of the project is an accompanying film in which Toby Smith and the Unknown Fields team depicts a reverse journey back up the entire supply chain in a single, continuous panning shot ending in Mongolia's rare earth mineral mines.

"The film presents the supply chain of tech gadgets as a continuous factory that stretches across the planet – almost like a continuous conveyor belt spanning from the Apple shop to the Mongolian rare earth mineral mines," Young says.

"The three vases are presented as objects of desire, but their elevated radiation levels and toxicity make them objects we would not want to possess," adds Davies. "They represent the undesirable consequences of our materials desires."

Iran's Nuclear Timetable

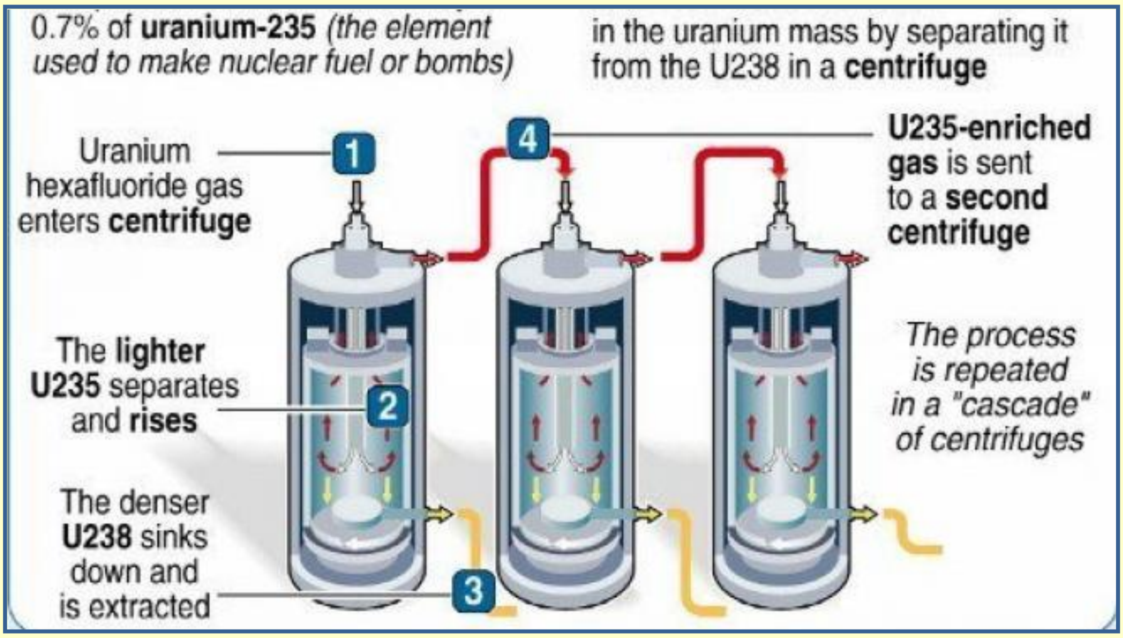
February 24, 2015
Source: http://www.iranwatch.org/our-publications/articles-reports/irans-nuclear-timetable

This report estimates how soon Iran could fuel a nuclear weapon. With its thousands of gas centrifuges, Iran now has the ability to enrich uranium to a grade suitable for use in nuclear reactors or to a higher grade suitable for use in nuclear warheads. The data below, which are based on reports from the International Atomic Energy Agency, describe Iran's uranium stockpile, its centrifuges, and the rate at which its nuclear capacity is growing. [a]

Highlights:

- **By using the approximately 9,000 first generation centrifuges operating at its Natanz Fuel Enrichment Plant, Iran could theoretically produce enough weapon-grade uranium to fuel a single nuclear warhead in about 1.7 months.**

- Iran's more advanced IR-2m centrifuges, about 1,000 of which are installed at Natanz, would allow Iran to produce weapon-grade uranium more quickly.


0.7% of uranium-235 (the element used to make nuclear fuel or bombs)
in the uranium mass by separating it from the U238 in a centrifuge
Uranium hexafluoride gas enters centrifuge
1
4
U235-enriched gas is sent to a second centrifuge
The lighter U235 separates and rises
2
The process is repeated in a "cascade" of centrifuges
The denser U238 sinks down and is extracted
3

- Iran's stockpile of low-enriched uranium is now sufficient, after further enrichment, to fuel approximately seven nuclear warheads.

- Because Russia has a ten-year contract to fuel Iran's only power reactor at Bushehr, Iran has no present need for enriched uranium to generate civilian nuclear energy.
- Iran could fuel approximately 25 first generation implosion bombs if it had the ability to enrich the uranium needed to supply the Bushehr reactor annually.

Bomb potential of Iran's low-enriched uranium

- Total amount of uranium hexafluoride (UF6) enriched to approximately 3.5 percent U-235 produced as of February 2015: 14,175 kg [b]
- Amount of this material ready for further enrichment (i.e., stored in gaseous form) as of February 2015: 7,953 kg [c]
- Amount theoretically needed to produce a bomb's worth of weapon-grade uranium metal: 1,053 kg [d]

- Number of first generation implosion bombs this 7,953 kilograms could fuel, if further enriched: 7 [e]
- Time needed to convert this uranium to one bomb's worth of finished uranium metal enriched to 90 percent U-235: 3 - 12 months [f]
- Date by which Iran's uranium stockpile probably was sufficient to fuel one first generation implosion bomb, if further enriched: February 2009 [g]
- Approximate number of first generation IR-1 centrifuges being fed with UF6 at the Natanz Fuel Enrichment Plant, as of the last reported visit by IAEA inspectors: 9,000 [h]
- Number of months theoretically needed for these 9,000 centrifuges operating at their present capacity to produce enough enriched uranium for one bomb: 1.7 [i]

Civilian need for this uranium

- Approximate amount of low-enriched uranium needed annually to fuel Iran's sole civilian power reactor at Bushehr: 21 metric tons [j]
- Percent of this uranium Russia will supply under a ten-year fuel contract: 100 [k]
- Number of years it would take the roughly 9,000 operating IR-1 centrifuges at Natanz to produce one year's worth of fuel for Bushehr: 10.7 [l]
- Approximate number of separative work units (amount of enrichment work)[m] Iran would need to generate in order to produce one year's worth of fuel for Bushehr: 100,000 [n]
- Number of IR-1 centrifuges Iran would need to operate in order to produce this level of work annually: 128,000 [o]
- Approximate number of first generation implosion bombs Iran could fuel if able to enrich the uranium needed to supply Bushehr annually: 25 [p]

Comments

- Before using uranium in a warhead, it must be enriched to weapon-grade (90 percent or more U-235) and processed into a metallic shape sufficient to explode in a chain reaction.
- This assessment assumes that Iran would use 16 kg of weapon-grade uranium (~90 percent U-235) in the finished core of each nuclear weapon. Sixteen kilograms are assumed to be sufficient for an implosion bomb. This was the amount called for in the implosion device Saddam Hussein was trying to perfect in the 1980's, and the design for such a device has circulated on the nuclear black market, to which Iran has had access. Some experts believe that Iran could use less material, assuming Iran would accept a lower yield for each weapon. According to these experts, Iran could use as few as seven kilograms of this material if Iran's weapon developers possessed a "medium" level of skill, and if Iran were satisfied with an explosive yield slightly less than that of the bomb dropped on Hiroshima, Japan. [q] If Iran chose to use an amount smaller than 16 kg, the time required to make each weapon would be less than estimated here. Or, in the amount of time estimated here, Iran could make a greater number of weapons. Iran could decide not to use such a smaller amount of weapon-grade uranium if Iran wanted to have more confidence that its weapons would work, or if it wanted to reduce the size of its weapons by reducing the amount of high explosive required.
- Iran has converted 337.2 kg of 20 percent enriched uranium gas (or 227.6 kg of uranium) into oxide form, producing 162.3 kg of uranium, some of which has been used to produce fuel for the Tehran Research Reactor. If it is not irradiated in the reactor, this material could be returned to gaseous form and enriched to weapon grade. However, it would not be sufficient to fuel more than one nuclear weapon and it is unclear how long it would take to convert and further enrich the material.
- Uncertainties about the number of centrifuges that Iran is operating make it difficult to draw a conclusion about the performance of individual machines. An increase or decrease in the production rate could be attributed to the fact that more machines were operating when IAEA inspectors were not present at the plant, rather than because the machines were operating more efficiently. [r] A change in production rate could also be attributed to a decision by Iran to lower the output of its centrifuges.[s]
- Following start-up, centrifuge cascades must be operated for a time without product withdrawal. This process is called passivation.

▶ **Read the notes and more details at source's URL.**

Here's what would really happen if the US bombed Iran

Updated by Zack Beauchamp on April 14, 2015

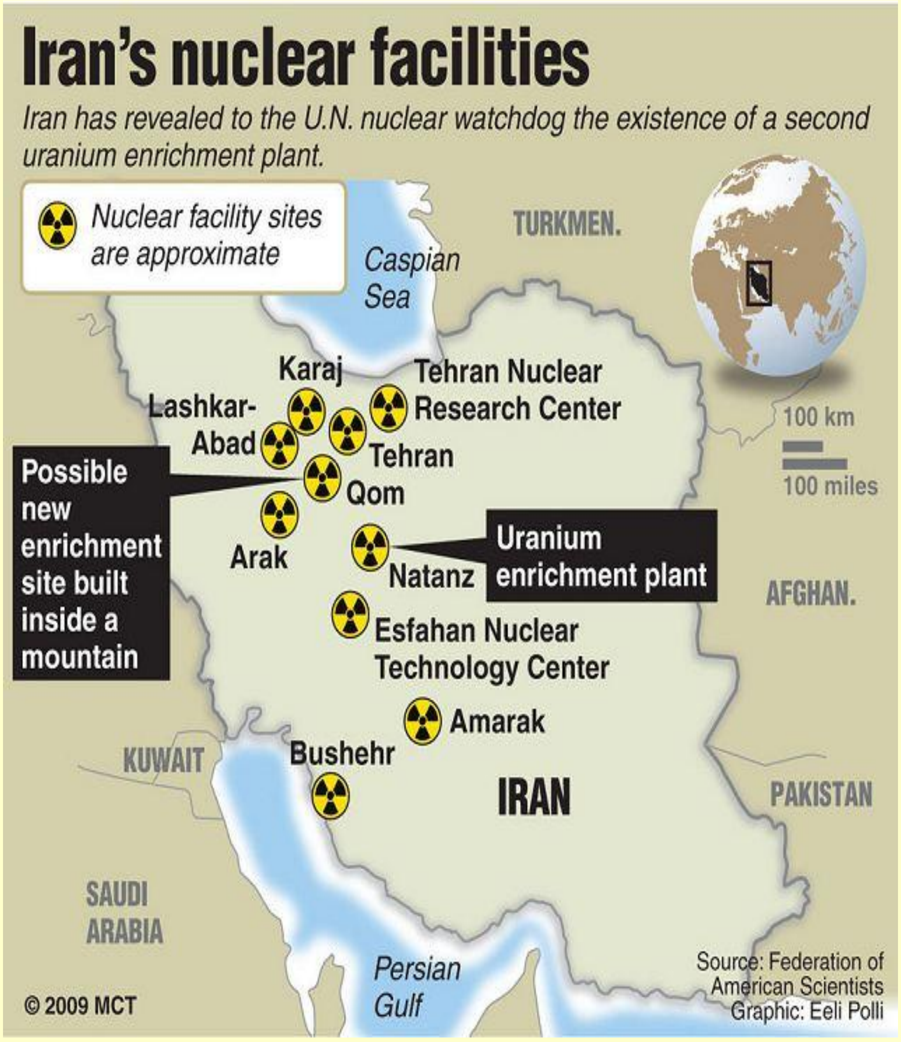
Source: http://www.vox.com/2015/4/14/8389515/iran-war

Last week, Republican Senator Tom Cotton criticized President Obama's nuclear deal framework with Iran, saying Obama was refusing to admit that airstrikes against Iran's nuclear facilities would only take "several days" and wouldn't require any longer-term military commitment to be effective. Obama, he said, was offering a "false choice" between the deal and war.

A number of influential foreign policy analysts, particularly at some of the more hawkish conservative institutions in DC, have openly endorsed military action as the best possible way to prevent Iran from getting a bomb. And while Cotton is notably more hawkish than most politicians, few of whom openly support a strike on Iran's nuclear facilities now, many have suggested that airstrikes or even war should be on the table if talks fail.

Advocates of bombing Iran sincerely believe it's the best possible option for dealing with a bad situation. And the position isn't totally crazy: if the Iranians are dead-set on getting a bomb, it'll be hard to stop them peacefully. A nuclear-armed Iran would be a major threat to the Middle East, and the US military is easily capable of overpowering Iran's armed forces in a straight fight.

But attacking Iran would end in disaster. Surgical strikes would only set Iran's nuclear program back temporarily; destroying the country's nuclear capacity entirely would require outright war. That would kill thousands of people, destroy whatever vestiges of political stability remain in the Middle East, potentially wreak havoc on the global economy, and — barring a total, Iraq-style military occupation of the country — fail to permanently end Iran's nuclear program.


Iran's nuclear facilities
Iran has revealed to the U.N. nuclear watchdog the existence of a second uranium enrichment plant.
Nuclear facility sites are approximate
TURKMEN.
Caspian Sea
Karaj
Tehran Nuclear Research Center
Lashkar-Abad
Tehran
Qom
Possible new enrichment site built inside a mountain
Arak
Natanz
Uranium enrichment plant
Esfahan Nuclear Technology Center
Amarak
Bushehr
IRAN
KUWAIT
SAUDI ARABIA
AFGHAN.
PAKISTAN
100 km
100 miles
Persian Gulf
© 2009 MCT
Source: Federation of American Scientists
Graphic: Eeli Polli

Why many Iran hawks believe airstrikes are the only way

In a certain sense, the case for attacking Iran is very similar to the case for making a deal with Iran. Both sides agree that a nuclear-armed Iran would be dangerous. Both argue, correctly, that simply continuing to put economic pressure on Iran and hoping it will give up its nuclear ambitions won't be enough to stop Iran's nuclear program.

Advocates of military action differ from Obama in their assessment of the Iranian regime. They believe the Iranian government is unshakably attached to its nuclear weapons program and will never abandon it willingly. Therefore, the only way to keep Iran from getting a bomb is to destroy its nuclear facilities.

In this view, Iran's leaders will never abandon their quest for nuclear weapons because nukes are essential to the revolutionary anti-Western foreign policy Iran has pursued in the Middle East.

"The Iranian regime will not abandon its 30-year project," Reuel Marc Gerecht, a senior fellow at the Foundation for the Defense of Democracies, writes. "So the U.S. will face an unavoidable choice: accept a nuclear Iran or launch a pre-emptive military strike." Since the former is unacceptable, they say, the latter is the best option.

Generally, advocates of military action against Iran propose a limited air campaign targeted at the heart of Iran's nuclear program (a few suggest an even more ambitious campaign aimed at total regime change). "An attack need not destroy all of Iran’s nuclear infrastructure, but by breaking key links in the nuclear-fuel cycle, it could set back its program," former US Ambassador to the UN John Bolton writes.

Under this theory, the key targets would be the nuclear facilities at Fordow, Natanz, and Arak (the uranium conversion facility at Isfahan is also often referenced). Some of these, Fordow particularly, are fortified, but the US has bunker-buster bombs that are capable of doing real damage to them.

Strike advocates aren't blind to the fact that Iran could simply rebuild these facilities after any bombing campaign ended. Rather, they argue, it would be *really hard* for Iran to do that anytime in the near future, or Iran would simply give up on its quest for a bomb after being targeted by US airstrikes.

In fact, airstrikes would not be simple, effective, or quick

In fact, even "limited" strikes would be a massive military operation. Destroying the big enrichment facilities wouldn't cripple Iran's program, and the critical targets would be hard to find. Even if everything went perfectly, the strikes would delay Iran by perhaps four years at best — unless the US committed to open-ended war.

The first issue is that the US would need to destroy Iran's air defenses, including fighters and surface-to-air missiles, in order to ensure the bombs hit their targets and to prevent Iran from doing serious damage in response. According to Robert Farley, a professor at the University of Kentucky and expert on air power, this "would involve long-range bombers, drones, electronic warfare, land-based fighter bombers, carrier aircraft, and submarine-launched cruise missiles."

Even the strikes against the nuclear program would need to hit a broad range of targets. Contrary to hawkish assumptions, the strikes couldn't be limited to Iran's big nuclear production facilities. The real problem, according a Rand Corporation brief by Robert J. Reardon, would be Iran's centrifuge production facilities. Simply destroying Iranian enrichment plants would not be enough to end the nuclear weapons program if Iran could just build centrifuges for new ones quickly.

But in order to destroy the centrifuge production facilities, the US would have to find them — which would likely prove difficult. "These facilities are not under IAEA [International Atomic Energy Agency] safeguards, and identifying and locating them would require good intelligence and involve significant uncertainty. Sites that have been identified, or ones that were known in the past, have typically been small, easily concealed from reconnaissance satellites, and located in densely populated urban areas," Reardon writes. "Failure to destroy these sites would allow the Iranians to rebuild their enrichment program, because the machines could be manufactured relatively quickly."

If the first round of strikes didn't destroy every target, the US might need to return again and again. It would require the US to "continue a sustained campaign over a period of time and re-strike after an initial battle damage assessment [if] it is found that further strike sorties are required," defense analysts Anthony Cordesman and Abdullah Toukan write in a comprehensive 2012 CSIS report.

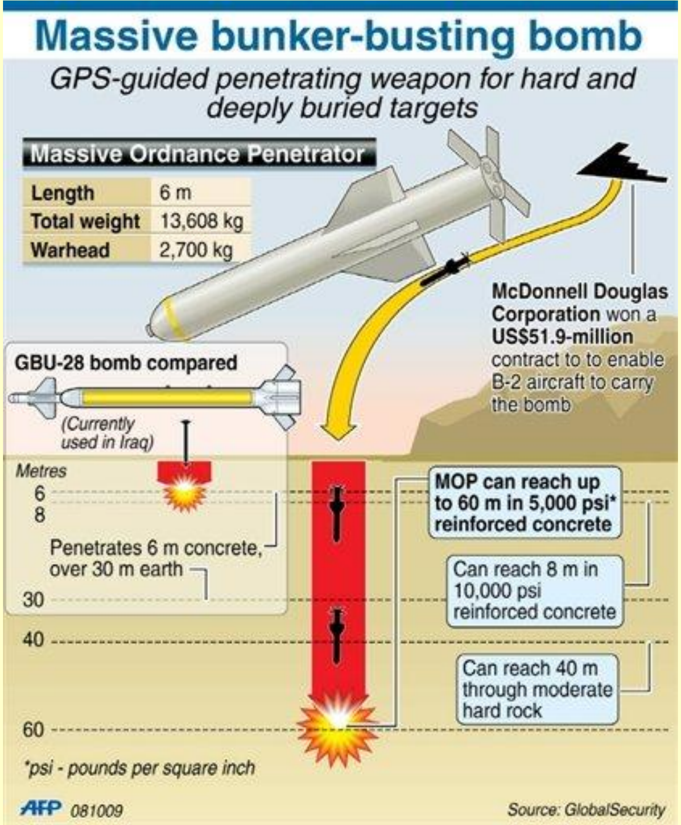
And even that probably wouldn't get it all. "Depending on the forces allocated and duration of air strikes, it is unlikely that an air campaign alone could alone terminate Iran’s program," Cordesman and Toukan argue.

They're not alone in that conclusion. A blue-ribbon panel at the Wilson Center, after reviewing the military studies on the issue, concluded that even if extended military strikes were carried out "to near perfection," the best case scenario is still only a four-year delay in Iran's progress toward a nuclear weapon.

Ultimately, the only way military force could stop Iran from going nuclear is if the US committed to a more or less indefinite war. "To fulfill the stated objective of ensuring that Iran never acquires a nuclear bomb," the Wilson Center report finds, "the U.S. would need to conduct a significantly expanded air and sea war over a prolonged period of time, likely several years."

The consequences would be disastrous

Even limited strikes against Iran would have the potential to spark a broader conflict. The consequences of that, especially in today's Middle East, would be disastrous. Iran has the power to make an unstable Middle East even worse: it could directly target and kill Americans in the region, exacerbate a number of the region's festering conflicts, and potentially threaten the global oil supply — and thus the global economy.


Massive bunker-busting bomb
GPS-guided penetrating weapon for hard and deeply buried targets
Massive Ordnance Penetrator
Length 6 m
Total weight 13,608 kg
Warhead 2,700 kg
McDonnell Douglas Corporation won a US$51.9-million contract to to enable B-2 aircraft to carry the bomb
GBU-28 bomb compared
(Currently used in Iraq)
Metres
6
8
30
40
60
Penetrates 6 m concrete, over 30 m earth
MOP can reach up to 60 m in 5,000 psi* reinforced concrete
Can reach 8 m in 10,000 psi reinforced concrete
Can reach 40 m through moderate hard rock
*psi - pounds per square inch
AFP 081009
Source: GlobalSecurity

US military leadership has worried; Politico's Michael Crowley reports that if talks fell apart then Iranian proxy militias could decide to attack American troops in Iraq. It's difficult to imagine Iran staying its hand in the event of an outright US attack. While the US is particularly exposed in Iraq, it has people and assets across much of the region; Iran, too, has proxies across the Middle East.

Iran could also attack oil infrastructure or blockade the Straits of Hormuz, a critical oil-shipping route, which would have tremendous effects.

"Iran can use a mix of mines, submarines, submersibles, drones, anti-ship missiles, small craft, and assault forces anywhere in the Gulf region to threaten the flow of oil exports," Cordesman and Toukan write. "Any major disruption affects the entire economy of Asia and all world oil prices — regardless of where oil is produced. It can lead to panic and hoarding on a global basis."

If the US strikes Iran, the anti-Iran coalition will collapse

Airstrikes could destroy what has been a key constraint on Iran's nuclear program: the system of international inspections and sanctions that are currently in place.

European and particularly Asian countries have given the US strategy much of its force by helping to isolate and sanction Iran; that is what compelled Iran to negotiate and agree to make concessions in the first place. If the US attacked Iran, the international community would surely be appalled and abandon its support for sanctioning and isolating Iran, leaving the country wealthier and in a stronger diplomatic position. And that's just the start.

"U.S. relations with Russia have gone sufficiently south, and the U.S. attack against Iran itself would be sufficiently destabilizing, that we can almost surely expect Russia to militarily support Iran in the form of aircraft and air defense systems," Farley writes.

"Moreover, if Russia opens up the Iranian defense market, we can expect China to follow. The sanctions regime cannot survive a U.S. attack on Iran."

That would cripple any serious attempt to prevent Iran from rebuilding its nuclear program. "To prevent Iran from reconstituting its nuclear program after a strike, the United States would have to be prepared to encircle an even more hostile adversary with a costly containment regime — much like the 12-year effort to bottle up Saddam Hussein after the 1991 Gulf War — and be prepared to re-attack at a moment's notice," Georgetown University's Colin Kahl told Congress in 2012 testimony.

"In the absence of clear evidence that Iran was dashing for a bomb," Kahl testified, "a US strike risks shattering international consensus, making postwar containment more difficult to implement. And with inspectors gone, it would be much harder to detect and prevent Iran's clandestine rebuilding efforts."

Striking Iran, then, wouldn't be Tom Cotton's "several-day" endeavor. It wouldn't stop Iran's nuclear program unless the United States committed to more or less permanent war with Iran, if it even did it then. And it would likely have devastating consequences for the US and its allies.

But the hawks do get one thing right: a nuclear-armed or nuclear-threshold Iran also would be very dangerous. The conclusion is pretty obvious: we better hope the deal succeeds.

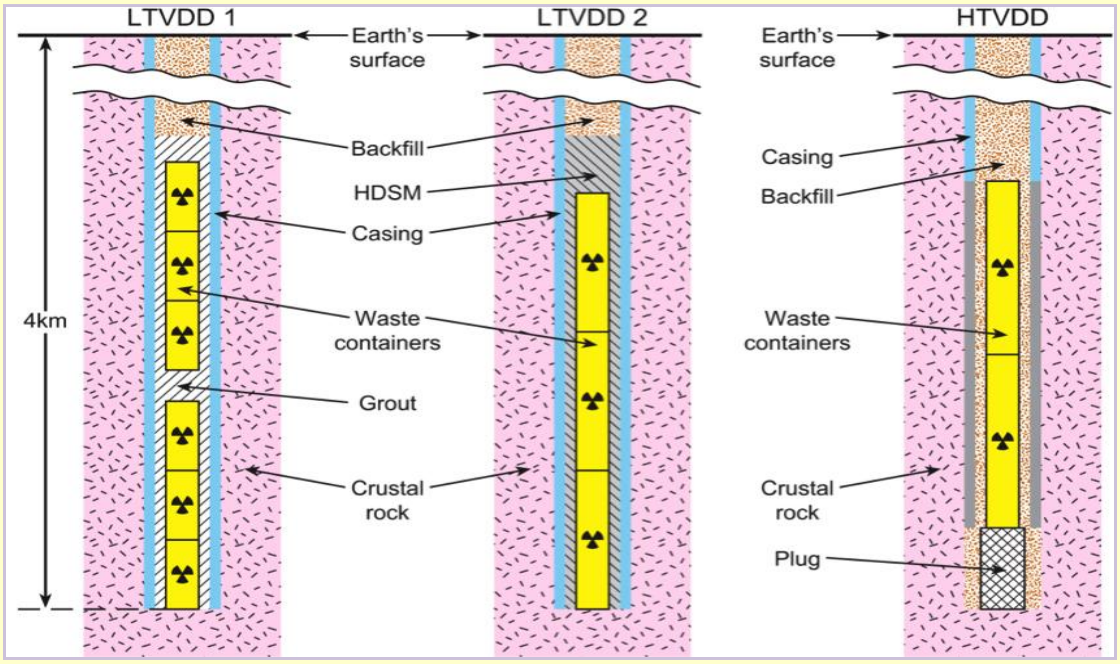
***Zack Beauchamp** writes about all of the things that are not American things. He previously edited a section on political thought at ThinkProgress and, before that, contributed to The Dish. It's pronounced BEE-chum.*

Scientists develop deep borehole disposal (DBD) method to deal with nuclear waste

Source: http://www.homelandsecuritynewswire.com/dr20150416-scientists-develop-deep-borehole-disposal-dbd-method-to-deal-with-nuclear-waste

Technologies which will enable nuclear waste to be sealed five kilometers below the Earth's surface could provide a safer, cheaper and more viable alternative for disposing of the U.K.'s high level nuclear waste.

Scientists at the University of Sheffield calculate that all of the U.K.'s high level nuclear waste from spent fuel reprocessing could be disposed of in just six boreholes five kilometers deep, fitting within a site no larger than a football pitch.



The concept — called deep borehole disposal — has been developed primarily in the United Kingdom, but is likely to see its first field trials in the United States next year. If the trials are successful, the United States hopes to dispose of its "hottest" and most radioactive waste — left over from plutonium production and currently stored at Hanford in Washington State — in a deep borehole.

A University of Sheffield release reports that university researchers are presenting the latest findings relating to these trials and new concepts for sealing the waste into the boreholes at the American Nuclear Society (ANS) conference in Charleston this week (April 13-16 2015).

Professor Fergus Gibb of the University of Sheffield's Faculty of Engineering explained: "Deep borehole disposal is particularly suitable for high level nuclear waste, such as spent fuel, where high levels of radioactivity and heat make other alternatives very difficult. Much of the drilling expertise and equipment to create the boreholes already exists in the oil and gas and geothermal industries. A demonstration borehole – such as is planned in the US – is what is now needed to move this technology forward."

At the ANS conference, Professor Gibb, with co-researcher Dr. Karl Travis, presented modeling work carried out by the University of Sheffield team on the Hanford waste, which confirms that around 40 percent of the waste, in terms of radioactivity, currently stored at the U.S. site could be disposed of in a single borehole.

Fundamental to the success of deep borehole disposal is the ability to seal the hole completely to prevent radionuclides getting back up to the surface. Professor Gibb has designed a method to do this, which he presented at the conference: to melt a layer of granite over the waste, which will re-solidify to have the same properties as natural rock.

Professor Gibb's colleague at the University of Sheffield, Dr. Nick Collier, proposed a method of fixing and surrounding the waste within the borehole by using specialist cements able to handle the temperatures and pressures at that depth.

Deep borehole disposal (DBD) has a number of advantages over the current solution envisaged for all U.K. nuclear waste, which is in a mined repository at 500 meter depth: DBD is effectively "pay-as-you-go" disposal. A mined repository can cost from hundreds of millions to tens of billions of dollars to construct before any waste can be disposed of; DBD costs a few tens of millions of dollars per borehole.

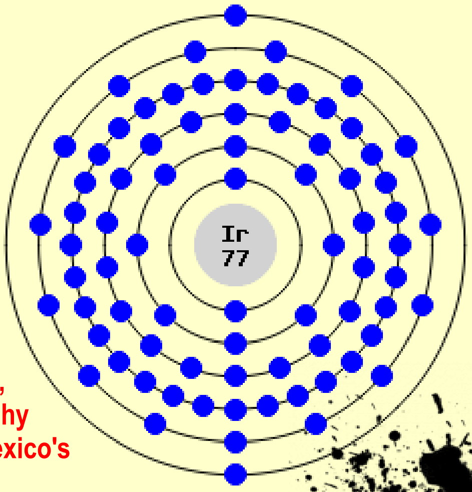
There are more geological sites suitable for DBD, as the granite layer which is required can be found at appropriate depths under most of the continental crust.

- A borehole could be drilled, filled, and sealed in less than five years, compared to the current timescale for a U.K. mined repository, which is to open in 2040 and take its first waste by 2075 (although a site has not yet been agreed).
- As DBD disposes of nuclear waste at greater depths and with greater safety, and because there are more potential sites available, it should be easier to obtain public and political acceptance of the technology.
- DBD has limited environmental impact and does not require a huge site: the holes are a maximum 0.6 meter in diameter and can be positioned just a few tens of meters apart. Once a borehole is complete, all physical infrastructures on the surface can be removed.
- While seismic activity might damage the containers within the borehole, fracture the surrounding rock and disrupt some of the nearest barriers in the borehole, it would still not destroy the isolation of the waste or make it possible for radioactivity to reach the surface or any ground water.

The demonstration borehole in the United States will be drilled just under half a meter in diameter and trials will be conducted to ensure waste packages can be inserted into the borehole and recovered if required. Initial results are expected in 2016. If these results are positive, disposal of the Hanford waste capsules would then take place in another borehole, just 0.22 meter in diameter.

Radioactive material stolen in Mexico

Source: http://www.cbsnews.com/news/mexico-on-alert-after-radioactive-iridium-192-stolen-from-truck-in-tabasco-state/



Apr 16 – **The Mexican government has put civil protection agencies in five southern states and some federal agencies on alert following the theft of radioactive medical material from a vehicle on Monday.**

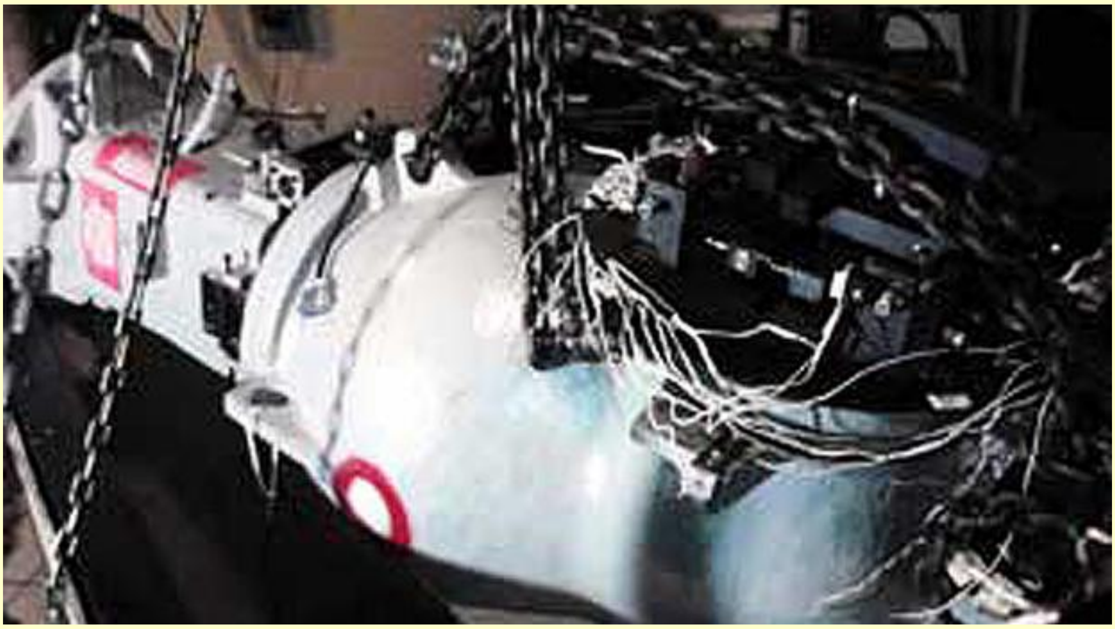
CBS News partner network UNO TV reported the iridium-192, a radioactive compound used in mobile medical radiography work, was stolen from a vehicle in Tabasco state, near Mexico's border with Guatemala.

According to the report, the material is classified as Category 2 under the international nuclear watchdog's (IAEA) rating scale. While the iridium-192 was safely encased when stolen, UNO TV said a Category 2 material could cause serious lesions or even death within a day of exposure if removed from its protective casing.

The alert issued to authorities included the states of Tabasco, Campeche, Chiapas, Oaxaca and Veracruz.

According to UNO TV, the alert called on any local authorities who were to locate the radioactive material not to try and handle it, but rather to establish a secure perimeter around it of approximately 90 feet, and report it to federal officials.

This week's incident was at least the second time in recent years that dangerous radioactive material has been stolen from a vehicle in Mexico.



A decommissioned and safely encased cobalt-60 medical teletherapy unit is seen being lowered into a wooden box for transport to radioactive waste facility in Mexico. CNSNS/Handout

In December 2013, thieves made off -- apparently unwittingly -- with a container full of cobalt-60, also used in medical equipment, from a vehicle transporting it for safe disposal.

The cobalt, which is a Category 1 source under the IAEA's ranking system and thus more dangerous than the iridium stolen this week, was found in a field abandoned by thieves days later. Several people were treated for radiation exposure after its discovery.

There was no indication as of Thursday morning that the thieves behind the iridium's disappearance in Tabasco were anything other than misguided bandits, as turned out to be the case in 2013, but it will again pique the interest of security forces that worry about criminal and terrorist groups trying to obtain such materials.

In an article posted on the Bulletin of the Atomic Scientists after the 2013 theft was resolved, two nuclear experts -- one of whom is a former IAEA employee -- wrote that medical sources of radioactivity like cobalt are more dangerous to those who handle them in their undiluted form than they would be "if spread using a radiological dispersal device such as a so-called 'dirty bomb.' Nonetheless, had the Mexican source been used in a dispersal device, the economic consequences could have been extremely significant."

The scientists urged greater accountability by national authorities in reporting to the IAEA incidents of theft like the ones in Mexico. They also suggested establishing global standards for the transport and handling of radioactive medical materials, saying it "would be an important step toward enhancing the global nuclear security regime," but admitting it was a tall order, "given the difficulty of negotiating and implementing binding international instruments."

Nuclear risksIn South Africa, bomber of apartheid era nuclear power plant is a hero, not a terrorist

Source: http://www.homelandsecuritynewswire.com/dr20150420-in-south-africa-bomber-of-apartheid-era-nuclear-power-plant-is-a-hero-not-a-terrorist

Apr 20 – **In December 1982, Rodney Wilkinson planted four bombs that caused $519 million in damages at the Koeberg nuclear power plant north of Cape Town, South Africa. The attack, which many believe to be the most ambitious and successful terror attack against a nuclear facility,** remains a symbol of African National Concress (ANC) triumph against South Africa's then-apartheid government.

The 1982 Koeberg assault, however, and a 2007 raid by two yet-to-be-identified armed groups on South Africa's Pelindaba nuclear research site, are at the root of U.S. concerns about the safety of South Africa's roughly 485 pounds stockpile of highly-enriched uranium.

The Obama administration says that security at South Africa's nuclear facilities, where the cou8ntry's nuclear material is held, is lax, leaving the bomb-grade materials vulnerable to thieves and terrorists. South Africa president Jacob Zuma has insisted that the threat of nuclear terror is overplayed.

Wilkinson, a white South African, was a collegiate fencing champion whose hopes of competing in the Olympic Games in the 1970s were dashed by international sanctions against the South African government. After dropping out of college and serving briefly with the South African military in Angola, Wilkinson joined a commune near the construction site of the Koeberg nuclear power station. When he ran out of cash, he landed a job as a laborer, helping build the twin-reactor plant.

Supporters of the anti-apartheid movement and the ANC saw Koeberg as a symbol of a racist regime's nuclear ambitions, and therefore a legitimate target for ANC saboteurs. Wilkinson became an active supporter of the ANC after he was inspired by the 1979 arrest of Renfrew Christie, an ANC figure with a doctorate from Oxford who spent seven years in prison for spying on South Africa's nuclear program.

After working at Koeberg for a few months, Wilkinson managed to get his hands on a copy of the facility's blueprints. He traveled to neighboring Zimbabwe and handed the copy to Sathyandranath "Mac" Maharaj, who was convicted in 1964 of more than fifty acts of sabotage against the apartheid government. After serving twelve years in prison, Maharaj became a senior ANC official in exile.

Upon verifying that the blueprints were authentic, Maharaj, who is now the official spokesman for South African president Jacob Zuma, suggested Wilkinson plant bombs at the facility before it was loaded with radioactive fuel. "The purpose was to make a political statement and to cause as much damage as possible," Wilkinson said in an interview with the Center for Public Integrity. "We didn't want to hurt anybody, and I completely didn't want to get killed."

Wilkinson took on the challenge, and through a series of maneuvers, which included getting a job that allowed him access to the facility's most sensitive areas, he planted the last of four Soviet-made limpet mines on 17 December 1982 and set the timers to go off a day later. Wilkinson had announced months earlier that he would quit his job on that day, so when the explosion occurred, he was not considered a suspect. The ANC claimed credit for the attack, which caused no injuries, and Wilkinson was never caught or identified as a suspect.

"It was because I was white," he said. Years later, Wilkinson told his story to the South African *Mail and Guardian* newspaper, and was granted amnesty by South Africa's Truth and Reconciliation Commission in 1999.

The *Washington Post* quotes Gabrielle Hecht, a University of Michigan historian who published *Being Nuclear: Africans and the Global Uranium Trade* in 2012, as saying that the aphorism that one person's terrorist is another person's freedom fighter is relevant to the longstanding disagreement between Washington and Pretoria. The difference in perspective, she said, makes nuclear security a lower priority for South Africa than the prospect of establishing energy and economic security from nuclear power. "It's utterly unsurprising that the two nations would not be seeing eye to eye" on the threat of nuclear-related terror, Hecht said.

Illegal Iranian Procurement Network Exposed

Source: http://www.iranwatch.org/our-publications/nuclear-iran-weekly/illegal-iranian-procurement-network-exposed

Apr 21 – **The US Justice Department has charged four companies and five individuals for participating in an international network that illegally procured $24 million in controlled goods for the Iranian military and for nuclear end-users.** According to a 24-count federal indictment unsealed on April 17, the procurement network conspired to export sensitive American-made electronic components with military applications to Iran via companies in Taiwan and Turkey, in violation of U.S. law. The network allegedly began operating in July 2010 and was still active at the time of the indictment. Its exposure raises the question of how ongoing illegal procurement by Iran will be handled as part of a final nuclear agreement.

The alleged ringleader of the operation was Bahram Mechanic, a 69-year-old resident of Houston, Texas. Mechanic is the majority owner of Faratel Co. in Tehran and sister company Smart Power Systems (SPS) in Houston. Faratel and SPS design and manufacture uninterrupted power supplies (UPS), an electronic component critical for air defense systems, missile systems, and the nuclear energy sector. Faratel's client list included the Iranian Ministry of Defense, the Atomic Energy Organization of Iran, and the Iranian Centrifuge Technology Company (TESA).

The network allegedly procured at least $24 million worth of U.S.-origin microelectronic components, including microcontrollers, digital signal processors, transformers, and ferrite cores, needed for the manufacture of UPSs. Using a shopping list of goods sought by Faratel in Iran, Mechanic directed one of his associates, a Taiwanese businessman named Arthur Shyu, to use his company, **Hosoda Taiwan Ltd.,** to obtain the export-controlled items from sources worldwide. Shyu would then either ship the goods directly to Iran or through a “cut out” in Turkey, a shipping company named **Golsad Istanbul Trading Ltd**. **Between July 2010 and the time of the arrests, Faratel received at least 250 shipments in Iran totaling 28 million parts.**

According to the indictment, Mechanic was previously investigated by U.S. enforcement authorities for illegal trade with Iran, resulting in one criminal conviction and one civil action. Mechanic then used his knowledge of U.S. restrictions “to devise a sophisticated transnational network of individuals and companies to mask their activities […] and continue to expand his illegal transactions with Iran.”

His experience showed. The network relied on well-known methods to get around U.S. export control law and international sanctions, including: transshipment through third countries to mask the final destination; undervaluing goods; falsifying product codes to remove military designations; mingling export-controlled items with non-controlled items to avoid scrutiny; falsifying shipment statements to remove reference to Iranian ports; modifying and tailoring payments to insure that amounts and bank names would not raise flags; and the use of personal email accounts to discuss how to evade U.S. law.

In all, nine defendants are charged with violating the International Emergency Economic Powers Act (IEEPA). Mechanic and two U.S.-based associates, Tooraj Faridi of Houston and Khosrow Afghani, are in federal custody. Shyu and the operator of the Turkish shipping company, Matin Sadeghi, have outstanding arrest warrants and are believed to be outside of the United States.

Seven foreign nationals and companies were added to the Department of Commerce's Bureau of Industry and Security Entity List. In addition to listing Faratel, Shyu, Hosoda Taiwan Ltd., and Golstad Istanbul Trading, the Commerce Department also designated two managers at Faratel in Tehran -- Arash Servatian and Elaheh Siahpoush -- and Abbas Goldoozan, a company official at Golstad Istanbul Trading.

This Iranian-based network operated during nuclear talks with the United States, in violation of U.S. export control laws and despite international sanctions against Iran. This raises the question of how illicit procurement will be treated if a nuclear agreement is reached between Iran and the P5+1 countries.

According to the Obama administration's “fact sheet” on the framework agreement, a dedicated procurement channel will be established for Iran’s nuclear program “to monitor and approve, on a case by case basis, the supply, sale, or transfer to Iran of certain nuclear-related and dual-use materials and technology.” **But many questions persist.** How will violations of procurement channel restrictions be handled? Will the channel cover only items destined for Iran’s nuclear program? How will procurement of dual-use items for other sectors be monitored? As in this case, Iran’s civilian industries could act as procurement agents for illicit government activity. They provide additional avenues for evading sanctions on missile and other military technology. These critical questions must be resolved by the June 30 deadline.

Drug cartels, terrorists may cooperate in smuggling materials for a nuclear device into U.S.

Source: http://www.homelandsecuritynewswire.com/dr20150421-drug-cartels-terrorists-may-cooperate-in-smuggling-materials-for-a-nuclear-device-into-u-s

Detonating a nuclear device or dirty bomb in the United States has long been goal of terrorists groups including al-Qaeda. Doing so, however, would require access to nuclear materials and a way to smuggle them into the country.

For now, considerable roadblocks exists that would prevent such a plan from coming into fruition, but Steven Sin, a senior researcher in the unconventional weapons and technology division of the National Consortium for the Study of Terrorism and Response to Terrorism (START), says that what seems like a plot in a spy thriller could become a real-life nightmare scenario.

According to the Nuclear Regulatory Commission (NRC), a radiological device, or dirty bomb, is a conventional explosive with radioactive materials such as Cesium 137 attached. A nuclear device, now limited to a few nation states, involves splitting the atoms of a radioactive material such as highly enriched uranium.

The *Tampa Tribune* reports that last week, Sin released a study about the nexus between drug organizations, crime groups, and violent extremists and the trafficking of radiological and nuclear materials. In it he points out that **al-Qaeda, Hezbollah, and Fuerzas Armadas Revolucionarias de Colombia (FARC) are the three organizations with the motivation and capability to obtain a radiological or nuclear device**. These groups, Sin explains, are hybrid organizations, a meld between the ideological and criminal, driven primarily by ideology and using crime to fund their ideological actions.

Of the three groups, only al-Qaeda and Hezbollah would be likely to use such a device in the United States. FARC makes a bulk of its money selling cocaine to users in the United States, and would not want to unleash a radioactive bomb on its best customers.

Still, Sin explains that while a drug trafficking organization may make too much money from the United States to want to help unleash chaos and disrupt business, a rogue high-ranking member of a drug trafficking group may use his or her position and the respective organization's capability to smuggle radiological or nuclear devices into the United States on behalf of a terror group.

Should al-Qaeda or Hezbollah find a way to smuggle a radiological or nuclear weapon into the United States, the group would still have to get its hands on the device or nuclear material. The technical complexities, and its limits to a few nation states, make it unlikely that terrorist groups would obtain a nuclear weapon. **Radioactive materials, on the other hand, which are useful for a dirty bomb, could be obtained from MRI and X-Ray scanners, but recent cases show that the quest still remains a challenge for terror groups.** According to the NRC, "Since September 11, 2001, terrorist arrests and prosecutions overseas have revealed that individuals associated with al-Qaeda planned to acquire materials for a (dirty bomb) or radiological dispersal device (RDD)."

In 2004 British authorities arrested Dhiren Barot and seven associates on various charges, including conspiring to commit public nuisance by the use of radioactive materials. Barot admitted to plotting to bomb the New York Stock Exchange, the International Monetary Fund headquarters, and the World Bank, among other targets. **In another 2004 case**, British police arrested British national Salahuddin Amin and six associates on terrorism-related charges. According to the NRC, al-Qaeda linked-Amin "is accused of making inquiries about buying a 'radioisotope bomb' from the Russian mafia in Belgium."

Neither Barot nor Amin's plans came close to an operational stage, but they demonstrate "the continued interest of terrorists in acquiring and using radioactive material for malicious purposes," the NRC points out.

Radioactive Drone Lands On Japanese PM's Roof

Source: http://news.sky.com/story/1469873/radioactive-drone-lands-on-japanese-pms-roof

Apr 22 – A drone carrying a "small quantity" of radiation has landed on the roof of Japanese Prime Minister's office in Tokyo.

It was spotted by an official taking new employees on a tour of Shinzo Abe's rooms - he was away at the time in Indonesia at an Asia-Africa summit.

The drone was quickly covered with tarpaulin

The aircraft was carrying a small camera, water bottle and flare and was marked with a radioactive sign, according to media reports.

Aerial footage showed it covered by cardboard and later by a blue tarpaulin.

It was subsequently carried away by police and later tested positive for small amounts of radiation, Kyodo news said, quoting police sources who claimed the radiation was so low it was not harmful to humans.

A government spokesman said the country might need to consider regulating the devices - at present there are no restrictions over unmanned equipment flying at 250m (820ft) above ground, except for flight routes.

"This situation concerns the centre of Japanese government, the prime minister's office, and we will take every necessary step, including a detailed investigation by police," he said, adding that Japan had begun studying the matter after a drone landed in the White House grounds in January.

It is not known who sent the drone or why but it comes after a group of Japanese citizens failed in a legal attempt to halt the restart on a nuclear power plant in the southwest of the country.

A court discarded their concerns about the safety of nuclear power since the Fukushima radiation disaster in 2011.

Small drones are becoming increasingly popular in Japan and being used for performances, aerial filming and other events.

Meanwhile, at the Asia-Africa summit Mr Abe expressed "deep remorse" for Japan's part in World War Two.

He did not go as far as former Japanese PMs in making a full apology but reports suggest there was a thaw in relations with China, with Mr Abe and Chinese President Xi Jingping shaking hands at the start of the meeting and planning a possible one-to-one meeting later.

The Hidden Enemy In Iraq

By Mike Giglio

Source: http://www.buzzfeed.com/mikegiglio/the-hidden-enemy-in-iraq#.owQwoWDlV

Soldiers strapped on their helmets as Col. Mohammad and his bomb-disposal team pushed closer in an armed convoy toward the front, through villages newly freed from ISIS control. The ethnic Kurdish forces working to roll ISIS back in northern Iraq relied on specialists like Mohammad to cut through the web of explosives the militants left behind. They snipped wires in booby-trapped homes, found and detonated roadside bombs, and regularly lost their lives.

When the team reached the battered village of Mullah Abdullah, outside the city of Kirkuk, they found a sedan packed with explosives. Soldiers watched warily as Mohammad approached, then stepped back as a specialist prodded the car with a rod. ISIS designs bombs to detonate on specialists, who rely on simple tools to survive: metal wire cutters from a hardware store, a laser pointer to scan for tripwire. “There are too many tricks,” Mohammad said. “All we have to count on is our eyes.”

Col. Mohammad shows equipment he bought in a local hardware store to help defuse IEDs. Ayman Oghanna for BuzzFeed News

ISIS is using improvised explosive devices, or IEDs, in staggering numbers across its fronts in Iraq. Experts say the weapon has never been used on this scale before — it is “unprecedented,” says Jonah Leff of the arms-tracking firm Conflict Armament Research, and “a revolution in their use and deployment.”

IEDs were the weapon of choice for Iraqi insurgents during the U.S. occupation — and their use by ISIS now is playing a crucial role as the war against them reaches a pivotal moment in Iraq. While U.S. warplanes pound the militants, they face multipronged assaults from local forces: the Kurds, Iraqi troops, and Iran-backed militia. New offensives countrywide have been billed as preludes to a battle for the northern city of Mosul, the prize of ISIS’s summer onslaught and the Iraqi heart of its self-styled caliphate.

The offensives span from Kirkuk in the north to the edge of Anbar province west of Baghdad and the city of Tikrit, where some 20,000 militia and Iraqi soldiers are engaged in the largest operation against ISIS to date. All have slowed amid the havoc wreaked by IEDs. Fighters from each of the forces battling ISIS say that — like U.S. troops before them — they suffer most of their casualties from the bombs.

In hard-won territory in Kirkuk, Anbar, and Tikrit over the last two weeks, soldiers and specialists scrambled to deal with the IED threat, defusing and detonating what they could or simply stepping over suspicious wires. Their efforts at bomb disposal ranged from the professional to the reckless. Kurdish forces, called *peshmerga*, which are increasingly America’s main ally on the ground, deploy special explosive ordnance disposal (EOD) units whose members work with little training and rudimentary equipment in what the U.S. military treats as a highly specialized field. In Mullah Abdullah, Mohammad’s team destroyed the car bomb safely — they detonated it from afar with a homemade charge, and the blast blew out windows a quarter-mile away — but peshmerga specialists often fall victim to the bombs they're working to neutralize.

The Iraqi government has skilled EOD technicians with experience dating back a decade. But they say they're overwhelmed by the scale of IEDs and the chaos of the myriad battlefields. Some government soldiers have attempted to fill the gap with ad hoc training. The militia, meanwhile, appear to rely on some assistance from Iran as well as inexperienced volunteers whose main qualification is a willingness to sacrifice themselves to the bombs. "The whole country is surrounded now by IEDs, so what do you expect of us?" said Settar al-Khaffaji, a retired Iraqi colonel and official with the militia group Abu Fadhil al-Abbas. "We have to clear them ourselves."

On a recent afternoon, crater after crater lined a road to the front outside Kirkuk as Mohammad and his men prepared to detonate a last IED before the sun set. Pickup trucks full of camouflaged soldiers took care to straddle the median as they passed. The team had dispatched around 45 IEDs that day — inching up to place a small charge on each, then taking cover in an armored vehicle as the blasts pulsed the air, showering dirt onto the asphalt. Across a field from the road, a collapsed house was a reminder of the danger: The previous day an IED had killed four of their colleagues there.

The peshmerga have defused or detonated more than 6,000 IEDs along their 650-mile front with ISIS since the war began in August, Kurdish officials said. Those were the ones they'd been able to find. Mohammad pointed to the fields that stretched to a set of hills on one side of the road and the village with the flattened home on the other. "To be honest, we believe that those open fields beneath the hills, and the hills, are filled with IEDs. All those houses are full of IEDs," he said.

"This is a hidden enemy," said a 46-year-old lieutenant in tan fatigues and designer sunglasses, who gave the nickname Abu Akram. "The fighters, you see them on the other side. But I don't know where this enemy is going to attack."

Like most officers working with IEDs, Abu Akram declined to be photographed or use his real name. Mohammad, likewise, requested to withhold his first name. It showed the sensitivity of their work: The specialists worried ISIS would target them to eliminate a crucial source of expertise. Abu Akram said he'd identified 12 main types of IEDs used by ISIS, but the militants kept changing tactics. "When you beat them today, they will think of a way to build an even more sophisticated bomb, so you won't beat them again," he said.

One specialist recounted a U.S. expert calling the EOD teams "insane" when he saw how they worked.

Experts and local soldiers said ISIS employs its IEDs — which can come in the form of suicide attackers, car bombs, roadside bombs, and booby traps — with increasing sophistication. The group's predecessor, al-Qaeda in Iraq, was infamous for its use of the bombs. But ISIS truly stands out in deploying the weapon en masse, in the fashion of landmines, which are banned under international law because they cause indiscriminate carnage both during a conflict and after it ends.

The IEDs that the EOD specialists uncovered were often simple and complex at once. They could be made with basic items like paint, fertilizer, kitchen pots, and jerry cans. They could also have devious designs, like a cell phone the militants called to trigger the bomb when the specialists arrived or a device that detonated it if it moved. The vast territory and resources ISIS controls, meanwhile, appeared to allow it to produce some IEDs on a large scale: Some peshmerga specialists believed there were workshops or factories. One type of IED they found often outside Mosul had containers made from oil pipeline. The thick metal cylinders were cut and welded with precision, with a hole for the fuse drilled on one end. The explosives were packed in so tightly that a captain said it took 30 minutes to spoon them out. He thought the packing had been done by machine, but chemical reactions in the explosive mix could also account for what he described.

The peshmerga specialists working through the lines of IEDs had little training from their Western allies and lacked modern tools like signal jammers, X-rays, and robots. Even their metal wire cutters were a dangerous departure from the norm: Professional EOD technicians use plastic or ceramic ones to avoid short-circuiting the bombs. One specialist recounted a U.S. expert calling the EOD teams "insane" when he saw how they worked. Though officials wouldn't give figures, the peshmerga seemed to lose EOD specialists with most major operations. "When one of our men dies in an explosion, you will be collecting the pieces," said the general who heads the peshmerga's EOD division. "And this is very hard to see."

Michael Knights, an Iraq expert at the Washington Institute for Near East Policy, said ISIS's success in employing an "economy of force" has been surprising. "They have a defensive model," he said. "That model is restless counteroffensive operations that keep the enemy scared and on its back foot combined with the use of massive harassment [IED] minefields. To just instill delay on everything. To make every single task the coalition has to do one and a half times as hard. And that's been very effective."

IEDs would play a crucial role in any battle for Mosul, which U.S. and Iraqi officials have said will begin this year. "These are the world-class leaders in IEDs," said Christopher Harmer, an analyst at the Institute for the Study of War. "The U.S. was barely able to deal with this. If these forces are seriously considering moving into Mosul, how will they deal with the IED threat?"

Soldiers who push into ISIS territory looking for a fight often find themselves instead facing explosive traps and sniper fire. "There is no confrontation between fighters," complained a fighter with the Badr Brigades, one of the largest in the coalition of Shiite militias that has taken up arms against ISIS, which preaches an extremist version of Sunni Islam. "It's not like a normal war."

The fighter and his colleagues stood along a pockmarked road in a village called Saadan, on the edge of Al-Garma, a district on the outskirts of Anbar province where Iraqi forces and Shiite militia launched an offensive against ISIS this month. They'd won the village the previous week; it was a mess of battered buildings and decapitated palm trees. Some of the IEDs that had covered the area remained. "Don't ever step on the other side of this road," a fighter said.

A dirt path off the road led to graves where ISIS had buried some of its dead.

The militiamen had fired on the area for days with mortars and machine guns, but by the time they arrived, most of the ISIS militants were gone. They left hoses and copper wire strewn about the path; some were attached to nothing and others the fighters took care to step around. A green set of Shiite prayer beads sat atop a pile of dirt, as if appealing to the religious-minded fighters to pick it up. "That is probably an IED," one of them said.

Gen. Qasim Attiya of the Baghdad Operations Command, which is helping to run the war effort in the area, said government and militia forces had won about five miles of Al-Garma in 10 days of fighting and uncovered hundreds of IEDs in the process. "We told our soldiers not to enter the houses, because most of them are targeted," he said. "Our engineers are working day and night to remove IEDs."

The scale of the IED threat leaves much of the disposal work to be handled by amateurs.

The Badr fighters said they had their own teams to deal with IEDs. As they walked through Saadan, explosions sounded in the distance — the specialists at work, they said. But the fighters refused to let the specialists be interviewed. A Badr commander could be overheard explaining the reason to a colleague: "because the experts are from Iran, and they don't want to be seen."

Mohammed Naji Mohammed, a Badr leader in the area, said Iranian specialists had been providing training and guidance on IED disposal, though he didn't say what they were doing in the field. Many of Badr's fighters are new and inexperienced, having answered a call this summer from Iraq's top Shiite religious authority to rise to the country's defense. They needed the assistance, Mohammed said. "Our best bet is to ask Iran for help," he said. "We don't have the experience to deal with all the IEDs in the field, so we have to rely on them."

Fighters from Badr and other militia make up the vast majority of forces in key government offensives — in Tikrit, for example, they number 20,000 compared to just 3,000 troops from the Iraqi military, according to America's top general. The heavy involvement of the militia, plus the presence of Iranian troops and advisers on the front, has led the U.S. military to keep its distance, concentrating its efforts elsewhere.

Iraq's top EOD technicians are based at the interior ministry's vast compound in Baghdad. They put their training and experience to work in the field, but the scale of the IED threat still leaves much of the disposal work to be handled by amateurs.

"Unfortunately the whole place has become a frontline. And we have to work fast," said a lieutenant in the interior ministry's EOD team, who gave only his first name, Samer. "We don't have time to clear everything."

"We are working with a lot of people who don't have experience," he said. "These people don't know how to even walk through the fields. They come to tell us there's an IED, and then they walk right up to it."

Inside the division's headquarters this week, the bell rang at regular intervals, sending teams out to address suspected IEDs around the city, which remain a constant problem. Col. Riyad al-Musawi, the division's manager, said his teams across Iraq were overwhelmed. He criticized the U.S. for not doing more to help, saying he relied on tools like robots the U.S. had donated a decade ago, and that much of it was falling apart. "It's not just people. I don't have enough equipment," he said. He had hosted some EOD workshops for Shiite militia to fill the gaps, he added, "but it's not enough."

"I've been in the field so long and still can't consider myself an expert. These people have been coming to the field in just the last year," Musawi said. "We are familiar with the idea of IEDs. But the difference is the number and the quality and the amount of explosives they pack into each. It gets bigger and bigger."

In Tikrit, an EOD specialist seemed to be anyone willing to do the job — and the rash efforts at bomb disposal mirrored the effort against ISIS generally, with the Iraqi government relying on tens of thousands of religiously motivated volunteers as its U.S.-trained and -equipped military continues to fade into irrelevance.

Ahmed Abdul Wahad, 32, was a police officer when the conflict with ISIS began but took a one-week EOD course in Baghdad last fall, "because nobody else would do it," he said, standing in the Tikrit suburb of Al-Alam as residents returned amid bursts of celebratory gunfire. "After that I had to go out in the field to learn."

The road from Baghdad through the city of Samarra and to Tikrit is lined with checkpoints manned by different Shiite militia. At times, the various groups appeared at odds with one another. At one checkpoint, manned by the militia group Hezbollah, which says it has no ties to the Lebanese militant group of the same name, an altercation erupted when a Badr Brigades convoy that included local and international journalists tried to pass. "I don't give a fuck about you," one commander said to another. Hezbollah fighters later fired warning shots and threatened to blow up a news van with a rocket-propelled grenade.

With the militia groups competing for status and influence, even when government EOD teams are available, it might be hard for them to navigate the territorial maze. "Part of the problem is ego and glory," Musawi of the EOD division in Baghdad said.

Fighters in Al-Alam said IEDs were killing their comrades regularly. Sabbah Nadem, from the Iraqi national police, had photos on his phone that showed how ISIS had converted a farm building nearby into an IED workshop — artillery shells lined the floor, waiting to be converted into bombs. Ahmed al-Juburi, 24, was one of the militia fighters who considered himself an expert on handling IEDs. He said he had no formal training and had learned on the job; he was someone other fighters called on when they came upon a booby-trapped home or roadside bomb. "To be honest, if you're talking about real EOD, we have very few people. But a lot of us picked up experience," he said.

"What we had is one expert who taught some groups, and those groups taught other groups," said Raed Allawi, 55, a retired Iraqi general who is now a commander with the Badr Brigades. "The number of IEDs is so high that we all had to step in."

Allawi said the men tried to smell for explosives, and that when they suspected IEDs along a road or in a home, the first response was often to try to detonate them with bullets or grenades. Otherwise the amateur specialists attempted to defuse them. "We have to," Allawi said. "We are in a crisis right now."

The bombs hidden in homes and fields across the country promise to leave a lasting effect. "These are intended to be victim-activated, and there's no way they're going to distinguish between civilians and combatants," said Mark Hiznay, a senior arms researcher at Human Rights Watch.

He said ISIS uses IEDs no differently than factory-made landmines — which littered parts of Iraq after widespread use under the Saddam Hussein regime and required years of intensive effort to clear. "Now it's like going back to square one," he said. "And the result is that you're going to have civilians wandering into these areas and losing lives and limbs."

On an afternoon last week, not far from a frontline southeast of Mosul, a peshmerga captain walked through a field where he and his team had detonated more than 10 IEDs, ducking for cover as shrapnel flew over their heads. The craters were fading as winter turned to spring; the captain said that if there were any IEDs left, they could be harder to find amid the flowers and grass growing everywhere. He thought the area was safe now, but his eyes scanned the ground. "We're still looking," he said.

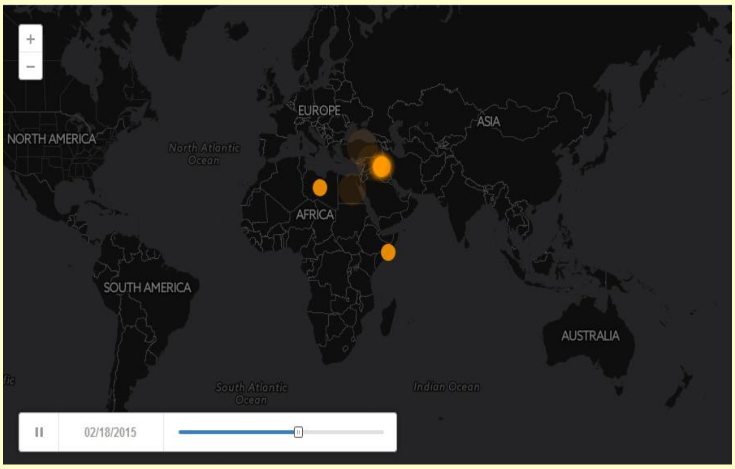
The craters were more recent as he climbed a hill where ISIS had once kept a sandbagged post, laying IEDs around it in all directions. The most recent were two weeks old. When he reached the top, the captain began to move more carefully, surrounded by brush that was newly overgrown. "Maybe just stay on the path," he said.

***Mike Giglio** is a correspondent for BuzzFeed News based in Istanbul. He has reported on the wars in Syria and Ukraine and unrest around the Middle East. With additional reporting by Ayman Oghanna in Iraq.*

VBIED Attacks in 2015

Source: http://intelcenter.com/maps/vbied-incidents-2015-time.html

This animated map shows **151 terrorist and rebel incidents involving VBIEDs in 2015 tracked in the IntelCenter Database (ICD) Incident Component as of 27 Mar. 2015.** The points are on a country level and placed on the center point for each country.



Methodology Note: While IntelCenter makes every attempt to identify all incidents, the nature of reporting makes that nearly impossible. These numbers should be viewed as minimums with the total number likely higher where it could be expected to be so. The original source data for all incidents shown here is located in the Incident Component.

Smell Test Helps Identify TBI in Blast-Injured Soldiers

Source: http://www.medscape.com/viewarticle/842541

Apr 02 – **Testing olfactory function in blast-injured soldiers may help diagnose traumatic brain injury (TBI) on the battlefield,** a new study suggests. Researchers found that olfactory impairment was highly predictive of abnormal neuroimaging findings in blast-injured troops with TBI.

This study shows that quantitative identification olfactometry has "limited sensitivity but high specificity" as a marker for detecting acute structural neuropathology from trauma, the researchers say.

"When considering whether to order advanced neuroimaging, a functional disturbance with central olfactory impairment should be regarded as an important tool to inform the decision process," they write.

The study was published online March 18 in *Neurology*.

The study included 231 soldiers acutely injured from explosions during combat operations in Afghanistan or Iraq and immediately evacuated to Walter Reed National Military Medical Center in Bethesda, Maryland, where they were evaluated for TBI and olfactory function using the University of Pennsylvania Smell Identification Test (UPSIT).

The 136 troops with mild TBI (concussion) and the 55 troops without TBI (blast-injured controls) had normal sense of smell. "More important," say the researchers, all troops with normal neuroimaging findings had normal sense of smell.

Central olfactory impairment was observed only in troops with concurrent acute traumatic radiographic abnormalities, they report. Olfactometric score predicted abnormal neuroimaging significantly better than chance alone (area under the curve, 0.78; 95% confidence interval [CI], 0.70 - 0.87; *P* < .001).

For troops with olfactory impairment, the most common radiographic abnormalities involved injury to the frontal or temporal lobes.

Frontline Test

"Our data are entirely consistent with the historical literature whereby damage to the brain, whether from trauma, stroke, or through neurodegenerative processes (eg, Alzheimer's disease, multiple sclerosis, et cetera) have been demonstrated to significantly impair memory and thereby the ability of the brain to correctly match-up and link common inhalational odorant molecules to past learning and experience," lead author **Michael Xydakis, MD**, US Air Force Colonel, Uniformed Services University of the Health Sciences, told *Medscape Medical News*. "This study is the first to investigate olfactory impairment in combat casualties during the acute and subacute phase of injury," added Dr Xydakis.

He said research is being conducted throughout the military health system on detection, diagnosis, and surveillance of mild TBI and on which blast-exposed troops require immediate neuroimaging. "Despite advances in radiology and the arduous search for confirmatory neuro-diagnostics, the diagnosis of a mild TBI (concussion) remains clinical and is entirely dependent on each individual caregiver's depth of knowledge and breadth of experience in neurotraumatology," Dr Xydakis said.

Olfactory function may serve as a "frontline test" to alert providers to the need for neuroimaging in blast-injured troops, he said. "Currently the indications for neuroimaging remain ill-defined and highly subjective. Since there is no way to know who needs to be scanned, essentially everyone is scanned. We conclude that when considering whether to order advanced neuroimaging, a functional disturbance with central olfactory impairment should be regarded as an important tool to inform the decision process."

Reached for comment, Douglas H. Smith, MD, director, Penn Center for Brain Injury and Repair and professor of neurosurgery, University of Pennsylvania, Philadelphia, told *Medscape Medical News* that very little is known about blast TBI. One problem, he said, is that in studies of blast injury and TBI, almost all participants have had head contact, so it's hard to differentiate the "blast" TBI from civilian TBI.

"There is a high need for a rapid screening test to diagnosis TBI and there are a lot of emerging olfaction tests. Since olfactory difficulties are so commonly associated with damage to the brain it is kind of a surrogate marker. It could help determine who should be removed from battle or training," Dr Smith said.

"Current olfactory testing is not widely used, but it's certainly well known that this could be a useful tool to identify individuals with subtle brain injury like concussion all the way up to more severe TBI. It can also be used for Parkinson's and other neurodegenerative diseases," Dr Smith added.

The study was funded by the US Department of Defense Combat Casualty Care Medical Research and Development Program. The authors have disclosed no relevant financial relationships.

***Neurology*. Published online March 18, 2015.**

Abstract

Objective: To determine whether a structured and quantitative assessment of differential olfactory performance—recognized between a blast-injured traumatic brain injury (TBI) group and a demographically comparable blast-injured control group—can serve as a reliable antecedent marker for preclinical detection of intracranial neurotrauma.

Methods: We prospectively and consecutively enrolled 231 polytrauma inpatients, acutely injured from explosions during combat operations in either Afghanistan or Iraq and requiring immediate stateside evacuation and sequential admission to our tertiary care medical center over a 2½-year period. This study correlates olfactometric scores with both contemporaneous neuroimaging findings as well as the clinical diagnosis of TBI, tabulates population-specific incidence data, and investigates return of olfactory function.

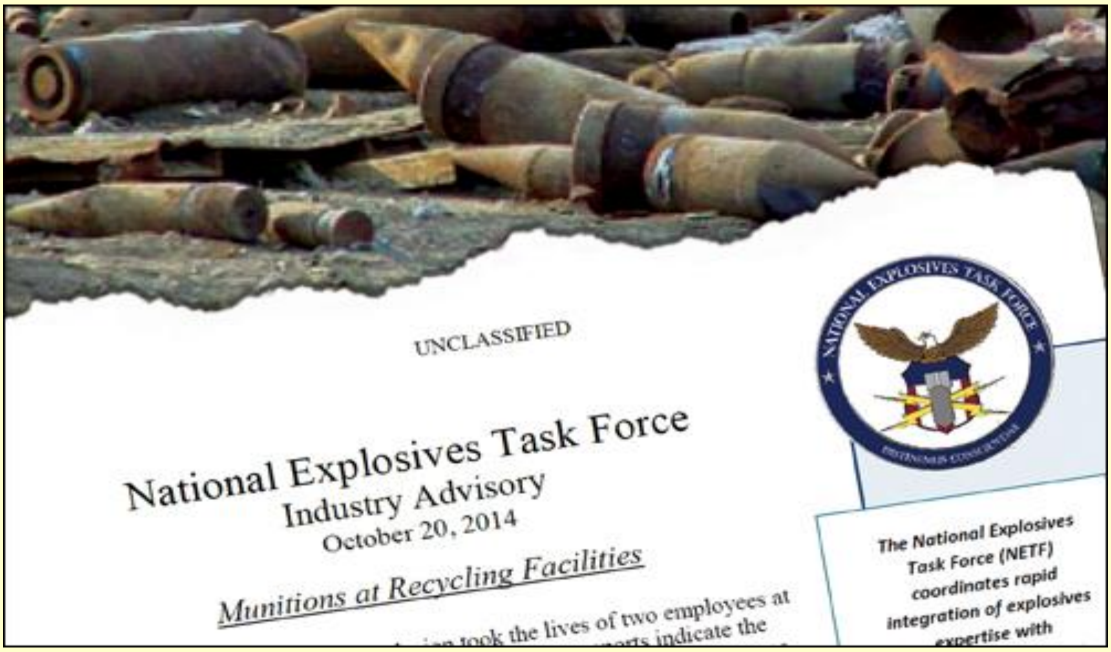
Results: Olfactometric score predicted abnormal neuroimaging significantly better than chance alone (area under the curve = 0.78, 95% confidence interval [CI] 0.70–0.87). Normosmia was present in all troops with mild TBI (i.e., concussion) and all control subjects. Troops with radiographic evidence of frontal lobe injuries were 3 times more likely to have olfactory impairment than troops with injuries to other brain regions (relative risk 3.0, 95% CI 0.98–9.14). Normalization of scores occurred in all anosmic troops available for follow-up testing.

Conclusion: Quantitative identification olfactometry has limited sensitivity but high specificity as a marker for detecting acute structural neuropathology from trauma. When considering whether to order advanced neuroimaging, a functional disturbance with central olfactory impairment should be regarded as an important tool to inform the decision process.

Classification of evidence: This study provides Class III evidence that central olfactory dysfunction identifies patients with TBI who have intracranial radiographic abnormalities with a sensitivity of 35% (95% CI 20.6%–51.7%) and specificity of 100% (95% CI 97.7%–100.0%).

ExplosivesThe National Explosives Task Force keeps a watchful eye on IEDs

Source: http://www.homelandsecuritynewswire.com/dr20150406-the-national-explosives-task-force-keeps-a-watchful-eye-on-ieds



UNCLASSIFIED

National Explosives Task Force
Industry Advisory
October 20, 2014

Munitions at Recycling Facilities

took the lives of two employees at

The National Explosives Task Force (NETF) coordinates rapid integration of explosives expertise with

Apr 09 – Bomb threats are not a new tactic for criminals and terrorists, but when scammers used them in a ruse in 2013 fraudulently to obtain pre-paid money cards from retailers around the country, first responders needed to know about it. A bulletin was sent to public safety officials explaining the scheme. The notice advised that although no devices had been found linked to this particular threat, first responders should not automatically assume any bomb threat is a hoax.

The awareness bulletin was a product of the National Explosives Task Force (NETF), a multi-agency assemblage of bomb technicians, analysts, and professional staff which formed in 2011 quickly to analyze and disseminate intelligence related to improvised explosive devices (IEDs) and other explosive materials in the United States. The FBI says that the task force, located at FBI Headquarters, includes personnel from the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Department of Homeland Security, and the Office of the Director of National Intelligence. The arrangement puts some of the nation's leading bomb experts together in the same room.

"We are trying to create a common operating picture for the federal government to look and see what the problem set is domestically in terms of explosives and IED incidents," said Whitney Barnhart, an FBI analyst who has been on the task force since its inception. "And we're using that information to create products to support federal, state, and local bomb technicians and the work that they're doing."

The NETF's main functions include gathering and analyzing intelligence on explosives, integrating the intel into investigations (to disrupt plots, for example), and pushing information out to partners — which include more than 3,100 public safety bomb technicians on more than 400 bomb squads around the country. The task force is notified every time the FBI or the ATF responds to an explosives-related incident, regardless of jurisdiction, and also reviews explosive incidents reported by public safety bomb squads, military explosive ordnance disposal teams, and other government reporting sources.

"It became apparent years ago that we really needed an interagency task force looking at the intelligence from these IED incidents and trying to quickly pull together joint intelligence products that we can disseminate to the bomb tech community to make sure that everybody is situationally aware," said James Yacone, assistant director of the FBI's Critical Incident Response Group, under which NETF operates.

Depending on circumstances, the task force might push out a detailed "Quick Look" report (within twenty-four hours of a major incident), an industry advisory, or an awareness bulletin like the bomb threat scam advisory in 2013. The bulletins typically contain device information and tactics, techniques, and procedures used by the perpetrator(s) to raise awareness among people who most need to know. Last May, for example, the task force sent an industry advisory about the use of chemical reaction bombs after four similar incidents occurred in the Washington, D.C. area (fortunately, the perpetrators in these incidents were quickly arrested). Last October, an advisory sought to bring attention to the dangers of unexploded munitions at recycling facilities after an explosion at one in Illinois killed two employees.

"We're taking information that's coming in to be more proactive about what we're seeing ahead of events and incidents," said Barnhart, the NETF analyst.

Another example is a system the task force developed to notify key personnel in local jurisdictions when inmates held on explosives-related charges are set to be released in their areas. The Bureau of Prisons notifies the task force, which vets the information and distributes it to ATF field offices and FBI bomb techs. Bradley Cooper, an ATF analyst who helped develop the inmate-release notification with an FBI partner, said the multi-agency approach makes sense.

"When everybody comes together from different agencies to work a common goal, it's remarkable," said Cooper, whose task force experience includes working alongside FBI personnel after the Oklahoma City bombing twenty years ago.

The FBI says that the full weight of the task force's effectiveness comes into focus when a major event occurs. When multiple agencies gather in a command post, they know each other and they know who has the critical explosives expertise to work an investigation.

"That's the beauty of NETF," Yacone said. "It brings together all the special mission experts."

New products to help train dogs for explosive detection

Source: http://doggymom.com/tag/transportation-security-administration/

The Department of Homeland Security (USA) has been conducting independent assessments and developing products to assist canine explosive teams.

One of the biggest challenges in the training and testing of canine teams results from the explosives materials themselves – especially new homemade explosives. Due to the potential safety risks of explosives, only specially trained federal explosive technicians can provide the material for training and testing. This not only limits training times and opportunities, but also increases the costs since the technicians must travel to a central location for multi-day training events.

Researchers have been developing a new training aid that matches the scent of explosive materials but poses no danger to the trainers, the canines or the

environment. It is currently undergoing field testing within federal, state and local canine detection teams. A key objective was to for the canines to react to the non-hazardous, non-explosive training aid the same way they would actual explosive material.

"It doesn't go boom if you drop it, hit it or light it on fire," said Canine Program Manager, Don Roberts. *"That allows teams to take the training from the very controlled environment we currently have to train in for safety reasons and put it in a real-world scenario – for example putting the odor in a cinderblock and seeing if the dog can find it. We can put this new training aid in car wheel wells, airports etc., without fear that they'll explode."*

S&T's partner, Johns Hopkins Applied Physics Lab, developed the new training aid, Roberts said. After a number of trials, they're ready to transfer the technology to the Transportation Security Administration, the primary customer for the aid. The bigger news, according to Roberts, is that the product was also designed to fit first responders' needs as well.

"The design price point and usability factor has been geared to the first responder community – state and local explosive detection dogs who don't have the regular training support TSA has. They are the ones who really need these products," said Roberts.

The training aids are made to be thrown away after being used. These aids can last for over eight hours and can be stored up to two years. The scent can be dissolved in water, as opposed to the previous explosive training materials, which required special handling, transport and had to be stored in a bunker.

Next steps for this program include developing a second scent for training the dogs, and licensing so that the products can be produced outside of the federal government.

Explosion at Power Plant Responsible for D.C. Area Outages

Source: http://washington.cbslocal.com/2015/04/07/white-house-state-department-lose-power-due-to-scattered-outages/

Apr 06 – **Problems at a Maryland electrical station caused widespread power outages across the nation's capital Tuesday, affecting the White House, the Capitol, museums, train stations and other sites.**

Many of the outages were brief, but some were longer and forced evacuations. Officials said a mechanical failure at a transfer station led to the outages, and terrorism was not suspected. Tens of thousands of customers lost power.

At the White House, the interruption last only a few seconds before backup generators kicked on. The complex quickly went back onto regular power. Electricity in the press briefing room dipped around lunchtime, briefly darkening cubicles and blackening TV screens.

White House spokesman Josh Earnest said he was with President Barack Obama in the Oval Office when the power blip occurred, and they didn't notice anything unusual.

Power also went out at the State Department during the daily press briefing, forcing spokeswoman Marie Harf to finish her comments in the dark.

Power in the U.S. Capitol building twice shut down briefly, and then came back on by way of a generator.

The root of the problem was actually an electrical station located about 35 miles southeast of D.C. in Charles County, Maryland.

A mechanical failure occurred shortly before 1 p.m. Tuesday at a transfer station there, which is controlled by utilities serving both Washington and southern Maryland.

Homeland security officials in Washington and Maryland confirmed there was an explosion at the station.

In a statement released later Tuesday afternoon, the Southern Maryland Electric Cooperative (SMECO) said a Pepco transmission conductor broke free from its support structure and fell to the ground.

Pepco says there was never a loss of permanent electric supply but rather a dip in voltage that caused equipment at some facilities to transfer to backup systems. The momentary outage occurred because of equipment in individual buildings throughout the area responding to the dip.

Some effects of the incident were still apparent later Tuesday afternoon. Some traffic lights were out, and Metro said several public transit stations were affected. Power to the trains remained on and trains were moving, Metro spokesman Dan Stessel said, but the affected stations were on emergency power, with dimmer lighting and nonworking elevators and escalators.

The Bethesda Metro station remained closed for six hours because of an escalator outage caused by the surge.

Some Smithsonian museums also lost power, were evacuated and closed to the public, including the popular National Air and Space Museum and the National Portrait Gallery, a spokeswoman said.

Thousands of tourists spilled from the museums onto the National Mall. It's a busy time of year for tourism as spring brings both better weather and the National Cherry Blossom Festival, which draws thousands to look at the pink-budded trees.

In a statement released later Tuesday afternoon, SMECO said the explosion was caused by a transmission conductor that broke free from its support structure and fell to the ground.

By officials' counts, at least 28,000 customers in the metro area were affected.

White House Spokesman: No Known Link to Terrorism in Power-Plant Blast That Caused DC Outages

Source: http://abcnews.go.com/US/wireStory/white-house-spokesman-link-terrorism-power-plant-blast-30142228

Apr 07 – White House spokesman: No known link to terrorism in power-plant blast that caused DC outages.

EDITOR'S COMMENT: Bad crisis communication management! When you say that it "was not terrorism" the next sentence would be: "Exlosion was caused by this or that technical problem or human negligence" and alike. Try better next time!

Seven hurt in car bomb explosion on Thai tourist island of Koh Samui

Source: http://www.telegraph.co.uk/news/worldnews/asia/thailand/11530069/Seven-hurt-in-car-bomb-explosion-on-Thai-tourist-island-of-Koh-Samui.html

A car bomb on the Thai resort island of Samui has wounded seven people, including an Italian 12 year old girl, police said Saturday, in a further blow to the country's tarnished reputation as a top tourist destination.

The bomb, packed inside a Mazda pick-up truck with false number plates, was detonated remotely by mobile phone late Friday in the underground car park of the Central Festival mall, sending late-night shoppers running for safety.

Police said the car had been stolen on March 31 from Yala, one of Thailand's three southernmost Muslim-majority provinces that have been scorched by a 10-year insurgency in which more than 6,300 people have been killed.

"It's a car bomb but we cannot confirm what type of explosive materials they used," Thai national police spokesman Lieutenant General Prawut Thavornsiri told AFP.

"The car used was a Mazda pick-up truck stolen from Yala," he added, without specifying whether the blast was believed to be linked to the conflict hundreds of kilometres (miles) away.

Six Thais and a 12-year-old Italian girl were treated for minor injuries and were all released from hospital, according to Poonsak Sophonsasmorong of the island's disaster prevention office.

Great interest in the Israeli system against shoulder missiles

Source: http://i-hls.com/2015/04/gerat-interest-in-the-israeli-system-against-shoulder-missile/

The growing number of shoulder launched missiles in the hand of terror groups has its effect The system, designated to protect large jet aircraft against shoulder-launched missiles (MANPADS), was proven effective and successfully performing all of the required functions.

The threat of MANPADS (ground-to-air heat-seeking man-portable missiles) has grown considerably over the last few years. **Elbit Systems Electro-optics's (EL-OP) MUlti Spectral Infrared Countermeasure (MUSIC) systems are a family of DIRCM (Directed IR Counter Measures) solutions for protecting aircraft against heat-seeking ground-to-air missiles.**

These systems integrate advanced fiber laser technology with a high rate thermal camera and a small, highly dynamic mirror turret to provide effective, reliable and affordable protection to all types of aircraft and under all operational conditions.

Designed in an open architecture, the systems can easily be integrated on any type of aircraft. EL-OP's systems are under production for several programs around the world – for a large variety of military, VIP and commercial aircraft. EL-OP's DIRCM solutions include the following:

J-MUSIC

MUSIC

A DIRCM system for the protection of helicopters and small to medium fixed-wing turboprop aircraft. This system has been selected by the Italian Air Force and is planned to be installed (in a dual turret configuration) on the C-130J, C-27J, AW101 and CSAR helicopters. The System has already been supplied and installed on VIP helicopters.

J-MUSIC
A DIRCM system for the protection of large aircraft (heavy transporters, tankers VIP jets, etc.), this system uses the same DIRCM as is in the C-MUSIC™ (see below). The system can be easily integrated on any type of aircraft, in a single or dual turret configuration. The J-MUSICT was selected for Embraer's KC-390 program in Brazil.

C-MUSIC

C-MUSIC
A complete self protection solution (including the J-MUSIC DIRCM and the PAWS IR Missile warning System), installed in an aerodynamic pod and especially designed for the protection of civil and VIP large jets. This system was selected by the Israeli government for the protection of its entire commercial airlines fleet and was designed to meet the requirements of both commercial certification and protection of large aircraft. This is the first program in the world to provide a complete protection solution for commercial aviation. The system is being offered on the international market and there is considerable interest by many potential customers operating commercial, VIP and military aircraft

The Second Most Dangerous Country For Land Mines Begins To De-Mine

Source: http://www.terrorismwatch.org/2015/04/the-second-most-dangerous-country-for.html

"My father was 79," says Donaldo Gomez, who lives in the steep Andes Mountains of Colombia. "He wasn't sick a day in his life. And then he gets killed by a mine!"

Gomez, whose father died in 2003, lives in an area that was once swarming with guerrillas. When the Colombian army moved into the region a few years ago, the Revolutionary Armed Forces of Colombia, or FARC, planted land mines to try to stop them. The same thing happened in many parts of the country.

As a result, some 11,000 Colombians have been killed or injured by mines over the past 25 years. These days, only Afghanistan racks up more annual land mine casualties: 451 people killed and injured in the past year. Colombia's total for deaths and injuries last year was 285, including 45 children.

But now things are starting to change. After 51 years, Colombia's guerrilla war is finally winding down. The Colombian government and Marxist rebels are holding peace talks in Cuba and have taken several steps to scale back the bloodshed — including a plan for the army and the FARC guerrillas to work together to locate and destroy rebel land mines. (The army got rid of its mines a decade ago.)

FARC has also called a unilateral cease-fire and has pledged to stop recruiting children under the age of 17. For its part, the Colombian military has halted bombing raids on guerrilla targets. Analysts say these moves show that the two sides are getting closer to a final peace treaty.

Such progress is good news for Liliana Lopez, who runs a hotel in Sonson, a farm town in the mountains. The area used to be a war zone. FARC guerrillas kidnapped Lopez's mother and killed two of her cousins around 15 years ago. But now, things have calmed down.

Even so, Lopez says leftover land mines are hurting efforts to promote agriculture and tourism in the region: "It's unsafe for people, for children, for animals."

To start addressing the problem, a British organization called HALO Trust is carrying out a small de-mining operation on the outskirts of Sonson. I went out with them. We trod carefully, steering clear of the red-and-white stakes marking areas that have yet to be cleared of explosives.

"We are now entering the minefield," said Jason Villamil, one of HALO's de-miners. "You can see on the right, right-hand side, this is all the minefield. This is all the suspicious area."

Villamil works with a state-of-the-art metal detector. But the FARC's rustic mines are often made with PVC tubing or glass jars and contain almost no metal, making them much harder to find.

"You see here we got a mine, which is in a glass container," Villamil said. "A person will step on the plunger. The plunger will inject sulfuric acid into the detonator, which is the only metallic piece of the mine."

To give me a better sense of the challenges he faces, Villamil conducted a test. My tape recorder contains just a small amount of metal. Still, it drew a strong signal from the metal detector while the land mine barely even registered.

After our experiment, Villamil used an explosive charge to destroy the mine.

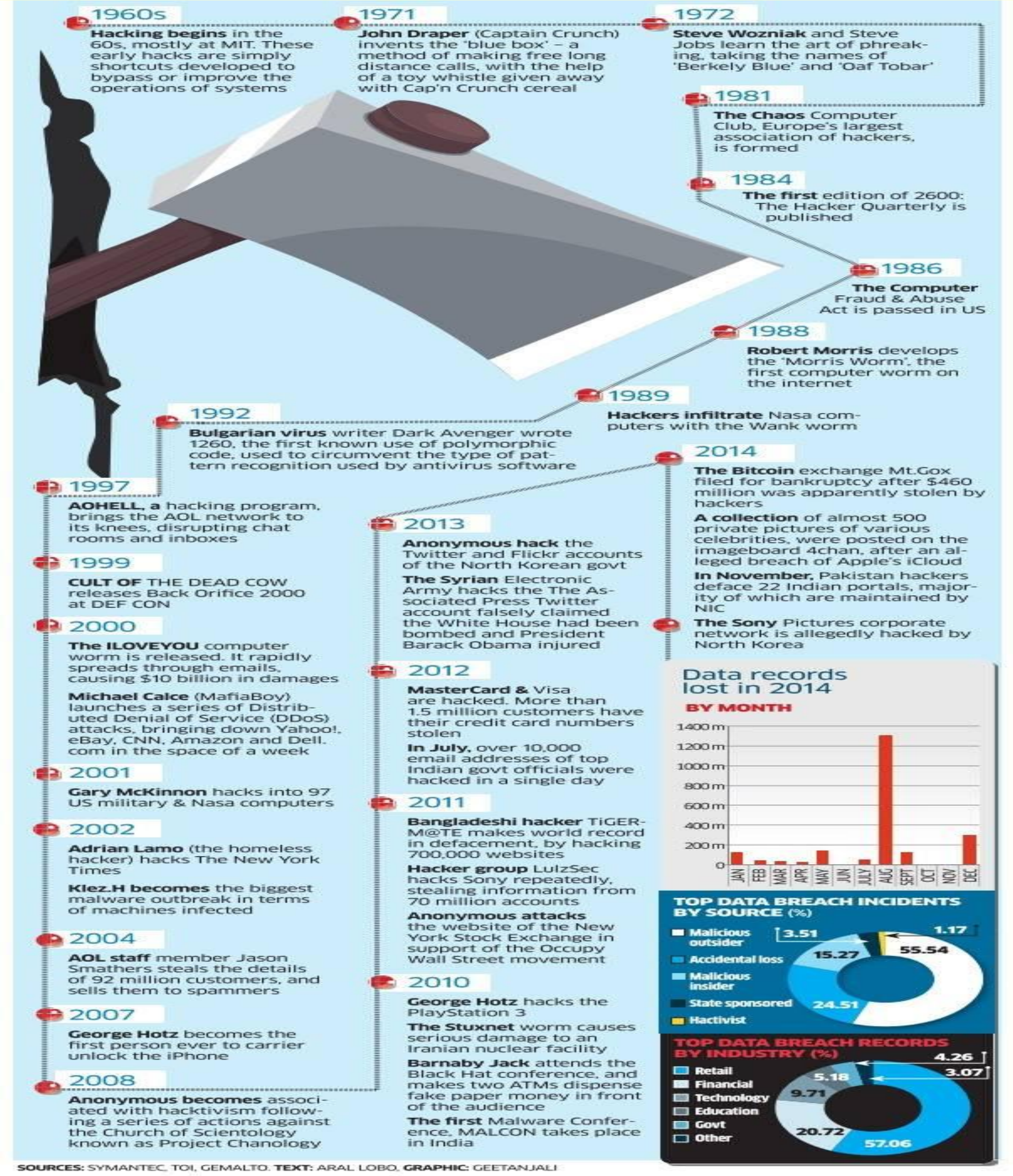
But there are thousands more out there. That's why the plan for the army and FARC to cooperate in destroying land mines is so important. The rebels know where many of the mines are buried, says a former FARC guerrilla who now works for HALO Trust.

After nine years of fighting with FARC, he says, "it now feels good to be doing this for a living because I'm helping to get these mines out of the ground."

Here's a brief history of the long and short of hacking

Source: http://economictimes.indiatimes.com/tech/internet/heres-a-brief-history-of-the-long-and-short-of-hacking/articleshow/46659391.cms

They say first computer hacker was born the second computer was born.Computer hacking was once the realm of curious teenagers. In essence, they were only trying to "hack" the system to see how it worked. However, it's now the arena of spies, professional thieves and soldiers of fortune. Today, it's all about the money. The days of mere curiosity are over. Here is the long and short of it.



1960s

Hacking begins in the 60s, mostly at MIT. These early hacks are simply shortcuts developed to bypass or improve the operations of systems

1971

John Draper (Captain Crunch) invents the 'blue box' – a method of making free long distance calls, with the help of a toy whistle given away with Cap'n Crunch cereal

1972

Steve Wozniak and Steve Jobs learn the art of phreaking, taking the names of 'Berkely Blue' and 'Oaf Tobar'

1981

The Chaos Computer Club, Europe's largest association of hackers, is formed

1984

The first edition of 2600: The Hacker Quarterly is published

1986

The Computer Fraud & Abuse Act is passed in US

1988

Robert Morris develops the 'Morris Worm', the first computer worm on the internet

1989

Hackers infiltrate Nasa computers with the Wank worm

1992

Bulgarian virus writer Dark Avenger wrote 1260, the first known use of polymorphic code, used to circumvent the type of pattern recognition used by antivirus software

1997

AOHELL, a hacking program, brings the AOL network to its knees, disrupting chat rooms and inboxes

1999

CULT OF THE DEAD COW releases Back Orifice 2000 at DEF CON

2000

The ILOVEYOU computer worm is released. It rapidly spreads through emails, causing $10 billion in damages

Michael Calce (MafiaBoy) launches a series of Distributed Denial of Service (DDoS) attacks, bringing down Yahoo!, eBay, CNN, Amazon and Dell.com in the space of a week

2001

Gary McKinnon hacks into 97 US military & Nasa computers

2002

Adrian Lamo (the homeless hacker) hacks The New York Times

Klez.H becomes the biggest malware outbreak in terms of machines infected

2004

AOL staff member Jason Smathers steals the details of 92 million customers, and sells them to spammers

2007

George Hotz becomes the first person ever to carrier unlock the iPhone

2008

Anonymous becomes associated with hacktivism following a series of actions against the Church of Scientology known as Project Chanology

2010

George Hotz hacks the PlayStation 3

The Stuxnet worm causes serious damage to an Iranian nuclear facility

Barnaby Jack attends the Black Hat conference, and makes two ATMs dispense fake paper money in front of the audience

The first Malware Conference, MALCON takes place in India

2011

Bangladeshi hacker TiGER-M@TE makes world record in defacement, by hacking 700,000 websites

Hacker group LulzSec hacks Sony repeatedly, stealing information from 70 million accounts

Anonymous attacks the website of the New York Stock Exchange in support of the Occupy Wall Street movement

2012

MasterCard & Visa are hacked. More than 1.5 million customers have their credit card numbers stolen

In July, over 10,000 email addresses of top Indian govt officials were hacked in a single day

2013

Anonymous hack the Twitter and Flickr accounts of the North Korean govt

The Syrian Electronic Army hacks the The Associated Press Twitter account falsely claimed the White House had been bombed and President Barack Obama injured

2014

The Bitcoin exchange Mt.Gox filed for bankruptcy after $460 million was apparently stolen by hackers

A collection of almost 500 private pictures of various celebrities, were posted on the imageboard 4chan, after an alleged breach of Apple's iCloud

In November, Pakistan hackers deface 22 Indian portals, majority of which are maintained by NIC

The Sony Pictures corporate network is allegedly hacked by North Korea

Data records lost in 2014

BY MONTH

TOP DATA BREACH INCIDENTS BY SOURCE (%)

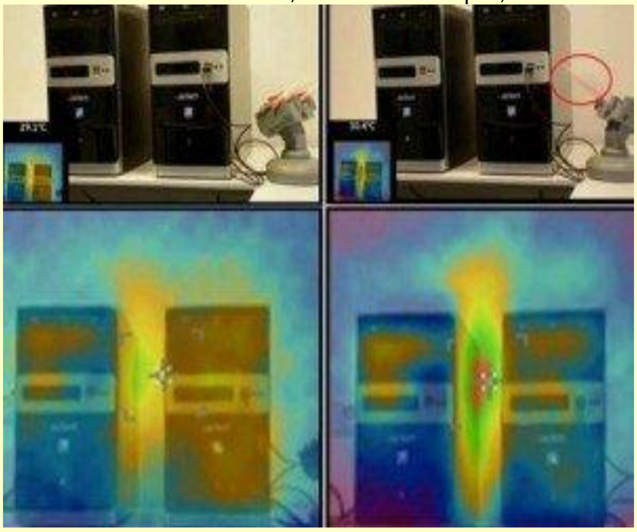
TOP DATA BREACH RECORDS BY INDUSTRY (%)

SOURCES: SYMANTEC, TOI, GEMALTO. **TEXT:** ARAL LOBO. **GRAPHIC:** GEETANJALI

CybersecurityAir-gapped computer systems can be hacked by using heat

Source: http://www.homelandsecuritynewswire.com/dr20150325-airgapped-computer-systems-can-be-hacked-by-using-heat-researchers

March 25 – **Computers and networks are air-gapped – that is, kept approximately fifteen inches (40 cm) apart — when they need to be kept highly secure and isolated from unsecured networks, such as the public Internet or an unsecured local area network.** Typically, air-gapped computers are used in financial transactions, mission critical tasks, or military applications. Israeli researchers have discovered a new method, called BitWhisper, to breach air-gapped computer systems. **The new method enables covert, two-way communications between adjacent, unconnected PC computers using heat – meaning that hackers to hack information from inside an air-gapped network, as well as transmit commands to it.**



Ben-Gurion University of the Negev (BGU) researchers have discovered a new method, called BitWhisper, to breach air-gapped computer systems. The new method enables two-way communications between adjacent, unconnected PC computers using heat.

The research, conducted by Mordechai Guri, Ph.D., is part of an ongoing focus on air-gap security at the BGU Cyber Security Research Center. Computers and networks are air-gapped when they need to be kept highly secure and isolated from unsecured networks, such as the public Internet or an unsecured local area network. **Typically, air-gapped computers are used in financial transactions, mission critical tasks, or military applications.**

According to the researchers, "The scenario is prevalent in many organizations where there are two computers on a single desk, one connected to the internal network and the other one connected to the Internet. BitWhisper can be used to steal small chunks of data (for example, passwords) and for command and control.

View BitWhisper video demo.

A release from American Associates, Ben-Gurion University of the Negev reports that BGU's BitWhisper **bridges the air-gap between the two computers, approximately fifteen inches (40 cm) apart and which are infected with malware, by using their heat emissions and built-in thermal sensors to communicate.** It establishes a covert, bi-directional channel by emitting heat from one PC to the other in a controlled manner. By regulating the heat patterns, binary data is turned into thermal signals. In turn, the adjacent PC uses its built-in thermal sensors to measure the environmental changes. These changes are then sampled, processed, and converted into data.

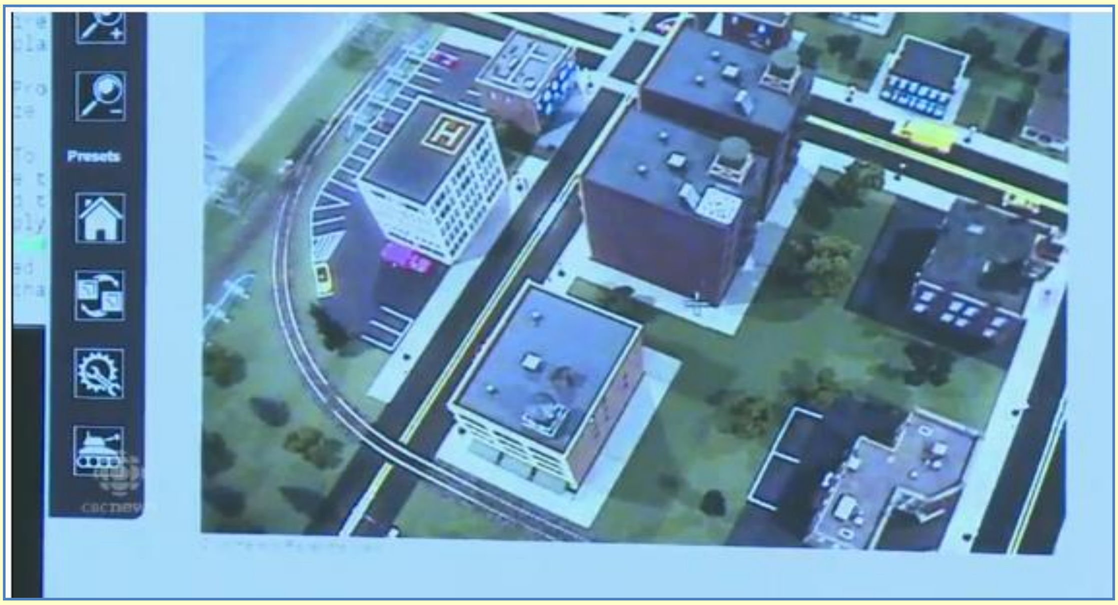
"These properties enable the attacker to hack information from inside an air-gapped network, as well as transmit commands to it," the BGU researchers explain. "**Only eight signals per hour are sufficient to steal sensitive information such as passwords or secret keys. No additional hardware or software is required.** Furthermore, the attacker can use BitWhisper to directly control malware actions inside the network and receive feedback."

***Mordechai Guri,** a student researcher in BGU's Department of Information Systems Engineering, is working under **Prof. Yuval Elovici**, director of the Cyber Security Research Center. He recently received the prestigious 2015-2016 IBM Ph.D. Fellowship Award.*

A 2-square-meter model city shows cyber-threats real cities face

Source: http://www.homelandsecuritynewswire.com/dr20150325-a-2squaremeter-model-city-shows-cyberthreats-real-cities-face

March 25 – Much attention has been focused on cyber breaches targeting U.S. private sector firms in retail, banking, and entertainment, but America's critical infrastructure also faces a threat from hackers looking to exploit the vulnerabilities of critical systems which are increasingly being connected to the Internet.



In a secret location in New Jersey, Ed Skoudis operates CyberCity, a model town of 15,000 people, which employs the same software and control systems used by power and water utilities in major cities. CyberCity has its own Internet service provider, bank, media outlets, military base, hospital, and school. The two-square-meter model town serves as a mock staging ground for the cyber threats faced by city officials around the world. There, computer security professionals get offensive and defensive training in their battle against hackers.

CBC News reports that Ed Skoudis, founder of CounterHack, designed CyberCity four years ago when military clients complained that most cybersecurity training felt too much like video games. "We need to demonstrate kinetic impact – that's the word the military folks use for physical things," Skoudis said. "Stuff moves, stuff could break, people could get injured, people could get hurt, and the military indicated to us 'we need the ability to train our people to prevent that kind of stuff from happening.'"

CounterHack designs, builds, and operates information security training programs, and hold sessions throughout the country, where computer consultants, public works employees, and military contractors spend time attacking and defending CyberCity. As students expose the vulnerabilities of CyberCity, they begin to understand the cyber weaknesses of critical infrastructure systems. In a late February class of thirteen students, CounterHack's Tim Medin led the team on their first mission to "Break into CyberCity's transportation system and change the message on an electronic billboard." To accomplish the task, the students searched through CyberCity's mock social network FaceSpace, studied the daily routines and posts of CyberCity's virtual employees who revealed details including the types of software their department uses to the format of log-ins and passwords.

With publicly available information at hand, the students were able to hack into CyberCity's transportation system in less than an hour. Watching via a remote camera, they saw the electronic billboard change from "Welcome to CyberCity" to "Zombies Ahead!"

Students also hacked into CyberCity's power grid, shutting the lights. Other CyberCity missions consist of an attack on the city's airport and military exercises involving a rocket launcher hackers hope to use against CyberCity. Students often play the role of both hacker and protector, the latter being the more difficult, Medin said. "Think of it like a giant castle and it's sort of an asymmetric game because you have to defend everything perfectly," he said, "whereas the bad guy has to find one or two ways in and it's off to the races."

Though attacks on critical infrastructure are less frequent partly because there is little monetary gain for the attackers, the public should be aware of the possibility of such attacks. "It's tough because what you don't want to do is panic everybody and say 'Hey look, this is going to happen,' but at the same time you want to raise awareness that things like this can happen," Medin said.

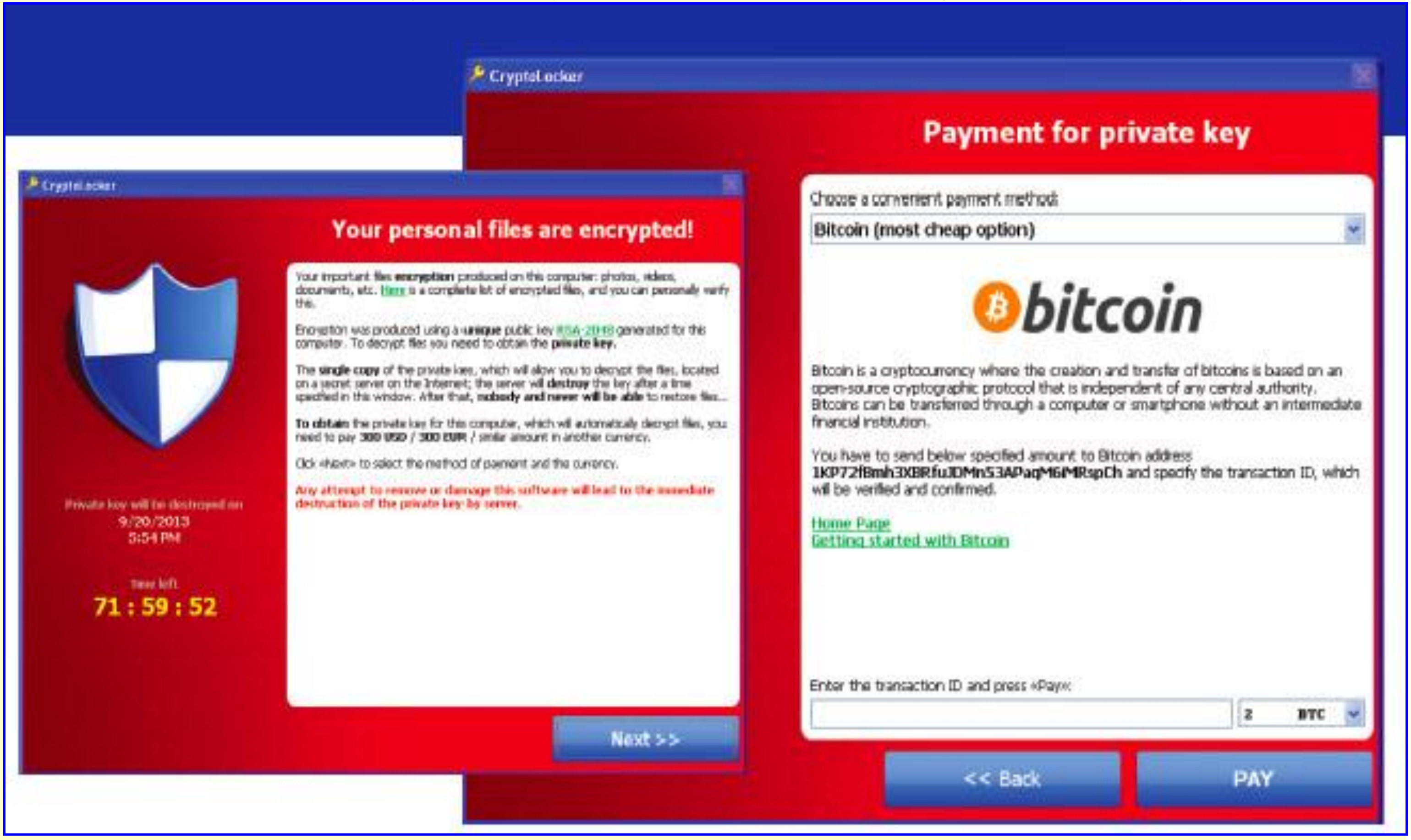
The U.S. government has issued voluntary guidelines to reduce cyber risks to critical infrastructure, but Skoudis knows that "If bad guys were really determined and they were to go after power generation equipment, they might be able to take our power for many days, maybe weeks," he said. "That's a worse-case scenario that I think about and worry about."

Police department pays ransom after hackers encrypt department's data

Source: http://www.homelandsecuritynewswire.com/dr20150406-police-department-pays-ransom-after-hackers-encrypt-department-s-data

Apr 06 – **Last December, cyberterrorists hacked into servers belonging to the Tewksbury Police Department, encrypted the data stored, and later asked for a $500 bitcoin ransom to be paid before department officials could regain control of their files.** The attack is known as the CryptoLocker ransomware virus, and it points

to a new frontier in cyberterrorism.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/20/2013
5:54 PM

Time left
71 : 59 : 52

Payment for private key

Choose a convenient payment method:
Bitcoin (most cheap option)

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Enter the transaction ID and press «Pay»:
2 BTC

For about five days, police systems in Tewksbury were down as the FBI, DHS, Massachusetts State Police, and two private sector firms worked to restore the department's data before paying the ransom.

According to the DHS Computer Emergency Readiness Team (US-CERT), CryptoLocker is a malware campaign which surfaced in 2013. It is a new variant of ransomware that restricts access to infected computers until victims provide payment to the hackers. Primary means of infection are generally phishing e-mails with malicious attachments, fake FedEx and UPS tracking notifications, and pop-up ads. Hackers usually refrain from stealing the encrypted information, so the attacks are different from breaches which have plagued U.S. banks and retail companies holding consumer information.

The *Tewksbury Town Crier* reports that **CryptoLocker has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, and all other drives and files connected to the affected computer or server.** Police Chief Timothy Sheehan said the virus is believed to have entered the department's system through the Officer-In-Charge's computer and began looking for a large store of data. Since all department computers have mapped drives and are networked, the virus went to the largest server — which housed the Computer Aided Dispatch, records management, arrest logs, calls for service, motor vehicles matters, and other department records. The data stored was then encrypted, making it impossible to access. "It basically rendered us in-operational, with respect to the software we use to run the Police Department," said Sheehan.

Tewksbury's police computers became infected on 7 December and the department became aware of the malware on 8 December. Once officers tried to access their stored data the day following the infection, they received a demand for a $500 bitcoin ransom sent to an untraceable Web address and account. Sheehan soon found out that other communities had faced similar intrusions and were forced to pay the ransom.

Since the infection was a new form of CryptoLocker, authorities did not have a key to undo the attack.

"Once hit with this kind of ransomware, only two alternatives are available," said Sheehan. If the files cannot be decrypted, then you must go to the most recent back-up. If a recent back-up isn't available, the ransom must be paid."

In Tewksbury's case, back-up files stored on an external hard drive were also corrupted, and the most recent non-corrupted files were 18-months old, not enough to rebuild missing information from paper reports.

Tewksbury has hired Delphi Technology Solutions to help diminish the town's vulnerability to future threats and system-wide hacks. Stroz Friedberg, a digital forensics and security firm, helped Tewksbury in the bitcoin transaction, refusing to take a fee because the experience would become valuable when serving the private sector.

"It was an eye opening experience, I can tell you right now," said Sheehan. "It made you feel that you lost control of everything. Paying the bitcoin ransom was the last resort."

White House Hack Is Proof Russia Is "Reassembling Its Evil Empire"

Source: http://www.ibtimes.com/white-house-hack-proof-russia-reassembling-its-evil-empire-congress man-claims-1873339

Apr 07 – **Russian hackers were recently able to breach "sensitive" computer networks at the White House after a large-scale attack gave them access to the State Department.** The news was first reported by CNN, citing U.S. officials who had been "briefed" on details of the investigation.

The State Department was forced to shut down its email network after the cyberattack last year, which the White House said had allowed the hackers to access only unclassified material. CNN now reports that **Russian hackers had access to details about President Barack Obama's schedule in real time** – which is not classified, but considered sensitive information.

Politicians responding to the attack said it was evidence of Moscow's antagonism toward U.S. interests. The president's schedule was "very sensitive" information, and the attack is "indicative that Russia is reassembling its evil empire," Rep. Darrell Issa, R-Calif., told CNN.

The Secret Service along with the FBI and other U.S. intelligence agencies were working together on an investigation of the attack, which is believed to be one of the most sophisticated ever launched against the U.S. government. Investigators believe hackers broke into the State Department's network as a way to breach White House computers, according to the report.

Investigators were unsure whether the hackers still have access to the State Department's system, CNN reported. The agencies believe the breach began with a phishing attack – where one user on the network is conned into giving their credentials to a hacker through an email disguised as being from an official source. Phishing is a common cause of many large-scale intrusions.

Hackers attempted to remain anonymous by routing the attack through computers around the world, but the report says investigators have found evidence that leads them to believe the attack was orchestrated by employees of the Russian government.

"While I can't go into detail here, the Russian cyberthreat is more severe than we had previously assessed," James Clapper, the director of national intelligence, told a Senate Armed Services Committee in February, according to Fox News. "We foresee an ongoing series of low-to-moderate-level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."

As they have in recent years, U.S. intelligence agencies once again listed cyberattacks as the top danger to U.S. national security, ahead of terrorism.

Intelligence officials now cite cyberattacks as the No. 1 threat to U.S. security, ahead of terrorism. Washington and Moscow have engaged in confrontations in the past year, including disputes over the crisis in Ukraine and American military operations in Syria.

Drug pumps vulnerable to dangerous online tampering

Source: http://thehill.com/policy/cybersecurity/238327-expert-drug-pumps-vulnerable-to-dangerous-online-tampering

Computerized drug-infusion pumps can be hacked to make it easier to deliver a deadly dose to a patient, a security researcher found.

The discovery highlights the vulnerability of network-connected medical devices to tampering online.

Experts say device manufacturers are just beginning to acknowledge and respond to the security threats.

Billy Rios, founder of security firm Laconicly, took a hard look at the workings of computerized drug pumps after using them as part of a medical treatment.

He discovered that **hackers or people within a hospital's network could break into the pumps in a way that changes the upper and lower boundaries for dosages.**

By raising the upper limit, a hacker could pave the way for someone to set the pump to deliver a dangerously high dosage, either intentionally or accidentally.

Rios found the flaw in the LifeCare PCA drug pump manufactured by Hospira and touted for its ability to defend against medical errors.

After alerting the Department of Homeland Security, officials notified Hospira and the Food and Drug Administration. DHS also issued a public alert about the flaw last week, just as Hospira attempted to patch the vulnerability in a new software update.

Rios said the patched version does not fully fix the problem, according to *Wired*, which covered the back-and-forth.

Lawmakers and regulators are beginning to take a closer look at medical devices' vulnerability to hacking, a possibility previously associated only with spy novels and TV shows.

Dr. Robert Wachter, associate chair of UC San Francisco's Department of Medicine, expressed concern about the problem with the drug pumps.

"The risk from changing the bumpers — the high and low permissible doses — doesn't seem to be very high," he told *Wired*.

"**But in a big institution giving 100,000 medications over the course of a month, screwing around with those bumpers is going to cause harm at some point.** That worries me. Anything like this at some point will kill someone."

Researchers have found a host of security vulnerabilities in medical equipment, including pacemakers, defibrillators, X-rays and drug storage refrigerators.

Electronic evidence - a basic guide for First Responders

Source: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence -a-basic-guide-for-first-responders

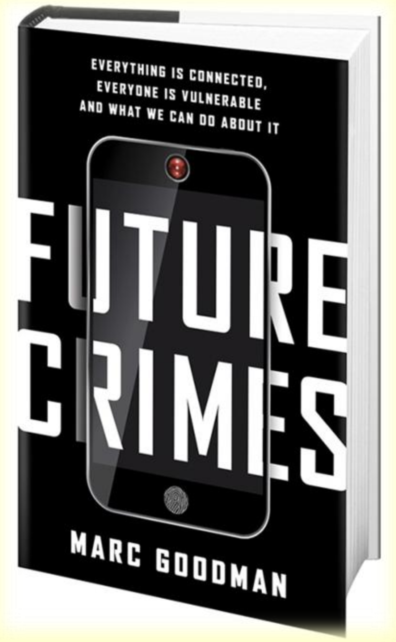
This report is a continuation of the work done by ENISA in the field of good practices for CERTs and LEAs in the fight against cybercrime. It aims at providing a guide for first responders, with a special emphasis in evidence gathering. It aims at complementing the existing (vast) material on the topic of digital forensics and evidence gathering, as these are in most cases written from the perspective of law enforcement. This guide rather aims at providing guidance for CERTs on how to deal with evidence and the evidence gathering process. For most CERTs this is a limited and (for many of them) relatively new field of operation with a growing importance.

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

Future Crimes

Source: http://futurecrimesbook.com/books/future-crimes-hc

One of the world's leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined.



Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation's power grid to air traffic control to financial services.

Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders.

With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, *Future Crimes* explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment.

Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, *Future Crimes* will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity—before it's too late.

***Marc Goodman** has spent a career in law enforcement, including work as Futurist with the FBI, Senior Advisor to Interpol and street police officer. As the founder of the Future Crimes Institute and chair for Policy, Law & Ethics at Singularity University, he has continued to investigate the intriguing, often terrifying intersection of science and crime, uncovering nascent threats and combating the darker side of technology.*

Praise

“OMG, this is a wakeup call. The outlaws are running faster than the architects. Use this book to shake up the companies you buy from, the device makers, telecom carriers, and governments at all levels. Demand that they pay attention to the realities of our new world as outlined within this thorough and deep book. Marc Goodman will startle you with the ingenuity of the bad guys. I'm a technological optimist. Now I am an eyes-wide-open optimist.”
-- Kevin Kelly, co-founder of *Wired* Magazine and bestselling author of *What Technology Wants*

"The hacks and heists detailed in *Future Crimes* are the stuff of thrillers, but unfortunately, the world of cybercrime is all too real. There could be no more sure-footed or knowledgeable companion than Marc Goodman on this guided tour of the underworld of the Internet. Everyone -- and the business world especially -- should heed his advice.”
— Daniel H. Pink, *New York Times* bestselling author of *Drive* and *To Sell is Human*

“From black ops to rogue bots and everything in between, *Future Crimes* is a gripping must-read. Marc Goodman takes readers on a brilliant, 'behind-the-screens' journey into the hidden world of 21st century criminal innovation, filled with one mind-boggling example after another of what’s coming next. *Future Crimes* raises tough questions about the expanding role of technology in our lives and the importance of managing it for the benefit of all humanity. Even better, Goodman offers practical solutions so that we not only survive progress, but thrive to an extent never previously imagined.”
--Peter H. Diamandis, *New York Times* bestselling author of *Abundance*; CEO, XPRIZE Foundation; Exec. Chairman, Singularity University

"*Future Crimes* reads like a collection of unusually inventive, terrifying plots conjured up by the world's most ingenious science fiction writer... except that almost every story in this goosebump-raising book is happening all around us right now. It's a masterful page-turner that warns of a hundred worst case scenarios you've never thought of, while also -- thank goodness -- offering bold and clever strategies to thwart them."
-- Jane McGonigal, *New York Times* bestselling author of *Reality is Broken*

“As new loopholes open up in cyberspace, people inevitably find ways to flow through them. Future-proof yourself by reading this book. No one has a better vantage point than Goodman, and you won't want to touch another keyboard until you know what's in these pages.”
-- David Eagleman, *New York Times* bestselling author of *Incognito*

"*Future Crimes* is the Must Read Book of the Year. Endlessly fascinating, genuinely instructive, and truly frightening. Be warned: Once you pick it up, you won't put it down. Super cool and super interesting."
-- Christopher Reich, *New York Times* bestselling author

“Technology has always been a double edged sword – fire kept us warm and cooked our food but also burned down our villages. Marc Goodman provides a deeply insightful view into our twenty-first century’s fires. His philosophy matches my own: apply the promise of exponentially growing information technologies to overcome age old challenges of humankind while at the same time understand and contain the perils. This book provides a compelling roadmap to do just that.”
-- Ray Kurzweil, inventor, author and futurist

“Much has been discussed regarding today’s cybercrime threats as well as the cybercriminals’ modus operandi. What is lacking, however, is what we can do about them. Mr. Marc Goodman’s book *Future Crimes* brings our global dialogue on safety and security to the next level by exploring how potential criminals are exploiting new and emerging technologies for their nefarious purposes. It provides a futuristic perspective grounded on current case studies. *Future Crime* is an essential read for law enforcers, corporations and the community alike. It offers answers beyond what comes next to what we can do, both individually and collectively, to secure ourselves and our communities.”
-- Khoo Boon Hui, former President of Interpol

"As with Naomi Klein’s *This Changes Everything* and Robert Whitaker’s *Anatomy of an Epidemic*, *Future Crimes* deserves a prominent place in our front-line library. Goodman takes us behind the computer screen to a dark world where Crime Inc. flourishes at our expense. When the criminal mind conceives “what if” it is only a matter of time before its dream becomes our nightmare. Goodman urges us to take responsibility for this new world we are speeding towards. If we don’t perhaps the greater crime will be ours."
-- Ed Burns, co-creator of *The Wire*

“This is a fantastic book and one that should be read by every cyber crime fighter. Technology breeds crime. . . it always has and always will. Unfortunately, there will always be people willing to use technology in a negative self serving way. Your only defense is the most powerful tool available to you - education. Read *Future Crimes* and understand your risks and how to combat them. The question I am most often asked in my lectures is ‘what’s the next big crime?’ The answer is in this book.”
-- Frank Abagnale, *New York Times* bestselling author of *Catch Me If You Can* and *Stealing Your Life*

"Hacking robots and bad guys using AI and synthetic biology to carry out bad deeds may seem like science fiction, but that is the real world of Future Crimes that awaits us. Marc Goodman, one of the world’s leading experts on the field, takes the reader on a scary, but eye-opening tour of the next generation nexus of crime, technology, and security."
--PW Singer, *New York Times* bestselling author of *Wired for War*

"In this highly readable and exhaustive debut, [Marc Goodman] details the many ways in which hackers, organized criminals, terrorists and rogue governments are exploiting the vulnerability of our increasingly connected society... Goodman suggests solid actions to limit the impact of cybercrimes, ranging from increased technical literacy of the public to a massive government 'Manhattan Project' for cybersecurity to develop strategies against online threats. A powerful wake-up call to pay attention to our online lives."
--*Kirkus* starred review

"Marc Goodman is a go-to guide for all who want a good scaring about the dark side of technology."
-- New Scientist

"In the wake of North Korea's cyber-terrorist attack on Sony as well as numerous hacker break-ins throughout the corporate world, it's become increasingly obvious that neither governments nor corporations are prepared for the onslaught of problems...Goodman nails the issue and provides useful input on the changes needed to make our systems and infrastructure more secure."
-- Inc.com

"Utterly fascinating stuf... Goodman weds the joy of geeky technology with the tension of true crime. The future of crime prevention starts here."
-- NPR, San Francisco

"[A] hair-raising exposè of cybercrime...Goodman’s breathless but lucid account is good at conveying the potential perils of emerging technologies in layman’s terms, and he sprinkles in deft narratives of the heists already enabled by them...A timely wake-up call."
-- Publishers Weekly

Former Israeli PM Ehud Barak invests $1 million in emergency reporting app developer

Source: http://www.homelandsecuritynewswire.com/dr20150415-former-israeli-pm-ehud-barak-invests-1-million-in-emergency-reporting-app-developer

Israeli start-up Reporty Homeland Security (note that the company’s Web site is still under development) has raised $1 million from former prime minister and minister of defense Ehud Barak. The company’s technology aims to improve and streamline communication between citizen and government agencies at the same time that it protects the user’s privacy.

The company says it is now developing a global platform for real-time reporting – reporting which is especially important during emergencies, when it can save lives.

Barak’s investment will accelerate product development, allows the company to hire more people, and distribute its system to emergency services and government organizations.

Jewish Business News reports that that emergency services and government agencies receive hundreds of millions of calls every year. The average time of a call to an assistance center is 2-3.5 minutes, during which center professionals must rapidly gain an understanding of the situation and identify the location of the call – and also evaluate the credibility of the incident report and the individual making the call – in order to make a quick decision about the best and most effective use of the resources on hand. Experts note that a vast amount of effort is invested in this process of understanding, clarification, identification, and evaluation – especially since studies have shown that 20-30 percent of calls to emergency help centers are false alarms.

JBN reports that in Israel, where emergency and security services are always on the ready, more than 20 percent of the ten million calls made every year to emergency services are nuisance calls. Magen David Adom, Israel's equivalent of the Red Cross – which is already working with Reporty — says that 23 percent of the nine million calls made to it annually are false alarms.

Quick identification of the location from where the caller is calling is also essential: In the United States, about 10,000 people a year die because emergency and rescue services fail to identify their correct location in time.

Reporty says its goal is to change this making the reporting of an emergency, and the reception of the report at the emergency help center, more efficient by using a system for real-time video transmission which incorporates a machine learning algorithm for identifying the location where the call is coming from, even if the call originates from inside a building. The application establishes a two-way video and audio connection to the emergency help center, transmitting information which gives the precise location of the person making the report and allowing for an evaluation of the incident report's credibility.

The application also allows for communication with pre-designated "guardians," that is, people designated by the user as individuals capable of helping them in emergencies.

Reporty's solution combines a smartphone app and a command and control system installed at emergency centers. The company notes that its system may also be installed at sites such as airports and company premises.

Tel Aviv-based Reporty was founded last year its CEO Amir Elichai, a former commander in an elite IDF unit with experience in venture capital in Israel. Pinchas Buchris, former director-general of Israel's Ministry of Defense and a former commander of the IDF's 8200 sig-int unit, is a director of the company.

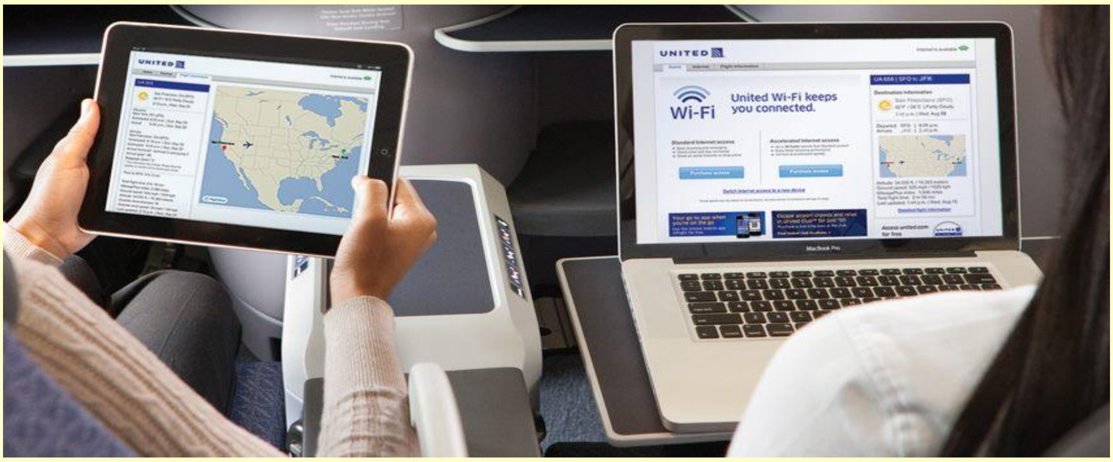
The company plans on hiring ten people by the end of the year, mainly in mobile and algorithm development.

"The solution we are developing is based on deep technology, both on the end-user side and on the command and control side," said Elichai, adding, "We are excited by the faith that Ehud Barak has placed in us. His rich experience in security will undoubtedly assist us is formulating our strategy and in launching the product in Israel and around the world."

Barak said, "Reporty provides an answer to a vital need of every citizen, namely a sense of security based on immediate and simple access to emergency services, and connection at critical moments with those closest to him or her. For organizations such as municipalities, hospitals, airports, the police, fire and rescue services and so forth, Reporty will provide a platform for control and reporting that involves citizens but maintains their privacy. Reporty is led by a group of well-qualified, goal-oriented professionals, and I believe that this high-quality team will be capable of continuing to develop the product for additional uses that are relevant to both official bodies and citizens everywhere in the world."

GAO reports warns hackers could bring down plane using passenger Wi-Fi

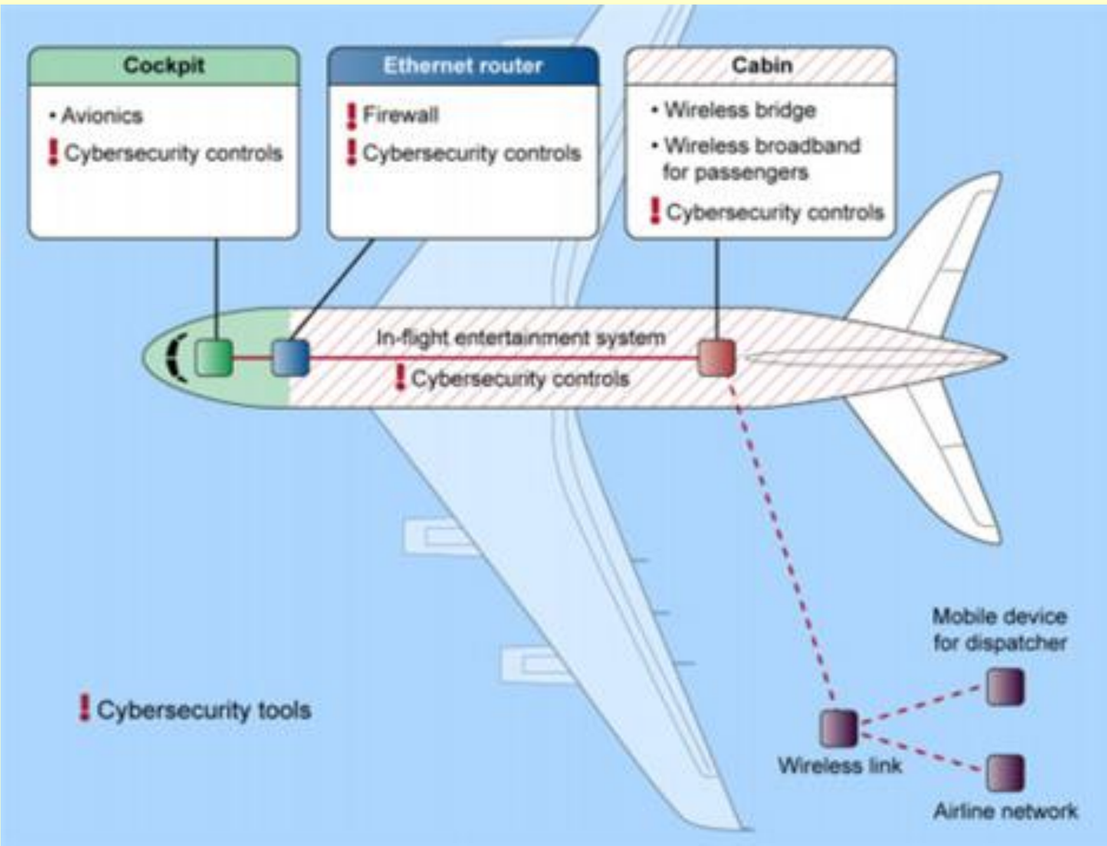
Source: http://www.foxnews.com/tech/2015/04/15/gao-reports-warns-hackers-could-bring-down-plane-using-passenger-wi-fi/



The same Internet access now available on most commercial flights makes it possible for hackers to bring down a plane, a government watchdog warned Tuesday.

The finding by the Government Accountability Office presents chilling new scenarios for passengers. The report doesn't suggest it would be easy to do, or very likely. But it points out that as airlines and the Federal Aviation Administration attempt to modernize planes and flight tracking with Internet-based technology, attackers have a new vulnerability they could exploit.

The avionics in a cockpit operate as a self-contained unit and aren't connected to the same system used by passengers to watch movies or work on their laptops. But as airlines update



their systems with Internet-based networks, it's not uncommon for Wi-Fi systems to share routers or internal wiring.

According to the report, FAA and cybersecurity experts told investigators that airlines are relying on "firewalls" to create barriers. But because firewalls are software, they could be hacked.

"According to cybersecurity experts we interviewed, Internet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors," the report states.

Chris Roberts, founder of OneWorld Labs, a Colorado based cyber security intelligence firm, told FoxNews.com that vulnerabilities exist within the in-flight entertainment systems.

“We can still take planes out of the sky thanks to the flaws in the in-flight entertainment systems,” said Roberts, who discovered susceptibilities in the system passengers use to watch television at their seats and is sharing his findings with the federal government. **“Quite simply put, we can theorize on how to turn the engines off at 35,000 feet and not have any of those damn flashing lights go off in the cockpit.”**

While commercial planes are potential targets, business, private and military aircraft also are at risk, according to another aviation security analyst who shared his findings with FoxNews.com.

“I discovered a backdoor that allowed me to gain privileged access to the Satellite Data Unit, the most important piece of SATCOM (Satellite communications) equipment on aircraft,” said Ruben Santamarta, principal security consultant for IOActive. “These vulnerabilities allowed unauthenticated users to hack into the SATCOM equipment when it is accessible through WiFi or In-Flight entertainment networks.”

.

The theoretical vulnerabilities exist within the In Flight Entertainment systems on both the Panasonic and Thales installations, the two main providers of these systems, across a wide variety of planes, Roberts said. The systems can breached wirelessly, and, once in, a clever hacker can gain access into other areas of the plane’s network, Roberts said.

“Worst case would likely be the ability to access the avionics systems, monitor and possibly influence the control interfaces and other critical flight environments typically found on the private plane subnet,” giving the hacker the ability “to intercept and possibly modify the packets of data being sent from the controls to the actuators using readily available software,” Robert said.

Neither Panasonic nor Thales responded to requests for comment from FoxNews.com.

The GAO released a separate report last March that determined the FAA's system for guiding planes and other aircraft also was at "increased and unnecessary risk" of being hacked.

One area of weakness is the ability to prevent and detect unauthorized access to the vast network of computer and communications systems the FAA uses to process and track flights around the world, the report said. The FAA relies on more than 100 of these air traffic systems to direct planes.

A worst-case scenario is that a terrorist with a laptop would sit among the passengers and take control of the airplane using its passenger Wi-Fi, said Rep. Peter DeFazio, D-Ore., a member of the House Transportation and Infrastructure Committee who requested the investigation.

"That's a serious vulnerability, and FAA should work quickly" to fix the problem, DeFazio said

A first: UAV inspects energy pipeline route in rural Virginia

Source: http://www.homelandsecuritynewswire.com/dr20150324-a-first-uav-inspects-energy-pipeline-route-in-rural-virginia

March 24 – **The first Mid-Atlantic Aviation Partnership at Virginia Tech test flight using a fixed-wing unmanned aircraft to inspect an energy pipeline route — with a piloted chase plane following behind to ensure safety beyond the ground observers' sight line — was completed last week.** The flight was a step toward making aerial inspections of energy pipelines safer and more economical, researchers say.

The flight lasted about ninety minutes and covered about eleven miles over a Colonial Pipeline Company right of way near Fork Union in rural Virginia. The mission was overseen by the Mid-Atlantic Aviation Partnership at Virginia Tech and supported by the Pipeline Research Council International, a collaborative research arm of the energy pipeline industry.

A Virginia Tech release reports that American Aerospace Technologies Inc., a Pennsylvania-based company that creates unmanned aircraft systems (UAS) for industry use, provided and piloted the test aircraft — an RS-16 UAS, which can be equipped with a special sensor package to identify threats to pipeline integrity. A piloted chase helicopter followed the unmanned aircraft for safety purposes.

"Aerial inspection of energy pipelines is federally required and typically performed using manned aircraft flying at low altitudes," said David Yoel, chief executive officer of American Aerospace Technologies Inc. "If we validate unmanned aircraft technologies, we can reduce risks to pilots and the public, and more efficiently protect the country's critical infrastructure."

Results thus far show that it is possible to use unmanned aircraft to conduct pipeline patrols, Yoel said. Ultimately, the Federal Aviation Administration will decide whether unmanned aircraft operations for utility inspections have met safety standards.

Virginia Tech, with academic partners Rutgers University and the University of Maryland, operates one of six FAA-approved unmanned aircraft testing programs in the nation under the banner of the Mid-Atlantic Aviation Partnership.

"This is important because it represents one of the first chase plane flights using a fixed-wing unmanned aircraft system for infrastructure inspections," said Rose Mooney, executive director of the Mid-Atlantic Aviation Partnership, headquartered at Virginia Tech's Institute of Critical Technology and Applied Science. "We received permission from the FAA to oversee flights of the unmanned aircraft with a chase plane. Chase aircraft observations will provide the FAA and the pipeline industry with a better understanding of UAS flight safety requirements for flights that involve long duration and great distances, such as pipeline inspections."

The research is part of Pipeline Research Council International's Right Of Way Automated Monitoring (RAM) Project, which is looking at innovative technologies to improve and automate pipeline monitoring in the United States and internationally.

Energy pipelines are mainly buried underground. Damage may inadvertently occur during land-clearing, construction, or farming work.

One of the objectives of the RAM project is to enhance aerial surveillance of the right of way through unmanned aircraft and other techniques, with the ultimate goal being continuous, real-time detection and reporting of machinery threats to pipeline integrity.

"As an entrepreneur who has been dedicated to using unmanned aerial technology to inspect infrastructure since 2008, it is my hope it can be used in remote and rural areas as early as 2017," Yoel said. "We need to do more work and additional testing to make sure we can deliver this service. I believe it is possible to improve safety and efficiency above today's levels."

Organizers say a new round of testing will be underway later this spring.

The release notes that the RS-16 aircraft has a wingspan of nearly 13 feet, a 25-pound payload capacity, and is capable of flying more than 12 hours before refueling. During future flight tests, the aircraft will be equipped with mapping capabilities and a sophisticated sensor package to detect threats to the pipeline.

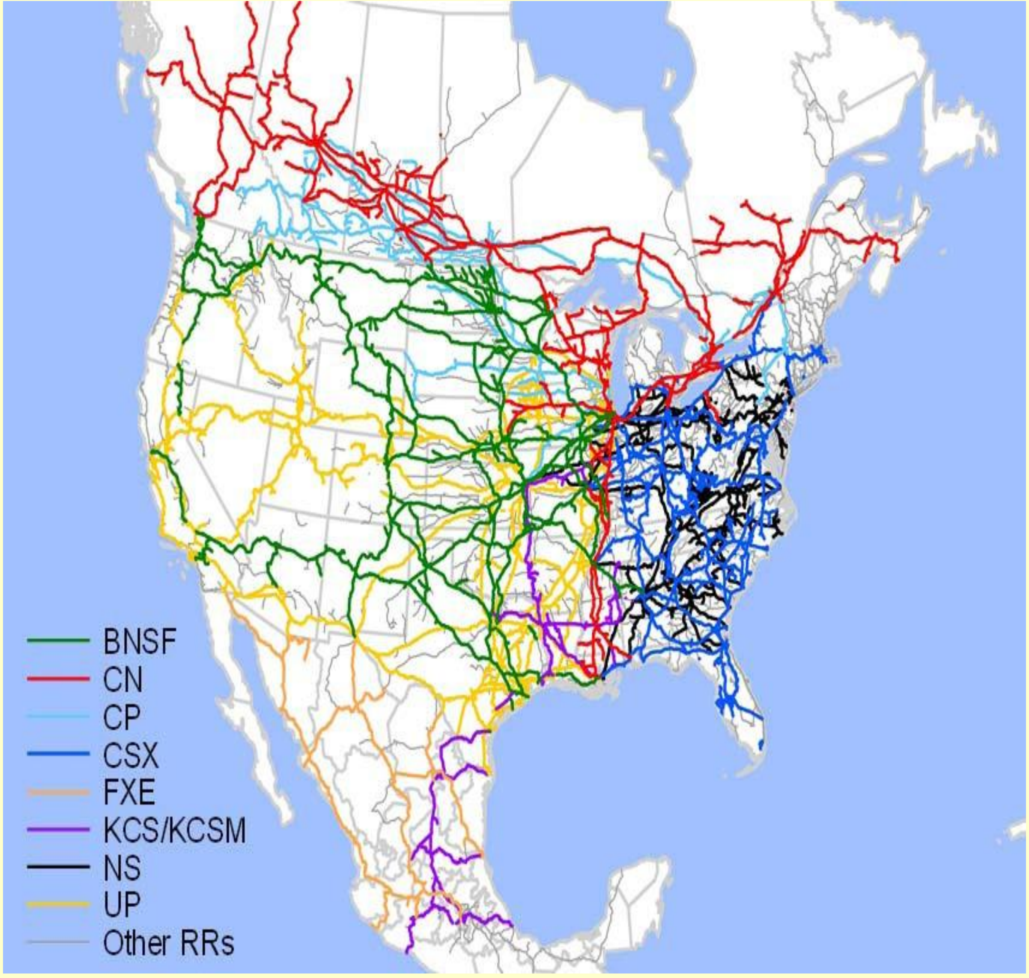
The Federal Aviation Administration selected Virginia Tech in December, 2013, as one of six national test programs to conduct research to integrate unmanned aircraft into the nation's airspace.

Living near railroad tracks? Prepare for crude-oil-train accidents, spills

Source: http://www.homelandsecuritynewswire.com/dr20150324-living-near-railroad-tracks-prepare-for-crudeoiltrain-accidents-spills

March 24 – The Minnesota Department of Transportation (MnDOT) reports that 326,170 Minnesotans live within a half mile of railroad tracks used by trains carrying crude oil from North Dakota's Bakken region. An area covering a half mile on each side of the tracks, public safety officials say, is the area from which residents are likely to be evacuated in the event of an oil train incident or explosion. The department urges all residents living near an oil train track to be prepared for a train accident.

"If you live by the train, people need to take some personal awareness of what's around them," Kevin Reed of the Minnesota Homeland Security and Emergency Management department said. '"How do I get out of the way before the fire department gets here?'" Residents should plan for how to deal with their loved ones in schools, nursing homes, businesses, and other locations near oil train tracks, Reed said, adding that first responders cannot do everything needed to protect residents when oil train accidents occur.



Last Friday, MnDOT released the number of people in thirty-four counties where Bakken oil trains travel. Hennepin County has the most residents in the danger zone with 59,359 people, followed by 44,967 in adjoining Ramsey County, and Anoka with 41,389 people. Almost half of those affected are in the Twin Cities area.

The *Daily Globe* reports that most Bakken oil trains come into Minnesota through Moorhead, passing into the Twin Cities, and then south along the Mississippi River. Some oil trains head south to Willmar then out the southwest corner of the state. An average of 6.3 oil trains cross Minnesota daily, mostly on BNSF Railway Co. tracks, according to a new state report.

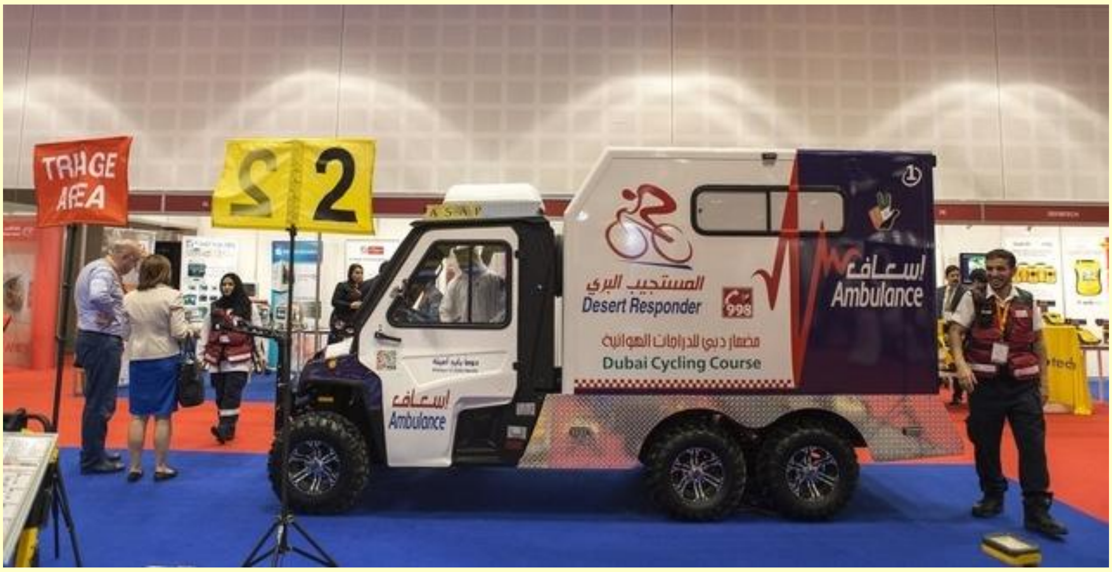
Derailments of Bakken crude oil trains in the past few years have caused explosions and in the case of a July 2013 derailment in Quebec, Canada, killed forty-seven people.

Minnesota governor Mark Dayton (D) has proposed more training for first responders who may have to deal with oil train derailments, railroad crossing improvements, and other measures, funded by increasing assessments on the state's largest railroads, taxing more railroad property, and borrowing money. The Republican-controlled state House has yet to announce a plan on how to improve rail safety. Railroads say Dayton's tax proposals would violate federal law and could be battled in court if passed.

"I'm very disappointed to hear some of the companies are strenuously opposing an increased share of the responsibility for these improvements," Dayton said Friday after visiting a Newport elementary school, blocks from heavily used rail lines along U.S. 61 in Washington County. "They're coming through the state in the volume they are and they're adding (to) their own profitability, which is why they're in business, but then to just turn their backs on the people who are living in the vicinity and say, 'Well, now you have to come up with your own resources to make these safety improvements,' I think is really, really irresponsible."

Dubai Desert Responder for cyclists introduced

Source: http://www.thenational.ae/uae/dubai-desert-responder-for-cyclists-introduced



Dubai Ambulance has launched a special vehicle for cyclists who encounter trouble and need assistance in the desert.

The six-wheel vehicle, called Desert Responder, is said to be the first of its kind in the region, catering specifically to cyclists.

"We have produced two so far," said Musallam Hussein, a paramedic. "We usually have 4x4 ambulances but these will be used for the cycling courses in Dubai, most of which are found in the desert."

The vehicle has a cycle rack attached to its front and tires that can adapt to the rough desert ground.

"Their bicycles are expensive so this metal rack can hold them," Mr Hussein said. "We used to have an ambulance which was open from the back so we had to inform the [manufacturers] that we needed a closed ambulance due to the sand and hot weather in the UAE," he said.

Although a specific number was not given, more vehicles are being produced.

Cycling accidents are all too common in the country. Last month, a British cyclist was killed in a 220-kilometre challenge ride after colliding with two motorbikes on the way to Fujairah from Dubai as part of a UAE tour.

Earlier this month, a professor from the American University of Sharjah died after a car hit him while he was cycling with a friend.

Cyclists experiencing issues in the desert were urged to call the service on 998.

UN Conference on Disaster Risk Reduction Adopts New Framework

Source: http://www.homelandsecurity.org/node/3691

March 23 – The Third UN World Conference on Disaster Risk Reduction was attended by over 6,500 participants including 2,800 government representatives from 187 governments. The Public Forum had 143,000 visitors.

Sendai Framework for Disaster Risk Reduction 2015-2030

Representatives adopted a new international framework for disaster risk reduction with seven targets and four priorities for action.

Sendai Framework for Disaster Risk Reduction 2015-2030 was adopted following a final round of negotiations.

Building on the Hyogo Framework for Action, the present framework aims to achieve the substantial reduction of disaster risk and losses in lives, livelihoods and health and in the economic, physical, social, cultural and environmental assets of persons, businesses, communities and countries over the next 15 years. To attain the expected outcome, countries will strive to prevent new and reduce existing disaster risk through the implementation of integrated and inclusive economic, structural, legal, social, health, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce hazard exposure and vulnerability to disaster, increase preparedness for response and recovery, and thus strengthen resilience.

The seven global targets are:

- Substantially reduce global disaster mortality by 2030, aiming to lower average per 100,000 global mortality between 2020-2030 compared to 2005-2015.
- Substantially reduce the number of affected people globally by 2030, aiming to lower the average global figure per 100,000 between 2020-2030 compared to 2005-2015.
- Reduce direct disaster economic loss in relation to global gross domestic product (GDP) by 2030.
- Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030.
- Substantially increase the number of countries with national and local disaster risk reduction strategies by 2020.
- Substantially enhance international cooperation to developing countries through adequate and sustainable support to complement their national actions for implementation of this framework by 2030.
- Substantially increase the availability of and access to multi-hazard early warning systems and disaster risk information and assessments to the people by 2030.

Study preliminary results show little prospect of reducing economic losses from disasters

Preliminary results of a catastrophe modelling study were presented at the conference. The results show little prospect of reducing economic losses from present levels of $240 billion per year. **The study normalized the economic losses from major natural disasters over the last twenty years and found that they oscillate around a baseline value of $240 billion. This is close to the $250 billion to $300 billion estimate of current annual levels of natural and man-made disaster losses presented in UNISDR's 2015 Global Assessment Report for Disaster Risk Reduction.**

The study recommends improving the availability of economic loss data, analyzing cost/benefits of measures such as land-use and urban planning, and promoting risk transfer. The full global study will be made available in July and will provide a breakdown of economic losses by region.

How smartphones could make emergency medical info more accessible

Source: http://www.fiercemobilehealthcare.com/story/how-smartphones-could-make-emergency-medical-info-more-accessible/2015-03-09

Smartphones could prove to be the easiest and least challenging approach to ensuring that emergency medical information (EMI), especially for the chronically ill, is within immediate reach while ensuring security of such data, according to Kristina Derrick, a pediatric endocrine fellow at the Children's Hospital at Montefiore in New York.

Mobile device handsets present a viable housing option for EMI for several reasons, including fast real-time access in emergency situations and protection of the confidential data, Derrick says.

In a paper published at *Clinical Pediatrics*, Derrick and fellow endocrinologists advocate for greater consumer education regarding EMI and the need for more consumers to focus on getting EMI within quick reach. The report also compares the pricing and utility of traditional EMI accessories.

"I believe people with chronic medical conditions would benefit if all platforms had EMI accessible from the locked screen integrated into their basic platform, as Apple has done," Derrick tells *FierceMobileHealthcare* in an email interview. "We will need to educate first responders and medical providers about these tools. Providers can then tell their patients about this option. Not every person with a chronic medical condition will have a smartphone, so this may not be the best form of EMI for everyone."

Getting consumers on board with an EMI strategy shouldn't be a huge challenge given a recent study that reveals roughly two-thirds of Americans are enthusiastic about tapping digital tools for managing personal health.

In addition, more consumers are already embracing smartphones and mobile devices for chronic disease management and treatment support services. Mobile tools, such as text messaging, can help boost adherence in global chronic disease management, which can lead to improved health and more cost-effective care, according to a recent study in the *Journal of Medical Internet Research*.

Currently, there are many options for driving EMI access, from ID tags and wallet cards to jewelry featuring data chips, Derrick says. But there can be a stigma attached to such approaches, as well as cost factors, she says, adding that using a smartphone eliminates all those issues.

"I think the most effective approach is to explain the importance of EMI and discuss all of the options with patients," Derrick tells *FierceMobileHealthcare*. "It's also very important for healthcare providers to follow up with patients to see if they have acquired EMI and remind them to obtain it, if they haven't already."

Fighting fires with low-frequency sound waves

Source: http://www.homelandsecuritynewswire.com/dr20150327-fighting-fires-with-lowfrequency-sound-waves

A thumping bass may do more than light up a party — it could flat out extinguish it, thanks to a new sound-blasting fire extinguisher by George Mason University undergrads. **The fire extinguisher uses low-frequency sound waves to douse a blaze.** Engineering seniors Viet Tran and Seth Robertson now hold a preliminary patent application for their potentially revolutionizing device.

The idea to fight fire with sound waves came when they were choosing a class project for ECE 492 and 493, Advanced Senior Design, in which students produce and present a project for a final grade.

A GMU release reports that Tran and Robertson’s 20-pound, Flash Gordon-style prototype was born through $600 of their own money and about as many trials. Their sound-wave device is free of toxic chemicals and eliminates collateral damage from sprinkler systems. If mounted on drones, it could improve safety for firefighters confronting large forest fires or urban blazes.

“Fire also is a huge issue in space,” Tran says.

"In space, extinguisher contents spread all over. But you can direct sound waves without gravity," adds Robertson.

Initially, both students thought big speakers and high frequencies would douse a fire.

"But it's low-frequency sounds — like the thump-thump bass in hip-hop that works," says Tran, who joked that rappers like 50 Cent could probably douse a fire, and that hip-hop celebrity endorsements might be just the ticket to hawk their fire extinguisher.

It has taken time for their idea to catch on. In researching ideas for the class project, Tran learned that the Defense Advanced Research Projects Agency (DARPA) was working on the concept, and that West Georgia University was working on "Prometheus." So Tran thought, "Why don't we be the ones to make it happen?"

Robertson and Tran's classmates said, "You guys will make us fail." Several professors also threw cold water on their idea before they convinced Electrical and Computer Engineering Professor Brian Mark to mentor their project.

"My initial impression was that it wouldn't work," he says. "Some students take the safe path, but Viet and Seth took the higher-risk option."

Mark knew nothing about fire extinguishers, so he took a wee step into the abyss himself.

"They're really special," Mark says. "Viet is the idea man, and Seth is practical. At the final presentation, he wanted to use some fancy new presentation technology, but Seth convinced Tran to stick with a simple PowerPoint. They didn't win the competition, but their presentation before a large audience was impressive."

The inventors make a powerful team. They met as freshmen. Tran, an admitted sub-stellar student in high school, and a pitiful culinary pupil who couldn't tell a zucchini from a cucumber, learned study discipline from Robertson, a student athlete who mastered time management.

"I'd wake up at six after we studied until three in the morning, and he'd already be at wrestling practice," Tran says.

Robertson works for the Department of Defense while studying, and he has been offered a permanent position at Hanscom Air Force Base in Bedford, Massachusetts. Tran has an internship at Zodiac Aerospace in Dulles with the promise of a full-time job upon graduation.

Mason helped the inventors apply for a provisional patent.

"The provisional patent application they filed gives them a year to talk publicly about the invention, to test the market and to determine whether pursuing the patent makes sense," says Carolyn Klenner, intellectual property paralegal, in Mason's Office of Technology Transfer, who assisted them with the patent application.

5 Tips for effective Risk Management Implementation

Source: http://levelhundred.com/5-tips-for-effective-risk-management-implementation/

Risk management is part of the lives of everyone involved in Information Security now. It is part of all the key standards out there including ISO27001 and PCI-DSS, both of which have just been updated. We have to do it but it takes time and effort to do well. So lets take a pragmatic look at the requirements of risk assessment for information security. Here are 5 tips for making it work for you:

Tip 1 – Make it meaningful

A risk assessment can be done as "paying lip service" to the requirements and can be completed because it has to be. However, when it is being done in this manner, we end up with results that are inaccurate and we don't care about. Treat it seriously as a tool to improve the business. But how do we make it meaningful? Well we have to get buy in from the senior management team and know they are going to act on the findings and resolve the issues.

Tip 2 – Define the process fully BEFORE starting

This seems a really obvious point, but frequently risk assessments are done in an unstructured way and it is often difficult to get good results. Remember the risk assessment must always be repeatable. Spend the time upfront, defining all the key parts of the risk assessment upfront , including

- How are we going to do the risk assessment

- How are we going to measure risk.
- What criteria we are going to use for accepting risk

Tip 3 – Group assets together

This is a key item for completing risk assessments. One laptop is generally pretty much like another. They can all hold sensitive data, they can all be lost stolen etc. From an asset management perspective reduce the number of assets as low as possible and group similar assets where sensible. In some cases this clearly isn't practical and with the example above you may have two or three different "types" of laptop, depending who is using them.

Tip 4 – Make sure the assets have real owners

Real owners? What I mean is that the person allocated the asset must have the power, ability, budget and resource to be able to resolve any issues that are found from the risk assessment. There is no point having findings that no one can resolve. Some assets are difficult to assign and people may not want to own them but this is key to controlling risk. They must have owners or the risk assessment will fail to address issues

Tip 5 – The risk assessment evolves over time.

The first time a risk assessment is done, it won't perfectly match absolutely everything within the business. Some assets will be over valued, some under valued. The impacts may not be perfectly accurate. It needs to be allowed time to bed in, be "tweaked" and changed so it is correct. That doesn't mean it get manipulated to get the answer that was expected! There will be risks that appear that weren't expected and yes, some of them may be more severe than had been considered.

To close, be methodical, realistic and as accurate and honest as possible when doing the risk assessment. It will produce the best possible answers to the ongoing question. What are my risks?

Could we or should we build an Australian version of FirstNet?

Source: http://push2talk.com.au/could-we-or-should-we-build-an-australian-version-of-firstnet/

FirstNet®

Signed into law on February 22, 2012, the Middle Class Tax Relief and Job Creation Act created the First Responder Network Authority (**FirstNet**). The law gives FirstNet the mission to build, operate and maintain the first high-speed, nationwide wireless broadband network dedicated to public safety.

What is FirstNet

FirstNet will be a public safety-grade network built to meet the needs of our nation's first responders.
FirstNet is working with the National Public Safety Telecommunications Council (NPSTC), the Association of Public-Safety Communications Officials (APCO), the FirstNet Public Safety Advisory Committee (PSAC), the Public Safety Communications Research (PSCR) program and standards organizations on network requirements and on defining how standards can support building future networks as public safety-grade. We believe it has many dimensions.
Some of them include:

- Coverage based on geography for public safety service as well as the population
- Solutions for serving rural and under served areas
- Reliability that public safety can count on
- Group communications to enable effective teamwork
- Redundancy and resiliency to sustain service
- A robust and reliable portfolio of devices for different user types

FirstNet will be a public safety-grade network built to meet the needs of our nation's first responders

FirstNet is working with the National Public Safety Telecommunications Council (NPSTC), the Association of Public-Safety Communications Officials (APCO), the FirstNet Public Safety Advisory Committee (PSAC), the Public Safety Communications Research (PSCR)

program and standards organizations on network requirements and on defining how standards can support building future networks as public safety-grade. We believe it has many dimensions.
Some of them include:

- Coverage based on geography for public safety service as well as the population
- Solutions for serving rural and underserved areas
- Reliability that public safety can count on
- Group communications to enable effective teamwork
- Redundancy and resiliency to sustain service
- A robust and reliable portfolio of devices for different user types

FirstNet will provide public safety users with priority access to the network

First and foremost, the FirstNet network is being built for public safety. The purpose of the network is to provide a broadband wireless communications to police officers, firefighters, paramedics and other public safety and support personnel to meet their important mission every day. We know that traditional first responders must have access to the network. During incidents where multiple agencies converge in a small area, first responders must be able to leverage access priorities.

FirstNet anticipates that the amount of available contiguous spectrum will provide capacity for public safety's needs. FirstNet also anticipates there may be times when there is excess capacity. FirstNet is exploring ways to make this valuable resource available to other users while preserving priority access to first responders.

FirstNet will harden the network to assist with resiliency during natural disasters, incidents and man-made threats

Hardening entails strengthening cell tower sites and the overall network to ensure maximum reliability. FirstNet intends to design a network with as much resiliency and redundancy that it can afford to support. The network will be engineered with back-up equipment and services to sustain operations during adverse conditions. Hardening will not be a one size fits all approach. Hardening for earthquakes may be needed in the western United States and along a vulnerable stretch of the Mississippi River. Hardening for wind speeds from hurricanes or super storms may be needed in the Midwest and along the East and Gulf Coasts. FirstNet will create hardening guidelines for all components of the radio access network (RAN). Hardening will look at towers and antennas, power supplies, temperature control and the physical and electrical connections from the network to the user devices. We also plan to determine how best to address hardening for data centers, aggregation points and servers.

FirstNet will enhance public safety communications by delivering mission-critical data and applications that augment the voice capabilities of today's land mobile radio (LMR) networks

When the FirstNet network is initially deployed, it will provide mission-critical, high-speed data services to supplement the voice capabilities of today's LMR networks. FirstNet users will be able to send and receive data, video, images, text, as well as use voice applications. They will communicate over the network and benefit from the ability to share applications.

In time, FirstNet plans to offer Voice over LTE (VoLTE). VoLTE can be used for daily public safety telephone communication. FirstNet can't predict the arrival of mission critical voice in part because the standards are still under development. Standards will determine the functionality and performance requirements for mission critical voice. FirstNet is actively involved in the standards-setting process. The industry at large is working to accelerate the development of this new worldwide standard.

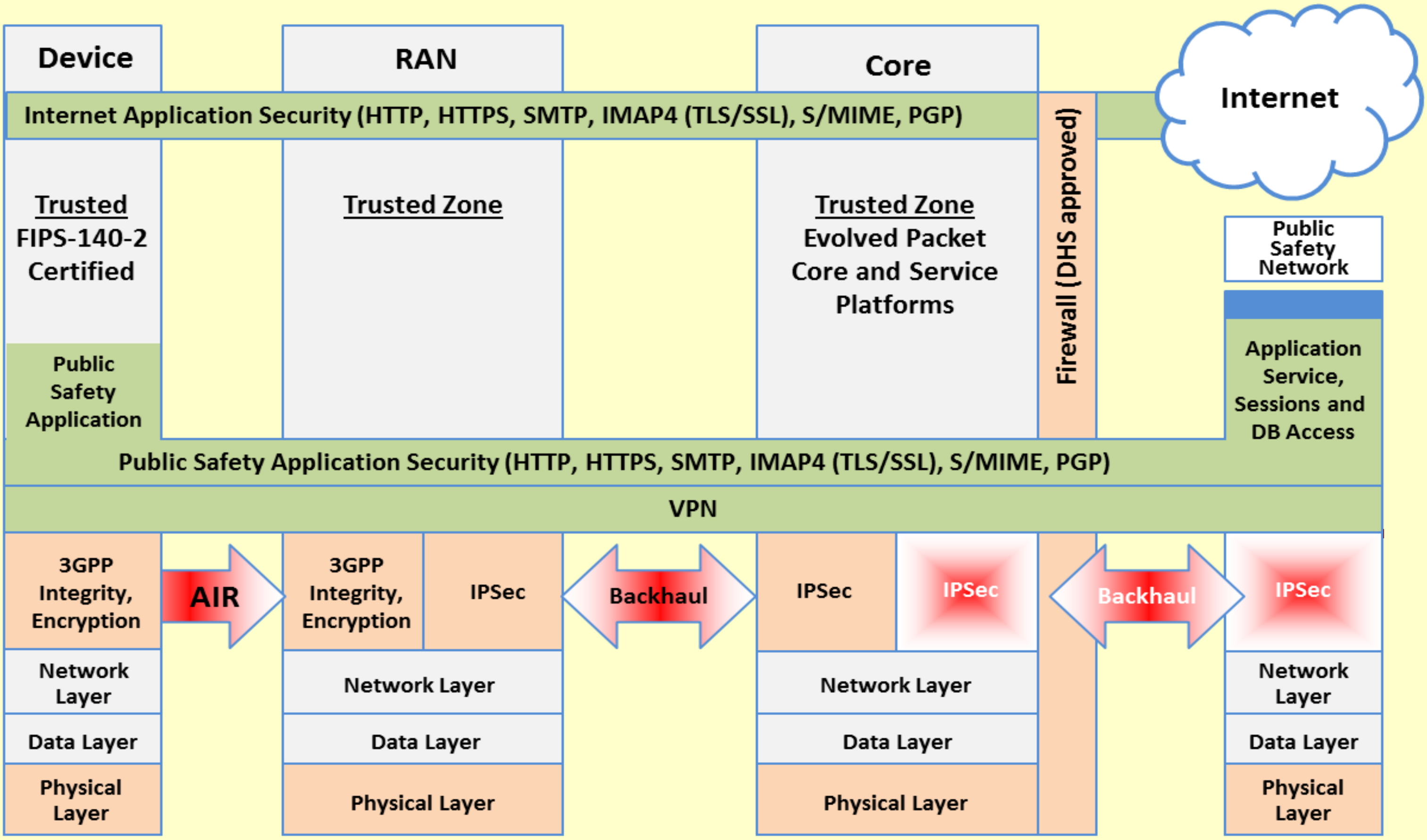
FirstNet will enable local communications management and keep incident commanders in control

FirstNet understands the importance of local control. We know that most incidents are local and need to be managed at the local level. How we enable local control has not yet been determined. In addition, FirstNet will be operated as a nationwide public safety broadband network with the ability for national and regional operations centers (NOC/ROC) to exercise control. These hierarchical control levels parallel many incident management plans already in use by public safety.

The FirstNet vision of a single, nationwide public safety broadband network with local control has many dimensions. If needed, FirstNet intends to make it possible to shift capacity to different parts of the network. Local control means that agencies will determine who has local priority to use the network to ensure public safety priorities are met. FirstNet is committed to enabling local control in a manner that aligns with public safety incident management protocols.

FirstNet will be judicious with taxpayer dollars while remaining focused on offering its services to public safety at a compelling cost

FirstNet plans to deliver valuable applications and services as well as a network tailored to the requirements of the public safety community. FirstNet acknowledges that public safety-grade reliability, security and resiliency come with a price. FirstNet plans to invest in building the first nationwide network with this level of performance. FirstNet also intends to meet its mandate to find a way to better service unserved and underserved areas. FirstNet will make every effort to keep user costs down. FirstNet plans to leverage its buying power as a nationwide network serving millions of public safety users. In addition, FirstNet will enable multiple jurisdictions to cost-effectively share access to applications and common databases such motor vehicle and criminal background information.


Device
RAN
Core
Internet
Internet Application Security (HTTP, HTTPS, SMTP, IMAP4 (TLS/SSL), S/MIME, PGP)
Firewall (DHS approved)
Trusted FIPS-140-2 Certified
Trusted Zone
Trusted Zone Evolved Packet Core and Service Platforms
Public Safety Network
Public Safety Application
Application Service, Sessions and DB Access
Public Safety Application Security (HTTP, HTTPS, SMTP, IMAP4 (TLS/SSL), S/MIME, PGP)
VPN
3GPP Integrity, Encryption
AIR
3GPP Integrity, Encryption
IPSec
Backhaul
IPSec
IPSec
Backhaul
IPSec
Network Layer
Network Layer
Network Layer
Network Layer
Data Layer
Data Layer
Data Layer
Data Layer
Physical Layer
Physical Layer
Physical Layer
Physical Layer

The legislation that established FirstNet stipulated that FirstNet would be self-sustaining and that any fees collected by FirstNet shall not exceed the amount necessary to recoup expenses. FirstNet is working to establish a pricing model that will attract users and ensure the network is self-sustaining. FirstNet will strive to price its services in a manner that enables public safety users to benefit fully from everything the network has to offer.

FirstNet will have effective security controls that protect data and defend against Cyber Threats

To defend against today's complex and rapidly changing security threats, FirstNet will be built with layers of security at every vulnerable point. Security will be designed into all radio access networks (RAN), the evolved packet core (EPC) network, service platforms, as well as the devices that use the network. Firewalls will enforce stringent security policies developed in cooperation with the Department of Homeland Security (DHS) and

Department of Defense (DoD) to meet National Institute of Standards and Technology (NIST) requirements. The FirstNet design will be guided by 3GPP (3rd Generation Partnership Project) standards for encryption as well as other standards-based security measures and best practices. FirstNet also plans to work closely with across Federal agencies with expertise in telecommunications security design modeling

FirstNet also will enable robust identity management and authentication practices at the local level. Proper credentialing will be essential to enabling the network to carry protected confidential and private information. We are seeking input from the world's leading experts. For example, FirstNet board member Teri Takai is a government information technology expert and previously served as the former CIO for the states of Michigan and California. She currently is the Chief Information Officer at the Department of Defense. We are fortunate to have her expertise and leadership on security topics.

FirstNet will design a backhaul approach that keeps the network up and running

Backhaul carries the voice, data and video traffic on the network. Backhaul provides the connections between cell sites and the core wireless broadband network. Backhaul will also connect FirstNet to the Internet and other networks such as 911 centers. Typically these connections are made via fiber optic and microwave technology. To meet the reliability needs of public safety, backhaul will be redundant wherever feasible to ensure that network traffic continues to flow during periods of extreme network demand and stress.

Through its request for information (RFI) process, FirstNet is learning about the existing backhaul capabilities of suppliers and key stakeholders including managed service providers, power utilities, commercial providers and local government agencies and facilities. Whenever possible, FirstNet will work to leverage existing government and commercial backhaul to keep costs down. FirstNet is committed to building a network where multiple transmission paths keep the traffic moving so that first responders can rely on FirstNet.

FirstNet will leverage existing infrastructure where it makes economic and engineering sense

FirstNet is developing a public/private partnership strategy to help accelerate its deployment of a broadband wireless network dedicated to public safety. When Congress created FirstNet, $7 billion was allocated to build the network. The law directed FirstNet to explore the use of existing state, local, federal and commercial assets as a way to keep costs down. We are open to all ideas and proposals. A national arrangement as well as regional partnerships involving multiple commercial carriers or utilities or federal agencies might also make sense.

FirstNet plans to evaluate where it can use existing infrastructure to build its new Band 14 network. We welcome the opportunity to leverage existing government and commercial buildings, towers, fiber or microwave backhaul and data centers to help reduce costs and enable FirstNet to launch service as quickly as possible.

During the consultation process, FirstNet will talk with state and local representatives about assets that might be leveraged. We will assess certain characteristics such as how much a site will cost, what kind of coverage it will provide and whether it meets public safety standards, to determine if it could be incorporated into the network infrastructure. All of these considerations will influence site selection. FirstNet will look at lessons learned from commercial tower operators to help us identify existing state assets and sites we can incorporate into our local radio access network planning.

FirstNet will support and learn from its BTOP project partners

The Broadband Technology Opportunities Program (BTOP) administered by NTIA provided funding for seven public safety projects in 2010. These funds were partially suspended two years later, after Congress enacted the law creating FirstNet. The suspension was needed to ensure that any further activities would be consistent with the mandates of the new law. FirstNet reviewed the proposed BTOP projects and determined that there was value in continuing to support them. As a result, FirstNet reached spectrum manager lease agreements with the Los Angeles Regional Interoperable Communications Systems Authority (LA-RICS), Adams County, Colorado (ADCOM-911), the State of New Jersey and the State of New Mexico.

FirstNet will provide technical support to these BTOP projects and will share any lessons learned with the broader public safety community to enable the successful implementation of FirstNet's nationwide deployment.
Designing and deploying a network that lives up to these principles will require an extraordinary level of coordination and collaboration among all stakeholders.

It would be a challenge, but what would it take to make our government pass a similar law? We have the ability to deliver this type of network but do we have the governments that have the vision?

Relying on Good Fortune - Not an Acceptable Preparedness Strategy

By Robert C. Hutchinson

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/Relying_on_Good_Fortune_-_Not_an_Acceptable_Preparedness_Strategy/

When hundreds of people fall ill from a mysterious biological agent, public health and law enforcement agencies work seamlessly to implement the established policies and enforce any necessary quarantine procedures that they have planned and trained for well in advance of the current threat. At least, that is what should happen. During a short-notice tabletop exercise for the Ebola virus threat in late 2014 in a major metropolitan area, numerous federal, state, local, and private sector partners met to discuss the expanding viral threat and organizational responsibilities. The conversations were both useful and concerning due to the limited amount of experience with such an expanding pathogenic threat and effectiveness of existing emergency plans. Surprisingly, most of the representatives did not perceive many, if any, direct responsibilities for their organizations and looked to others to address the emerging threat.

One of the largest disconnections was between the different fields of public health and law enforcement. Public health officials are masters of their field on many diverse fronts, but the execution of involuntary quarantines involving resistant persons was not one of the areas with a well-established track record. Similarly, law enforcement officials are expected to address numerous diverse public safety issues that evolve, but the enforcement of involuntary quarantines involving noncompliant persons was not on their radar. A few thoughtful exercise injects quickly identified this critical disconnection and the serious impact of it if a quarantine order were issued for multiple resistant persons with a serious infectious disease.

Disconnect – Expectations, Responsibilities & Execution

During the exercise, the local law enforcement representatives were unexpectedly advised that they would be enforcing any local quarantine orders executed by local public health officials. This unanticipated assignment caused some fascinating conversations, and facial expressions, for this topic had not been discussed before the exercise or in the past. The law enforcement officials were unaware of this expectation and had not planned or trained for it. The public health officials, who rarely execute a quarantine order, expected that law enforcement officials were aware and prepared to enforce an order with little or no notice.
The exercise progressed past this discussion point with the topic not resolved, but the public health expectations were formally provided to the law enforcement officials. The public health officials also were advised of the issues that required their attention to plan and prepare for this joint responsibility. The valuable exercise demonstrated a great

need for further collaboration and partnership for complex threats.

At a March 2015 homeland security conference attended by a diverse group of senior federal, state, local, tribal, and private sector leaders, this same topic was discussed with similar results. Interestingly, the same disconnection was identified and debated in search of a solution. The execution and enforcement of mandatory quarantines were so rare that the majority of participants had never contemplated the serious challenges of the issue.

With the current Ebola threat apparently diminishing, it remains to be seen what the results will be for future preparedness levels. The lessons learned from the Ebola virus, if implemented and retained, shall be beneficial for future pathogenic and biosecurity threats. However, if these lessons learned and vulnerabilities identified are not fully understood and truly addressed, organizations may be exposed to legal liability – along with political, financial, and social consequences.

Possible Legal Ramifications

A nurse who contracted Ebola while working at a Dallas, Texas, hospital filed suit against her employer for not providing appropriate training and equipment for the disease. The merits of this tort claim will be argued both inside and outside the courtroom. This lawsuit should be a notice for public officials and leaders in all related fields to assess their intentions, planning, preparedness, and training for future public health and homeland security threats. There are consequences for ignoring these clearly identified threats and conditions under legal terms such as "failure to train" and "deliberate indifference."

Research and analysis in 2010 indicated that court rulings involving failure to train and deliberate indifference could become relevant in future tort claims and actions regarding the failure to adequately prepare and train personnel for incidents or events that have already occurred or are likely to occur within jurisdictions. The recent, and probable future, shrinking of grants, funding, and budgets for preparedness and readiness shall not likely reduce an organization's potential exposure, possibly assisting legal liability to join political and financial consequences as ramifications for actions or inactions.

The foundation of preparedness is established with the training of personnel to a basic and then advanced level or standard. Research has shown that, if appropriate or required training is not provided and subsequent injury occurs, the organization may be liable for the actions of its organization and employees through the legal concepts of failure to train and deliberate indifference. An analysis of the relevant case law identifies an area of interest regarding tort claims against organizations for their training, or preparedness, to execute their expressed or expected duties and responsibilities.

Beyond the accusation of failure to train, a finding of deliberate indifference may be more serious in that it can result in stronger consequences for an organization that has been provided notice of a training issue and chooses to ignore the need or requirement. "Deliberate indifference" is defined by U.S. Legal Forms Inc. as, "the conscious or reckless disregard of the consequences of one's acts or omissions." In the early court case of Estelle v. Gamble, 429 U.S. 97 (1976), the Supreme Court found that deliberate indifference can result in an agency's liability under 42 U.S.C. § 1983 (civil rights violation). The court ruled that it was only such indifference that can offend "evolving standards of decency" in violation of the Eighth Amendment. Numerous subsequent court cases have expanded this concept and concern for organizations and individuals.

Confusion Over Quarantine Enforcement

Although there are several areas for enhancement and improvement for the next serious public health or biosecurity threat, the implementation of an involuntary quarantine remains one of the most significant ones. The arrival of Ebola in the United States in 2014 caused immense debate and confusion about quarantine and isolation laws and policies, especially with the early state quarantine guidance announced in New Jersey, New York, and Maine.

The temporary quarantine of a nurse in New Jersey after returning from West Africa ignited a firestorm of controversy regarding laws, policies, procedures, risks, and priorities. The later quarantine of the same nurse at her residence in Maine only expanded the confusion and controversy due to her actions and statements. Maine later reached a settlement with the nurse allowing her to travel freely in public.

Fortunately, with the very limited number of infected persons in the United States, due process and civil rights conversations shaped the discussion and political skirmish without a serious public health consequence. Unfortunately, this good fortune permitted many to ignore this critical subject and the nation's vulnerabilities to execute a quarantine for a more serious and immediate public health or biological threat. This underlying issue has not gone away and cannot afford to be ignored due to its enormous difficultly.

Training Before the Next Threat Arrives

Before the arrival or emergence of the next natural or human-caused biological threat, it may be advantageous to conduct a tabletop exercise utilizing a scenario similar to the nurse arriving in New Jersey from West Africa. The quarantine actions in New Jersey and Maine transitioned and terminated long before the various partners in the public and private sectors could provide many crucial answers and determine possible solutions. Additionally, this exercise scenario involves both domestic and international concerns to challenge participants.

To begin the conversation and design an exercise with a law enforcement and public health focus, the following points would be beneficial to discuss and address before the next consideration of quarantine execution and enforcement:

- Sufficiency of laws, authorities, regulations, and procedures
- Federal vs. state and local execution
- Leadership and command structure
- Coordination with wide-ranging partner organizations
- Establishment of clear and agreed upon policies and procedures
- Use of force and rules of engagement guidance
- Procurement and distribution of proper resources
  - Personal protective equipment
  - Medical countermeasures
  - Residential, medical, and detention facilities
- Assessment of realistic personnel resources
  - Reduction due to ill, worried well, and family care
  - Surge capacity and cross-certification
  - Reduction due to collateral and military reserve/guard duties
- Sufficient pre-event training and exercising
- Messaging to partners, public, and politicians
- Clear acknowledgment of capabilities and intentions

A tabletop exercise or working group based on the events in Texas, New Jersey, and Maine, with the points listed above, may be a good place to start the honest and valuable discussion. Whether it is Ebola, Middle East Respiratory Syndrome, severe acute respiratory syndrome, or any emerging influenza, the risk of life-threatening epidemics and pandemics continues globally – so should robust planning and tangible preparedness.

There are potentially serious legal, political, financial, and social ramifications for ignoring these known homeland security threats. This subject remains a serious challenge that can only be resolved through collaboration and partnership within the entire homeland security community, especially public health and law enforcement. Action is required before the next event. Relying on good fortune is not an acceptable preparedness strategy.

The opinions expressed herein are solely those of the author in his individual capacity, and do not necessarily represent the views of his agency, department or the United States government.

Robert C. Hutchinson *is a supervisory special agent (SSA) with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement's Homeland Security Investigations in Miami, Florida. He was previously the deputy director and acting director for the agency's national emergency preparedness division. SSA Hutchinson's writings and lectures often address the important need for coordination and collaboration between the fields of public health and law enforcement for homeland security threats. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.*

Hospital Surge Evaluation Tool

Source:http://www.domesticpreparedness.com/Government/Government_Updates/Hospital_Surge_Evaluation_Tool/

Mass casualty incidents have happened throughout the country in places as large as Boston, MA and as small as Newtown, CT. Hospitals need to be ready to respond with rapid treatment, effective triage, and coordinated communications to help them respond effectively when every second counts.

The Hospital Surge Evaluation Tool is a user-friendly peer assessment tool that was designed to identify gaps in a hospital's preparedness and help assess its ability to respond to a mass casualty event. The tool takes the form of an essentially no-notice drill, and incorporates the real-life considerations of healthcare delivery in acute care settings.

The tool is intended for use by hospital emergency managers, hospital administrators, and clinical staff to assess and improve their hospital's surge plans. It is not intended for use as an accountability tool. Hospitals need to exercise their preparedness for a mass casualty incident regularly. This tool can help hospital emergency managers to make recurring tabletop exercises a reality by providing a fully developed tabletop exercise that can be used at their facilities. In some respects this tool can be thought of as "Surge Evaluation in a Box".

The tool has two components, one for triaging patients in the emergency department and another for the hospital incident command center.

Expected Outcomes

At the conclusion of the exercise there will be a "Hotwash" to discuss a variety of quantitative and qualitative metrics. The "Hotwash" include feedback from the two areas of activity for the exercise, the Hospital Command Center and the Hospital Emergency Department. This is supported by graphical displays of data that are automatically generated using the data collected throughout the exercise. These data displays, which can be projected on screen and saved for future use, include:

- Immediate Bed Availability Over Time
- Patients Arrivals Over Time (By Criticality Type)
- Patient Transfers Out Of The ED Over Time

Command Center Tabletop Exercise Component

The command center component requires incident command leadership and necessary staff to respond and to assess capabilities such as bed availability within the facility. These may also be referred to as "players". Both the Command Center and Emergency Department components of a drill are run concurrently.

Emergency Department Table Top Exercise Component

The ED component requires that the "players" in the exercise, typically a nurse and physician, be free of clinical duties and able to take instructions from the Command Center "players" during the course of the drill. They will be asked to triage the automated generated list of patients who are presenting. The ED must be able to communicate with the hospital's Command Center.

Staff Commitments & Time Requirements

In order for the drill to be successful four peer assessors, preferably from another health care entity, are required. Two will be positioned in the ED at the start of the drill (with their laptops) and applicable exercise software; two will be positioned in the Hospitals' Command Center with their laptops and applicable software.

The peer assessor roles:

- The ED Controller
- The ED Qualitative Evaluator
- The Incident Command (Command Center) Evaluator
- The Bed Control Evaluator

As mentioned above in the Emergency Department Table Top Exercise Component section, two ED staff, typically a doctor and a nurse, FREE OF OTHER CLINICAL DUTIES for the duration of the actual exercise (75 – 90 minutes) need to be on hand. They will triage the automated generated list of patients who are presenting. The command center component requires incident command leadership and necessary staff to respond and to assess capabilities such as bed availability within the facility.

HPP estimates that it will take 2 – 3 hours for the exercise director to become familiar with the exercise materials. Once the exercise commences, the entire drill should take between 90 minutes to two hours. The exercise scenarios can be modified and customized by incident type, patient load and treatment requirements. Additional time (approximately one to two hours) is also necessary for an after action debrief ("hotwash") with the peer assessors as described above.

Equipment & Exercise Materials

- Four (4) laptops (which will need to be pre-loaded with the applicable software (Excel/Adobe Reader/Word).NOTE: Each laptop should have the Excel (preferably version 10 or higher), as well as MS Word Office 2010 or newer and Adobe Reader X or newer.
- The Controller & Evaluator Handbook.
- The Arrival List Generator, ED Exercise Controller and Qualitative Tools, and the Command Center Incident Commander and Bed Controller Tools - embedded in the Excel – based automated tools/spreadsheet.

The Hospital Surge Evaluation Tool builds on a prototype developed by RAND in 2012. While well received in terms of the tool's practicality it was apparent that additional development would be needed in order to make the Surge Evaluation Tool both useful and user-friendly. The current version of the Hospital Surge Evaluation Tool was pilot tested at a number of hospitals during the second half of 2014. This particular tool is also being adapted by RAND Corporation , under the direction of the Hospital Preparedness Program, for use by Healthcare Coalitions in much the same manner as this tool.

Kids can Learn Emergency Preparedness through Two New Apps

Source: http://www.homelandsecurity.org/node/3706

Apr 09 – Monster Guard created by the American Red Cross, is designed specifically for kids. The app follows monsters as they teach kids about how to prepare for real-life emergencies in a fun and engaging game. Kids will learn how to stay safe from emergencies in their house and around the country, practice what they've learned through challenging levels, and share with their friends when they pass levels. The free app available to download on iOS and Android mobile and tablet devices.

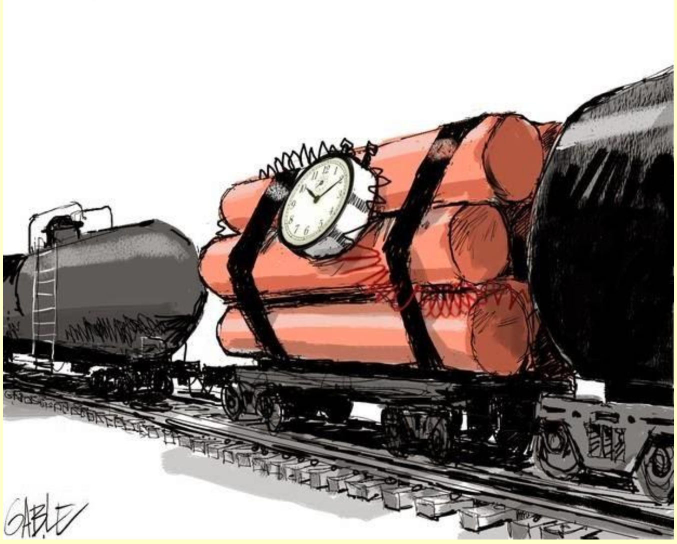
Ready Wrigley is an app designed by the Centers for Disease Control and Prevention (CDC) Office of Public Health Preparedness and Response to teach children what to do in emergency situations. Kids aged 2-8 can join the preparedness pup as she teaches kids and their families how to be safe during a public health emergency through games and activities. It is an adaptation of the Ready Wrigley activity book series. The app can be downloaded for free on the Apple App Store.

The Ticking Rail Car: First Responders Are Preparing for the Worst

Source: http://www.emergencymgmt.com/disaster/The-Ticking-Rail-Car.html

Emergency managers have been asked in recent years to do a lot more with fewer resources. **That job got even tougher with the advent of oil shipments from the Bakken shale region of North Dakota via rail around the country.**

Bakken is obtained by hydraulic fracking and horizontal drilling, which has increased since 2000 and can be highly explosive. And there have been several train derailments recently, including one in Lac-Megantic, Quebec, in July 2013 that killed 47 people.



In the U.S., a train carrying Bakken crude oil derailed in West Virginia on Feb. 16, 2015, sending orange flames skyward for days. There have been other derailments, and there's concern of a scene like the one in Quebec happening in a major U.S. city, including those in Pennsylvania. A report by PublicSource said 1.5 million people are potentially at risk if a train carrying crude oil derails and catches fire there.

Emergency managers are concerned and doing what they can to mitigate a derailment and possible explosion in their backyards. There's training available but questions remain: **Do emergency managers have all the information they need? Can one locale handle an explosion caused by a 30,000-gallon oil tanker incident?**

"From a people standpoint, the worst-case scenario is if you have one or more of these cars breach and start on fire," said Rick Edinger, assistant chief of the Chesterfield County, Va., Fire and EMS Department and a hazardous materials expert. "There's an ongoing debate about how volatile crude oil is. The feds and industry are coming to realize now that it really depends on where the oil comes from."

Because of that and other reasons, it's important to understand the nature of the product, according to Robert

Gardner, technological hazards coordinator for the Maine Emergency Management Agency. Emergency managers should study lessons learned and best practices and have safety data sheets. This information should be part of a risk assessment that lets first responders develop agency-specific response protocols that ensure responder safety and accounts for those exposed to potential fire.

Regional planning groups such as local emergency planning committees should review the routes that trains may use and identify sensitive receptors like water supplies, fisheries or agricultural areas.

Good to Know

There's ongoing debate about what information communities and emergency managers should know about train routes and shipments of crude.

"Flow studies have been around for a long time and that's an old tool that could be applied to figure out what's going through your community," Edinger said. "You may not have it down to the gallon and the day, but you have a great sense of what's coming through and frankly, from a hazmat standpoint, I don't need to know a specific time, I just need to know the worst-case scenario."

Gardner said that in terms of actual shipments, there's never enough information available. "We may know when a unit over a million gallons may be coming or where they are traveling, but those trains carrying fewer than 30 cars become unknowns," he wrote in an email.

Some railroads have systems in place that allow for real-time knowledge of what any particular train may be carrying and the tanks' location in the train.

Gardner said planning for Bakken crude oil transport is no different from any other hazardous material or even natural gas because you have an assessment and understand what you're planning for and the role of those involved. But he acknowledged that the volume of the product is a concern.

The biggest concern for many is that one or more cars loaded with crude breach can start a fire. **"Once you get past anything the size of a 9,000-gallon oil tanker, very few departments have the resources or capability to mitigate anything bigger,"** Edinger said. "If you're talking about a 30,000-tank car incident, even that would be beyond the capabilities of most departments in the initial stages, anyway."

New federal rules instituted last year require carriers to notify state emergency response commissions about the transport routes of cars carrying at least 1 million gallons of crude from Bakken. **But some emergency managers say that doesn't go far enough and doesn't include the typical load of 30,000 gallons.**

Training is available for mitigating such a circumstance, but managing the volume of an incident that size could be daunting, Edinger said. "With the exception of a couple of departments, most can't afford to stock and maintain the resources you would need to even approach doing something with one of these incidents."

Gardner said the local Maine railroads have worked to educate first responders on rail safety. "This is of particular importance as rail employees have the specific knowledge of cars and engines that not all responders have, but need [in order] to have a safe response."

Need Some Help

Gardner said it would help if the railroads could assist with the cost of the "gap pieces" of response equipment that have been identified as needed through the assessments. "It would be an immense help to many of the small volunteer agencies that we have in Maine and throughout the nation," he wrote.

An examination of the tank car fleet that carries flammable liquids may be necessary as well. Canada has banned certain cars that are known to be unsafe in crash situations, but the U.S. has lagged. Part of the reason is the price. It would cost up to $1 billion to retrofit all of the 300,000 DOT-111 tank cars in use and take years.

"The dialog is going in a good direction," Edinger said. "There seems to be agreement within public safety and the rail industry that we can do better with the construction of cars and that will improve, and perhaps prevent some incidents from happening."

***Jim McKay** is the editor of* Emergency Management. *He lives in Orangevale, Calif., with his wife, Christie, daughter, Ellie, and son, Ronan. He relaxes by fly fishing on the Truckee River for big, wild trout.*

San Antonio emergency teams train for worst scenarios

Source: http://www.homelandsecuritynewswire.com/dr20150420-san-antonio-emergency-teams-train-for-worst-scenarios

Apr 20 – Community Emergency Response Teams (CERT) in San Antonio, the sixth largest city in the United States, are worried that the large population and size of the metropolis could pose a major problem in an emergency situation.

ALAMO AREA CERT COMMUNITY EMERGENCY RESPONSE TEAM

As the *Daily Times* reports, individuals such as Alamo Area Regional Citizen Corps coordinator Scott Paul are concerned with the logistical issues presented by just how big the city is.

“You have 2.7 million people in San Antonio. Where would those people go?” he said. “Most of them would come right up I-10 to Kerr County and the surrounding area. Do you all have the resources to take care of them? No.”

The area is already at risk of tornadoes and fires, but teams have recently completed training for a wide variety of imaginable scenarios, according to Steph Lehman of the Hill County Preppers, an emergency response organization which works and trains with other CERT teams, in part with the Sheriff's Office in Kerr county.

“You need to be prepared for any scenario,” he said. “The same basic training applies to many situations.”

In training, participants learn plans and functions for traffic direction, logistical assistance, and search and rescue. Some CERT members have graduated the Kerr County Sheriff's Academy Class, while others are retired and simply want to help.

Volunteers were issued a “basic rescue bag” which included a helmet, gloves, vest, duct tapes, ponchos, and other simple emergency items, paid for by anonymous donors to the program.

“Low tech beats high tech any day,” said Lehman. “In a disaster, life's going to get really simple really quickly when the power grid goes down.”

Lehman urged awareness, as well, drawing from disaster experiences faced by the country in the earlier 2000's, such as the 9/11 terror attacks and the devastation from Hurricane Katrina in 2005.

“Do you have enough food and water to survive before the authorities can help?” he asked. “Is three days' supply sufficient? No. You need enough for ninety days, based on what we learned from Hurricane Katrina and some other recent disasters.”

Volunteers also practiced a wide range of disaster scenarios, included simulated F1 tornado drills near Wal-Mart Supercenters and mock searches for missing children. They were also taught how to secure the scene in certain situations, which included using portable switch and fuse boxes and building investigations.

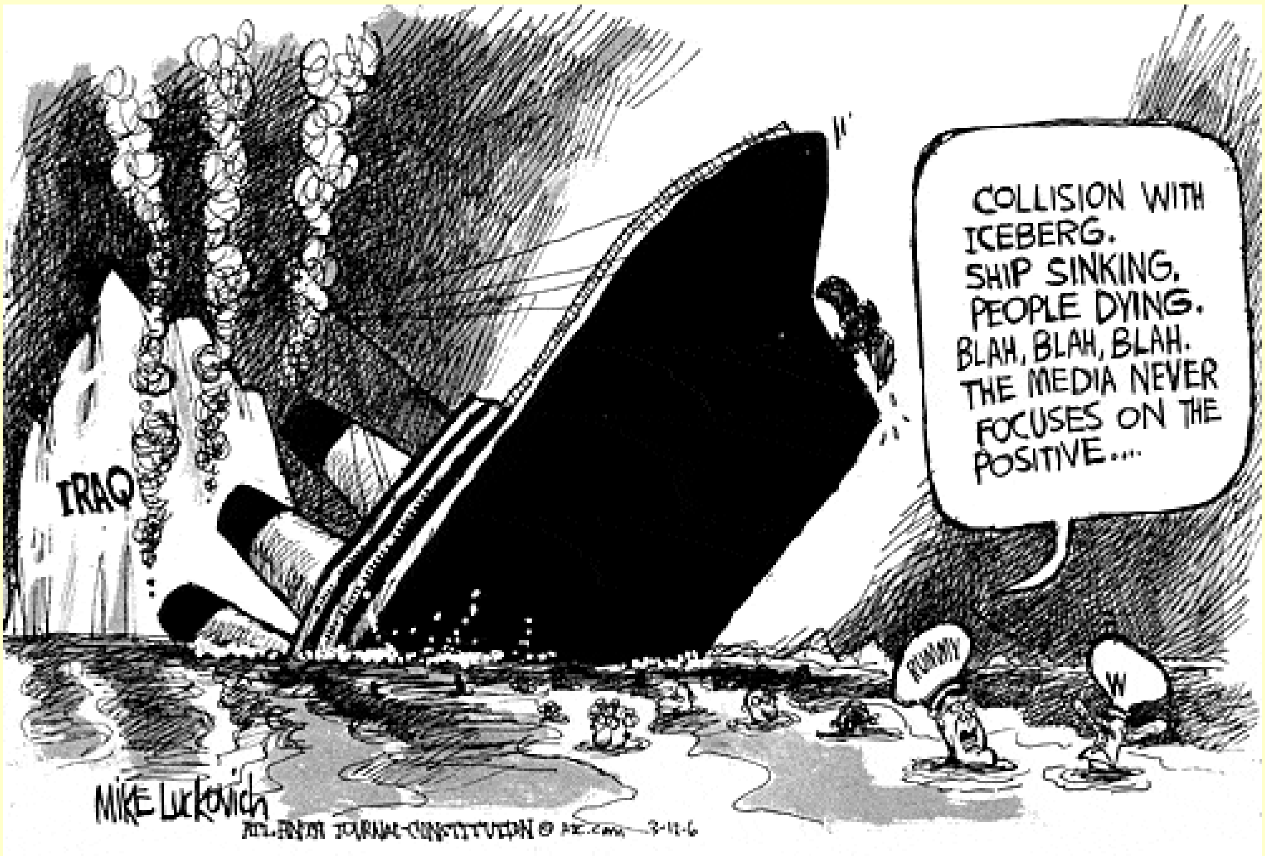
“You can't just run into a building,” said Paul. “You have to make sure electricity is turned off at the switch and the gas mains are cut off, otherwise you may wind up dead.”

More importantly, CERT members were taught ways to fight normalcy bias, or the inability to gauge emerging disasters as they unfold on the scene, such as expecting more twisters in an area that has already been recently struck.

Paul reported being pleased with the result of the recent training sessions.

"[They] aren't the best team we've had, but not the worst," he added. "No one was yelling at each other or fighting."

EDITOR'S COMMENT: Good effort! Citizens must realize – especially in big or very big cities – that First Responders will never be enough to counter all problems in a disasterous situation. Citizens must be one of the key players; not the isolated power that is left out of emergency planning. No plan is viable without them!


IRAQ
COLLISION WITH ICEBERG. SHIP SINKING. PEOPLE DYING. BLAH, BLAH, BLAH. THE MEDIA NEVER FOCUSES ON THE POSITIVE....
RUMMY
W
MIKE LUCKOVICH
ATLANTA JOURNAL-CONSTITUTION © AJC.com 3-11-6

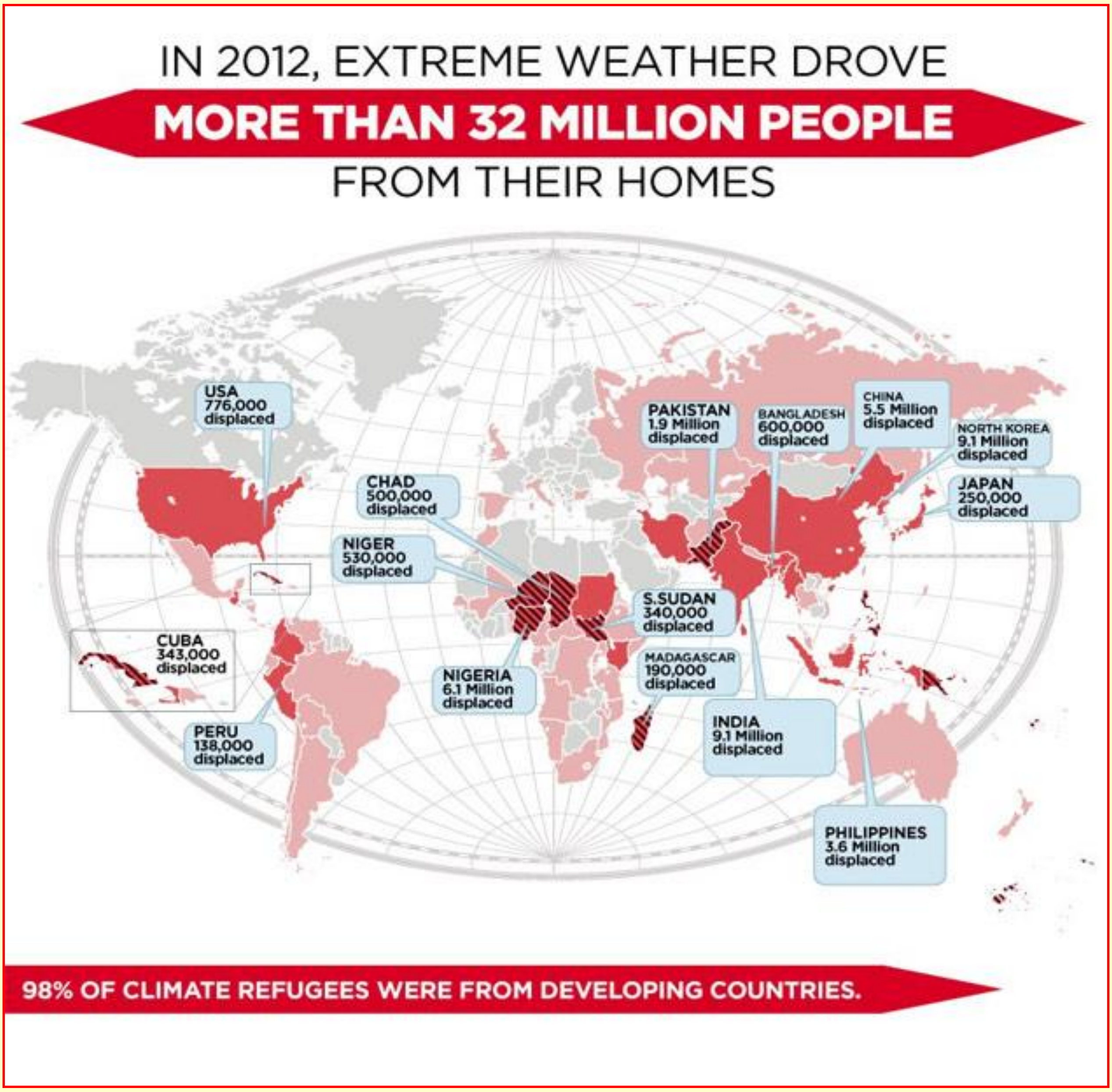
Countries brace for forced migration due to climate change

Source: http://www.homelandsecuritynewswire.com/dr20150330-countries-brace-for-forced-migration-due-to-climate-change

March 30 – **Scientists say that one of the more disturbing aspects of climate change-related disruptions is looming climate-induced migration crisis.** The *Huffington Post* reports that extreme weather disasters, sea level rise, and environmental degradation are factors which could trigger a mass migration, disrupting populations and destabilizing governments.

"We now know," said Mary Robinson, the UN Special Envoy for Climate Change and former president of Ireland, "that climate change is a driver of migrations, and is expected to increase the displacement of populations."

There are no exact predictions, but some forecasts place the number of "environmental migrants," or those displaced by climate change, at between 25 million to 1 billion by 2050. These estimates are often so wide-ranging because of the unforeseen links between climate change and migration — links which are not always direct. For instance, climate change may


IN 2012, EXTREME WEATHER DROVE
MORE THAN 32 MILLION PEOPLE
FROM THEIR HOMES
USA 776,000 displaced
CHAD 500,000 displaced
NIGER 530,000 displaced
CUBA 343,000 displaced
PERU 138,000 displaced
NIGERIA 6.1 Million displaced
PAKISTAN 1.9 Million displaced
BANGLADESH 600,000 displaced
CHINA 5.5 Million displaced
NORTH KOREA 9.1 Million displaced
JAPAN 250,000 displaced
S.SUDAN 340,000 displaced
MADAGASCAR 190,000 displaced
INDIA 9.1 Million displaced
PHILIPPINES 3.6 Million displaced
98% OF CLIMATE REFUGEES WERE FROM DEVELOPING COUNTRIES.

exacerbate a natural disaster that would have occurred anyway, or may lead to a secondary impact such as a landslide or flooding.

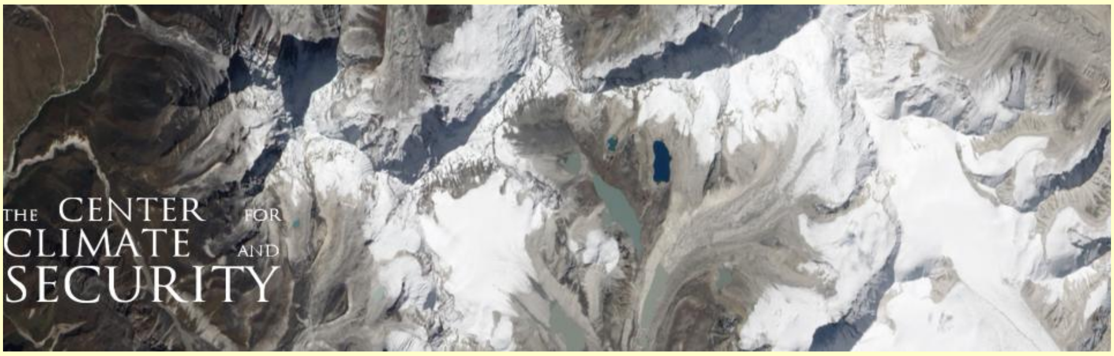
According to the Nansen Initiative, this process may already be underway. **The island nation of Fiji has finalized plans to relocate 646 coastal communities at risk.** A recent study sponsored by the governments of Switzerland and Norway found that an estimated 144 million people were at least temporarily displaced between 2008 and 2012. The United Nations Intergovernmental Panel on Climate Change has also warned that a failure to deal with the issue of climate change will only result in disarray.

"These numbers are staggering. Because climate change is expected to increase the frequency and intensity of weather-related disasters, the total number of climate change migrants will rise in the years ahead," Anika Rahman writes in the *Huff Post*.

She also cites examples of this already occurring, including continued destruction of farmland by rising sea levels, harm to global fish populations, and a lack of drinking water due to draught in places like the Colorado River, which currently serves the freshwater needs of about thirty million people.

Climate Change in the 2015 World Wide Threat Assessment of the U.S. Intelligence Community

Source: http://climateandsecurity.org/2015/03/05/climate-change-in-the-2015-world-wide-threat-assessment-of-the-u-s-intelligence-community/



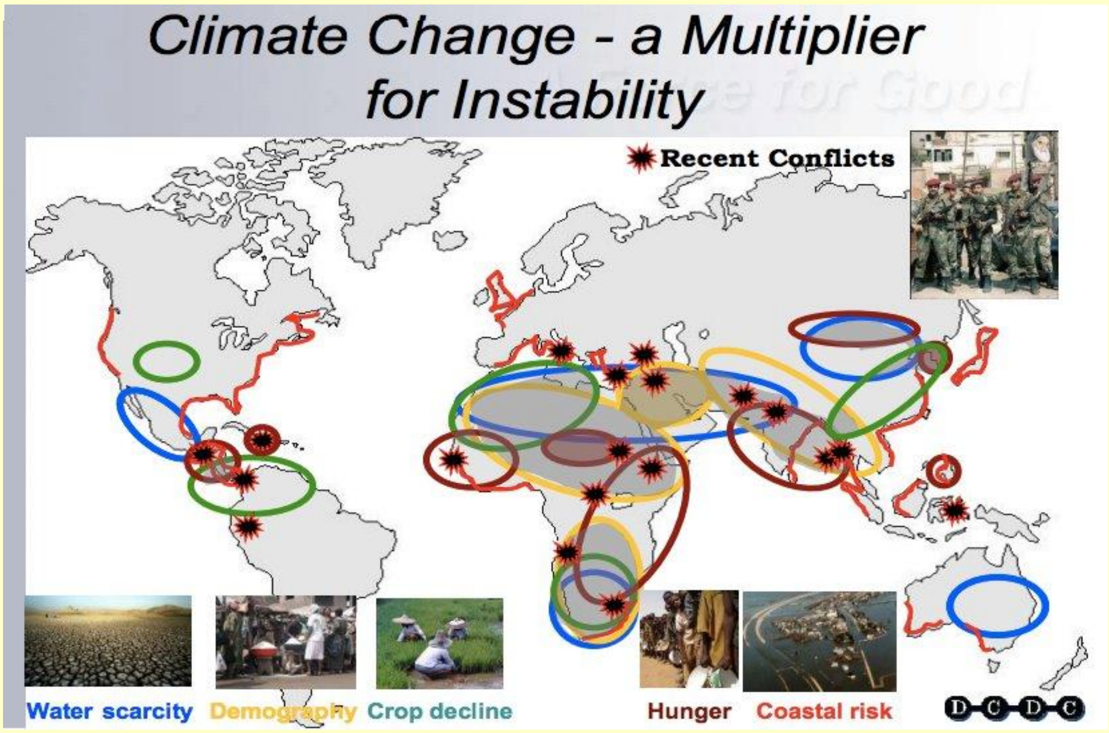
On February 26, 2015, Director of National Intelligence James Clapper presented the World Wide Threat Assessment for the US Intelligence Community Statement for the Record to the Senate Armed Services Committee. A significant portion of the assessment highlighted risks associated with the impact of climate-exacerbated extreme weather events on global food and water security (see below for those excerpts). The assessment also looked at how climate change is a factor in increasing human security risks related to infectious diseases.

This is not the first time climate change has been included in the World Wide Threat Assessment.

Here are the excerpts related to climate change in the 2015 World Wide Threat Assessment.

Extreme Weather Exacerbating Risks to Global Food and Water Security

Extreme weather, climate change, and public policies that affect food and water supplies will probably create or exacerbate humanitarian crises and instability risks. Globally averaged surface temperature rose approximately 0.8 degrees Celsius (about 1.4 degrees Fahrenheit) from 1951 to 2014; 2014 was warmest on earth since recordkeeping began. This rise in temperature has probably caused an increase in the intensity and frequency of both heavy precipitation and prolonged heat waves and has changed the spread of certain diseases. This trend will probably continue. Demographic and development trends that concentrate people in cities—often along coasts—will compound and amplify the impact of extreme weather and climate change on populations. Countries whose key systems—food, water, energy, shelter, transportation, and medical—are resilient will be better able to avoid significant economic and human losses from extreme weather.

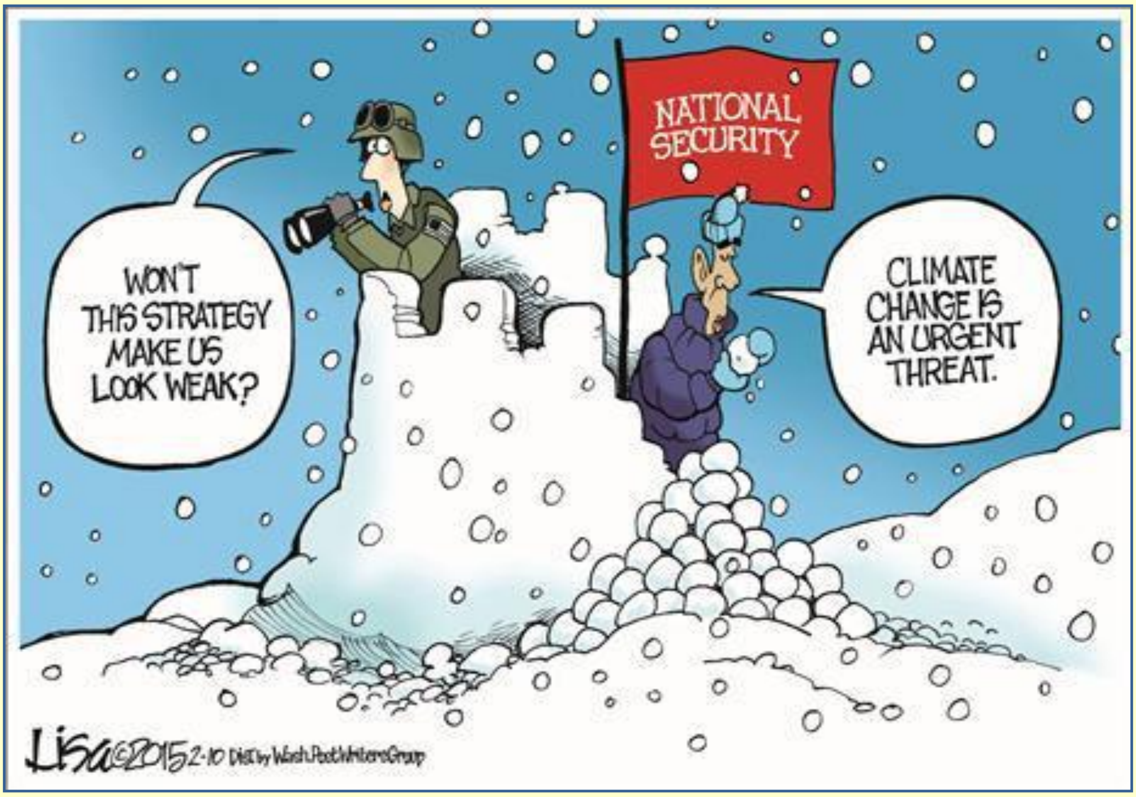


- Global food supplies will probably be adequate for 2015 but are becoming increasingly fragile in Africa, the Middle East, and South Asia. The risks of worsening food insecurity in regions of strategic importance to the United States will increase because of threats to local food availability, lower purchasing power, and counterproductive government policies. Price shocks will result if extreme weather or disease patterns significantly reduce food production in multiple areas of the world, especially in key exporting countries.
- Risks to freshwater supplies—due to shortages, poor quality, floods, and climate change—are growing. These problems hinder the ability of countries to produce food and generate energy, potentially undermining global food markets and hobbling economic growth. Combined with demographic and economic development pressures, such problems will particularly hinder the efforts of North Africa, the Middle East, and South Asia to cope with their water problems. Lack of adequate water might be a destabilizing factor in countries that lack the management mechanisms, financial resources, political will, or technical ability to solve their internal water problems.
- Some states are heavily dependent on river water controlled by upstream nations. When upstream water infrastructure development threatens downstream access to water, states might attempt to exert pressure on their neighbors to preserve their water interests. Such pressure might be applied in international forums and also includes pressing investors, nongovernmental organizations, and donor countries to support or halt water infrastructure projects. Some countries will almost certainly construct and support major water projects. Over the longer term, wealthier developing countries will also probably face increasing water-related social disruptions. Developing countries, however, are almost certainly capable of

addressing water problems without risk of state failure. Terrorist organizations might also increasingly seek to control or degrade water infrastructure to gain revenue or influence populations.

Climate change was also mentioned in the section on infectious disease.

Infectious Disease Continues To Threaten Human Security Worldwide
Infectious diseases are among the foremost health security threats. A more crowded and interconnected world is increasing the opportunities for human and animal diseases to emerge and spread globally. This has been demonstrated by the emergence of Ebola in West Africa on an unprecedented scale. In addition, military conflicts and displacement of populations with loss of basic infrastructure can lead to spread of disease. *Climate change can also lead to changes in the distribution of vectors for diseases.* (emphasis added)


NATIONAL SECURITY
WON'T THIS STRATEGY MAKE US LOOK WEAK?
CLIMATE CHANGE IS AN URGENT THREAT.
Lisa ©2015 2-10 Dist by WashPostWritersGroup

▶ **Read the full report at:** http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Can Saudi Arabia Feed Its People?

By Yossi Mann
Source: http://www.meforum.org/5098/can-saudi-arabia-feed-its-people

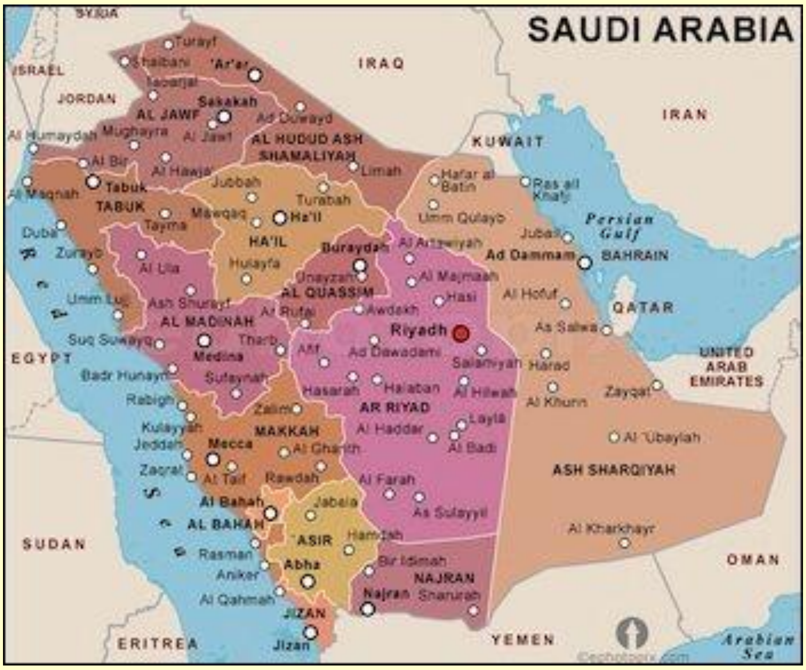
In 2007, almost thirty years after setting out on an ambitious agricultural project, Saudi Arabia announced it would be phasing out government handouts to the agricutural sector, which would end in their entirety in 2016. Outsiders criticized the project from its beginnings, emphasizing the burden it would place on the economy and the damage it would inflict on the country's water assets. Critics were particularly scathing of the decision to subsidize the project and its detrimental effects on the Saudi economy as a whole.

Nonetheless, Riyadh moved forward with what it saw as its quest to provide both food security for its burgeoning population as well as additonal employment opportunities. An examination of the wheat industry that flourished in the kingdom between 1980 and 2007, its achievements and failures, as well as the influence of the agricultural sector on the local economy and on water resources may prove a cautionary tale, reconfirming the truths behind the law of unintended consequences.

Subsidizing Food Security

Before analyzing the reasoning behind the decision to try to increase the agricultural output of the desert kingdom, it is necessary to get a full picture of what came before that decision and the actual, concrete steps taken to bring it to pass.

Despite a great deal of skepticism, Saudi Arabia managed to avoid dependence on the import of agricultural products such as wheat from the 1980s on. Indeed, Saudi increases in agricultural production were unprecedented, rising from 148,000 tons of wheat in 1981 to 4.1 million tons by 1993. The increase in its wheat exports was even more spectacular, shooting from a mere 2.4 tons in 1978 to a million tons in 2000, mostly to its Persian Gulf neighbors and to other Asian countries such as Bangladesh.



The Saudi wheat industry has been concentrated in areas including the Qasim area of the Najd plateau; the outskirts of Riyadh, Qatif, Taif, and Ha'il, and in the southern province of Asir.

One way in which this was accomplished was by significantly expanding available arable areas. The kingdom had an estimated 67,000 hectare of agricultural land in 1980, which grew to 907,000 hectare by 1993. Similarly, in 1980, the average production per farm was 2.2 tons of wheat per hectare; this grew to 5.19 tons by 2005. Some companies in the country's northern territories even managed to significantly increase production to 8-10 tons per hectare, an amount more or less on a par with production in Eastern and Central Europe.[1]

Over the years, the Saudi wheat industry became concentrated in several areas including the Qasim area of the Najd plateau, the outskirts of Riyadh, the outskirts of Qatif in the eastern province, Taif and its environs in the Northern Province, around the northwestern city of Ha'il and in the southern province of Asir.

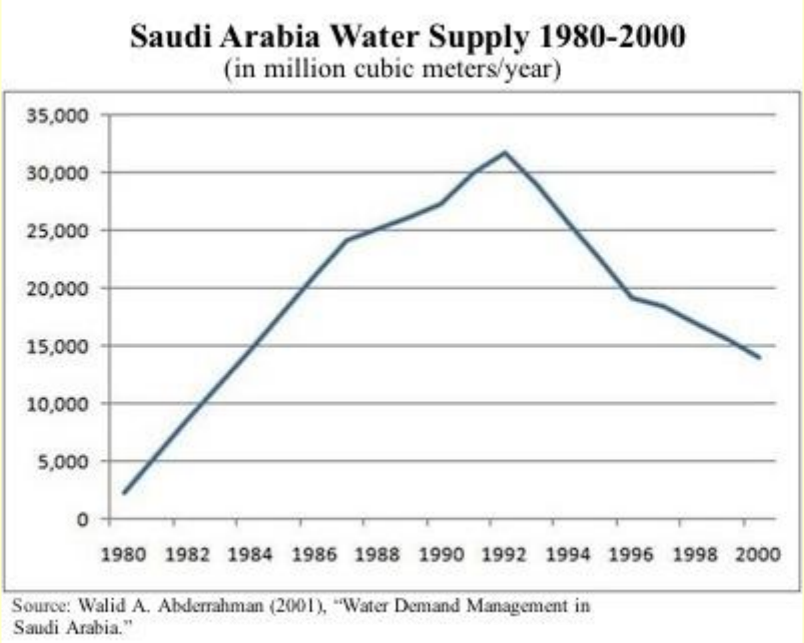
Due to better climactic conditions, the Saudi royal family invested greater effort in the northern parts of the country where agricultural companies controlled vast areas that expanded to over 268-380 hectares. In most other parts of the kingdom, the usual amount of land allotted to wheat was more in the 5-10 hectare range.

The explosion in wheat production could not have taken place, however, without government support. In the 1980s, Riyadh granted the agricultural sector incentives such as subsidies on grain, fertilizer, and irrigation water, and a 45 percent discount on purchasing agricultural machinery. Despite the huge price difference between locally produced wheat ($1,000 per ton) and what was available on world markets ($100 per ton), the Saudi government continued to purchase domestic agricultural produce and to sell it on the local market at artificially lowered prices.

This thriving agricultural sector brought about a significant rise in employment. In the mid-1970s, 274,000 people worked in agriculture; those numbers rose to 681,000 by 1992. The boom increased profits for the farming sector though mainly for large landowners.

To increase profits further and to administer their holdings better, the important Saudi trading families and the Saudi princes joined forces with international companies. In the 1980s, for example, Prince Muqrin bin Abdul Aziz, governor of the town of Ha'il, became a partner in the Ha'il Agricultural Development Company, which soon became the biggest agricultural company in the kingdom. Since most of the large agricultural companies were established by the Saudi elites, critics have claimed that the subsidies were essentially granted for the benefit of the same elites.[2] A further consequence of the policy was an increase in wheat smuggling from Yemen and Oman in order to sell it on the Saudi market at a huge profit.[3]

By the 1980s, Saudi government stability had become dependent on those who demanded subsidy guarantees in exchange for domestic stability. The subsidies took an enormous toll on the country's economy, though, eating up an estimated 20 percent of Saudi oil profits between 1980 and 2000. Nor were agricultural subsidies always consistently granted. When food and oil prices dropped, the Saudi government cut down on financial support in order to avoid excess production. Subsidies were at a peak in the beginning of the 1980s when the agricultural industry was just starting out, and government income was particularly high following a decade of oil-induced prosperity. However, low oil prices from 1995-96 made it hard to grant subsidies at the same level as in the preceding years. This, in turn, resulted in a decrease in agricultural production in those years. The royal house looked to avoid too drastic a subsidy cut even when the country was undergoing an economic crisis figuring that once the agricultural sector had been granted assistance, it would find it difficult to function without it. Indeed, the sector's dependence on subsidies was one of the factors behind violent clashes that broke out in the city of Buraida in January 1995 when those who earned their livelihood from agriculture protested against the possibility of cutbacks. Such guarantees provided a quid pro quo for domestic stability.[4]



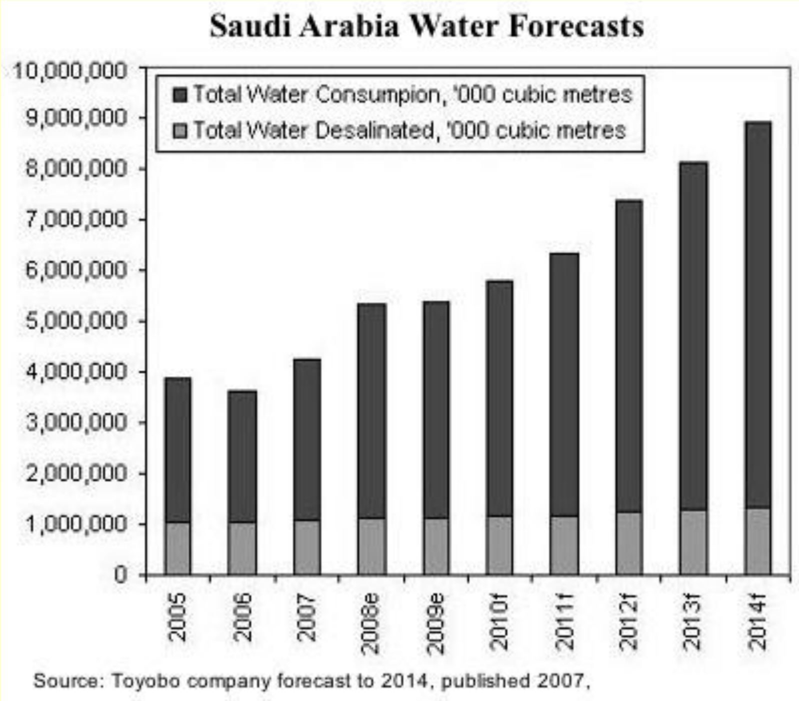
Saudi Arabia Water Supply 1980-2000
(in million cubic meters/year)

Source: Walid A. Abderrahman (2001), "Water Demand Management in Saudi Arabia."

The Most Precious Resource

But, the ambitious wheat project also had a negative impact on the country's fragile water supply. The Saudi summer is very hot and arid with temperatures often reaching as high as 120° Fahrenheit (49° Celsius). Average rainfall is 5 inches (130 mm) a year although there has been some occasional flooding in agricultural areas during the "rainy" season. The sporadic rain, soaring temperatures, and high evaporation rates in the eastern areas of the country make it very difficult to establish a viable agricultural economy. For example, an average of 13,173 cubic meters of water is required to irrigate a hectare of wheat in Saudi Arabia as compared to the world average rate of 1,622 cubic meters.[5]

The Saudi water sector only began to be developed in the 1930s. Until then, most of the kingdom's water came from wells that could be found near the main towns. In 1956, sewage water infiltrated many wells, forcing the government to accelerate the ground water pumping rate. In the 1970s, the use of non-renewable water resources was raised even further. A population explosion—from 6.2 million in 1970 to 16.2 million by 1990—led to a sharp increase in demand. Rapid urbanization also took its toll: While 2.7 million out of a population of 7.6 million Saudis lived in cities in 1974, the country's population had risen to 18 million by 1992 with only 3.8 million remaining in villages and peripheral areas.



Source: Toyobo company forecast to 2014, published 2007,

By the mid-1990s, the agricultural industry was responsible for 92 percent of total water consumption with 48 percent of that going to wheat. The sharp rise in water consumption for agriculture first began to take effect in the 1980s. In 1980, for example, the Saudis were consuming 2 billion cubic meters of water, but a mere three years later, consumption had already reached 7.2 billion cubic meters. This high consumption rate was also due to demographic changes in the kingdom, such as in Mecca, Riyadh, and Abha, and not exclusively as a result of increased agricultural needs.[6]

By 1993, the government began to realize what a heavy toll the agricultural sector had taken on its water resources. According to the Saudi Ministry of Agriculture, 140 billion cubic meters of water had been pumped from non-renewable water sources between 1980 and 1994, by which time there was significant depletion of drinking water resources in various parts of the kingdom as in the Tebrak area, which is about 95 kilometers from Riyadh and was one of Saudi Arabia's biggest sources of water. In other areas, such as the eastern province, water reservoirs dried up or became unavailable because of bad management, lack of sewage, and excess use of fertilizers, which contain high levels of toxic chemicals. All of these factors caused contamination of the water supply and resulted in a decrease of between 8-15 meters of ground water between 1980 and 1993.[7]

There were 26,000 wells in Saudi Arabia in 1982 and 52,500 by 1990. During this time, there was a marked increase in the use of non-renewable resources from aquifers such as those at Wajid, Saq, Tabuk, Minjur, Biyadh, Wasia, and Umm ar-Radhuma. Some measures were taken to reduce water consumption including the imposition of new water rates in 1994 in order to avoid wastage and excess consumption. Then in 2000, the government decreed that all private home owners and public establishments must install wastewater treatment apparatus.

These measures notwithstanding, Saudi Arabia continued to rank third in world water consumption at 248.7 liters per capita per day in 1993.[8] As a result, in 2005, the government began using desalinated water rather than water from non-renewable sources. Before then, 11,679 million cubic tons of water had been taken from non-renewable sources per year while only 8,000 million cubic tons of water came from renewable sources. As a result, neighboring countries such as Qatar, Jordan, and Iraq had begun to object to Riyadh's extensive use of shared ground water, which was depleting their own supplies.[9]

Sixty sewage collection disposal plants in the towns of Jeddah, Medina, and Khubar were established to supply 70 percent of the country's water between the early 1990s and the beginning of the twenty-first century. Riyadh also intends to establish forty wastewater treatment plants and to streamline water transportation pipelines. But there is a significant downside to these measures. Desalination plants are energy guzzlers, and depending on them takes a financial toll on governmental revenues accrued from oil and gas exports.[10]

The Roots of a Decision

As far back as 1993, Saudi government officials reported that water resources in the kingdom were dwindling, and yet Riyadh continued to opt for more investment in agriculture. What then were the considerations that motivated the House of Saud to continue subsidizing this project, despite deep financial and environmental losses?[11]

Some have contended that the policy was a misguided course of action derived from a sensible desire to reduce the country's number of foreign workers.[12] Unofficially, estimates are that seven million foreign individuals work in 80 percent of the private sector, making it difficult for native Saudis to find jobs.[13] Dependence on foreign workers has a direct impact on the economy: It is estimated to cause losses of billions of dollars every year because much of the derived income goes into the hands of foreigners who then transfer their wages to families outside the kingdom.

However, if recruiting native Saudis to the agricultural sector was a goal of these government subventions, the plan backfired. By the 1980s, most of the field workers were foreigners, and most farms were run by people of Egyptian, Omani, and East Asian origin. In addition, due to the gap between Saudi workers' abilities and industry requirements, more specialized work such as the operation of irrigation systems and advanced equipment were under the control of Westerners. Saudi citizens working in agriculture were mainly limited to positions in marketing and distribution.[14] Similar to the Saudi oil industry (which had been controlled by Western companies until 1980), large agricultural enterprises were established and run by outsiders. For example, Saad-co, a company that was operational in the 1990s, employed 450 workers, of whom 100 were Saudi, 60 American and European, and the rest from Asian countries.[15]

Others have pointed to a desire to diversify sources of revenue for the kingdom as key to the decision to invest so much in the agricultural sector. But an analysis of the contribution of the agricultural sector to the Saudi economy shows it to have consisted of 4.5 percent of the gross national product in 1975, 1.8 percent in 1986, almost 6 percent in 1998, and 4.2 percent in 2002.[16]

Instead, the roots of the Saudi decision must be found elsewhere. Surprisingly, it may be a result of the 1973 global oil crisis, ironically enough triggered by the Saudis' own behavior. The sharp rise in oil prices from that period produced an increase in the cost of agricultural goods from abroad, which in turn, persuaded the government to try to lessen dependence on foreign food sources. The government also feared the creation of an external food cartel that could arise in reaction to the Organization of the Petroleum Exporting Countries (OPEC) oil cartel. Alongside that, the closure of the Suez Canal between 1967 and 1975 raised transportation expenses and provoked fear that food supplies could be further disrupted. Moreover, a number of natural disasters that were detrimental to world wheat production occurred between 1970 and 1976—such as the deadly 1970 Bhola cyclone in east Pakistan as well as severe drought in Australia in 1972—and the Saudi government wanted to ensure that the country would not lack in food sources. With a rise in bread consumption due to the oil-induced economic boom and a 50 percent increase in Hajj pilgrims from 1980 to 1989, the Saudis needed more wheat as well as diversification of their food sources.[17]

Settling the Nomads

But perhaps the most significant factor behind the royal family's decision to subsidize and expand the agricultural sector lay in domestic, political considerations.

Before the establishment of the modern Saudi kingdom, 70 percent of society in the Arabian Peninsula was of a Bedouin tribal, nomadic nature. In that setting, tribal leaders controlled the lives of their clansmen in ways that were essentially inimical to a centralizing government. To some degree, even after the establishment of the kingdom, these leaders maintained their status for a time through political marriages, control over pasture lands, and acquiring administrative or army posts for their people. But to truly consolidate power, the central government decided it needed to settle these Bedouin nomads in the big cities and in permanent villages, thereby breaking their traditional tribal bonds.

Large areas of the Saudi desert have been turned into huge wheat fields although the country receives only about four inches of rain a year, one of the lowest rates in the world. The Saudi Grain Silos and Flour Mills Organization, established in 1972, is the government agency in charge of managing the kingdom's wheat program. In 2010, GSFMO expanded Saudi wheat storage capacity and is currently in the process of enlarging its wheat stocks in order to increase the country's strategic reserve.

It must be borne in mind that the House of Saud was not the long-time ruler of the peninsula and its members were in fact something of upstarts. Generous subsidies granted to farmers by the government would be suitable compensation for foregoing a previous nomadic life and drawing the beneficiaries of the Saudi largesse closer to the ruling house. A growing agricultural industry appealed to many Bedouin nomads because it meant that they would have access to pasturelands as well as a regular income and would be released from their rigid tribal structure. Indeed, while 25 percent of Saudi citizens were nomads in the 1970s, by 1989, fifteen years after the agricultural project began, only 3.8 percent of the population remained nomadic.[18]

Beginning in 1970, the Saudi government established a five-year plan to settle the Bedouin. The government not only granted subsidies to the agricultural sector, it also established authorities whose responsibility was to promote urban settlement. Between 1971 and 1974, for example, the government became increasingly involved in housing matters via the Real Estate Development Fund, which granted convenient loans to young people and to the financially disadvantaged who wanted to purchase homes. In 1975, the Ministry of Municipal and Rural Affairs was established to assist in the settlement of rural areas. By 1976, there was a wave of government-sponsored development in suburbs surrounding cities where the Bedouin cultivated their lands, including near Jeddah, Riyadh, Dammam, Ta'if, Abha, and Jizan, in which many nomadic families settled.[19]

A fundamental reason behind the determination to grant generous subsidies was the fear that the masses of Bedouins who had left their nomadic lifestyle would not have a steady income, and thus the subsidies aimed at avoiding social unrest amid the newly settled people. The royal family feared that it would lose its legitimacy if it could not provide a social and economic solution to accompany settlement.

Planning for the Future

Riyadh has not, however, entirely abandoned the agricultural sector abroad. In January 2009, King Abdullah announced the establishment of an "Initiative for Saudi Agricultural Investment" aimed both at cutting Saudi agricultural production and investing in countries that had agricultural potential but little financial means. The government announced an aid package worth $800 million for companies that invested in agriculture outside Saudi Arabia, pledging further support for the purchase of tractors and chemicals, the establishment of irrigation systems, and more in these countries. Thus, the government gave $95 million worth of aid to the Hail Agricultural Development Company (HADCO), a Saudi firm which operates in Sudan. The Saudis have also increased wheat imports from Europe, North America, Russia, and Ukraine, and, in 2010, began to expand the port of Jeddah where most of these imported agricultural goods arrive.[20]

Not everyone in Saudi Arabia was happy with King Abdullah's program. Some believed that discontinuing agricultural subsidies would, in the long run, be detrimental to those on society's margins.[21] There were also those who claimed that the cessation of subsidies could expose the kingdom to extreme fluctuations in the world food market[22] and create a balance of power that could cause conflict with agriculture-producing countries—mainly Germany, the United States, and France—which are dependent on OPEC oil exports. On that score, Riyadh joined the World Trade Organization (WTO) in 2005 and as such was obliged to stop subsidizing agriculture and import goods that are cheaper to produce elsewhere.[23] But WTO guidelines allow a country experiencing a food crisis to restrict its agricultural product exports, which could negatively affect the Saudi grain supply should such a crisis arise.

Still others asserted that discontinuing support for agricultural projects could cause a loss of public faith in future government attempts to diversify the Saudi economy.[24] Indeed, the king's pronouncement soon had repercussions: Following the announcement that the subsidies would end, 42 percent of the existing 9,231 Saudi agricultural companies closed down. Many agree that King Abdullah's decision has emphasized that the government attaches more importance to preserving water than to taking care of an agricultural sector that is likely to shrink significantly by 2016.[25]

Once the fundamental problem of water depletion was fully grasped and the decision made to stop subsidizing domestic wheat production, the Saudi government took concrete measures to both ensure its growing population's food security and develop other avenues to help farmers and land workers.[26] For example, the Saudi Grain Silos and Flour Mills Organization (GSFMO), established in 1972, is the government agency in charge of managing the kingdom's wheat program. In 2010, GSFMO expanded Saudi wheat storage capacity and is currently in the process of enlarging its wheat stocks in order to increase the country's strategic reserve and move it closer to its annual wheat consumption by the end of 2015. It has also announced that there would be an increase in reserves from six to twelve months of consumption by 2016.[27]

Saudi Arabia has built additional grain silos to store a 12-month reserve to counter the threat of supply disruptions. With the decision to stop domestic grain production in 2016, most of the new silos will be built closer to ports in order to receive imports.

Over the past few years, several new wheat silo projects have been initiated. By December 2015, these storage facilities are slated to yield additional wheat storage capacity of about 3.7 million tons (MT) on top of current GSFMO silos that have a combined storage capacity of 2.8 MT.[28] GSFMO also signed contracts to build five additional storage projects in Mecca, Jazan, Hasa, and Qasim with a combined storage capacity of 790,000 MT, which were to be operational by the end of 2014.[29] Storage silos may not be cheap to build and manage, but they are still much less expensive than growing cereal in such a harsh climate. Annual storage costs for wheat in Saudi Arabia are about $70 million, a minute figure in comparison to the cost of production subsidies, estimated at around $5 billion a year in 1984-2001.[30]

Critics, however, point to the fact that most of Saudi Arabia's current silos were originally designed to receive domestic crops and are thus located inland; of the 2.5 MT of current silo capacity, 90 percent is located in those regions. Silo location has a direct link to cost efficiency as high transportation costs will need to be offset somehow and perhaps shifted to the consumer.[31] With the decision to stop domestic grain production in 2016, most of the new silos will be built closer to ports in order to receive imports.[32] But even with plans to expand silos near Jeddah and Jazan, close to 80 percent of silo capacity will still remain for the time being in the interior of the kingdom. Others maintain that a 12-month reserve is more than is necessary even with the threat of supply disruptions.[33] There is also the difficult task of rotating such a large number of grain stockpiles to and from different locations as an inability to do so could result in stock spoilage.[34]

While looking to ensure food security for the kingdom, the government has also sought to maintain a stable social fabric that has the potential of fraying in the absence of water subsidies and a dramatic shift in domestic food production goals. It has promoted new water technologies such as drip irrigation systems and enhanced water use efficiency. Saudi agronomists are encouraging farmers to include more sustainable agriculture methods and crops. Different types of xerophytes—plants that are adapted to desert climates—have been introduced with the hope of future commercial potential from their fruits. These crops can offer new ways for farmers in arid areas to earn a living.[35]

Educational and extension programs are a significant part of the Saudi equation. Stressing the importance of these initiatives will raise awareness of the importance of water conservation among growers. Providing farmers with crucial research information[36] will help with the challenges the internal agricultural industry is facing such as low soil fertility and the need for environmental protection.[37] Thus, King Saud University in Riyadh established an agricultural extension center in May 1990. This is the only academic program of its kind in the entire gulf region and offers a degree in agricultural extension and rural development.[38]

In terms of the social dimensions and the challenges faced there, recent estimates indicate that only about 15 percent of the Saudi population still lives in rural areas. Riyadh feels it is of great importance to keep a balanced ratio of rural to urban population. If such a balance can be reestablished, it will alleviate pressures on the big cities and ease the delivery of essential services to the entire population.[39]

To many Saudis, rural areas epitomize something of a past golden age, and preserving them and their inhabitants is seen as a form of protecting a national heritage. The exodus of farmers to the cities is perceived as a loss, and agricultural education and farm extension programs may stem that loss. Rural industries such as herbal medicine, bee keeping, and sheep and goat rearing can continue with the assistance of modern technology. These initiatives may help make living in rural areas more inviting and economically feasible so that more people return to their ancestral farming communities.[40] In doing so, the Sauds will have made sure not only that the food supply is ensured but that society is secure and balanced as well. These decisions, combined with the Arab upheavals that have cascaded throughout the region since late 2010, gave Riyadh cause to consider its food security, more specifically, the challenge of securing wheat, the main source of sustenance for its people. The recent uprisings highlighted the problems for the Saudis that can arise concerning protection of this main food source if the correct measures were not taken and expedited solutions were not devised.[41]

Conclusions

The Saudi attempt to develop its own, internal agricultural industry to ensure food security was considered by many destined to fail from the outset. Indeed, subsidizing the agricultural industry had a devastating effect on the country's water supply as well as a negative impact on the economy as a whole.

Yet, despite the failure to guarantee food security from domestic sources, the project did have positive effects by providing employment for the hundreds of thousands of Bedouins who had abandoned their traditional, itinerant lifestyle because of the country's rapid urbanization. In the long term, the Saudi government was forced to look for other solutions for the food security challenge, notably purchasing lands abroad and creating food stockpiles that could reduce the challenge in any future food crisis.

▶ **Notes are available at source's URL.**

Yossi Mann, a lecturer in the department of Middle Eastern Studies at Bar-Ilan University, studies issues related to oil and gas industries in the Middle East.

Water scarcity a contributing cause of wars, terrorism in Middle East, North Africa

Source: http://www.homelandsecuritynewswire.com/dr20150401-water-scarcity-a-contributing-cause-of-wars-terrorism-in-middle-east-north-africa

Apr 01 – **Water scarcity driven by overuse, poor land management, and climate change, is one of the causes of wars and terrorism in the Middle East and North Africa. If governments fail to respond, shortages of major resources, including food and energy, will cause greater insecurity and conflict.**

The United Nations (UN) defines a region as water stressed if the amount of renewable fresh water available per person per year is below 1,700 cubic meters. A region is experiencing water scarcity if the figure is below 1,000 cubic meters, and below 500 amounts to "absolute water scarcity."

Between 2003 and 2009, the Tigris-Euphrates basin comprising Turkey, Syria, Iraq, and western Iran "lost groundwater faster than any other place in the world except northern India." The *Ecologist* reports that about 117 million acre-feet of stored freshwater were lost due to reduced rainfall and poor water management. If this trend continues, "trouble may be brewing" for the region.

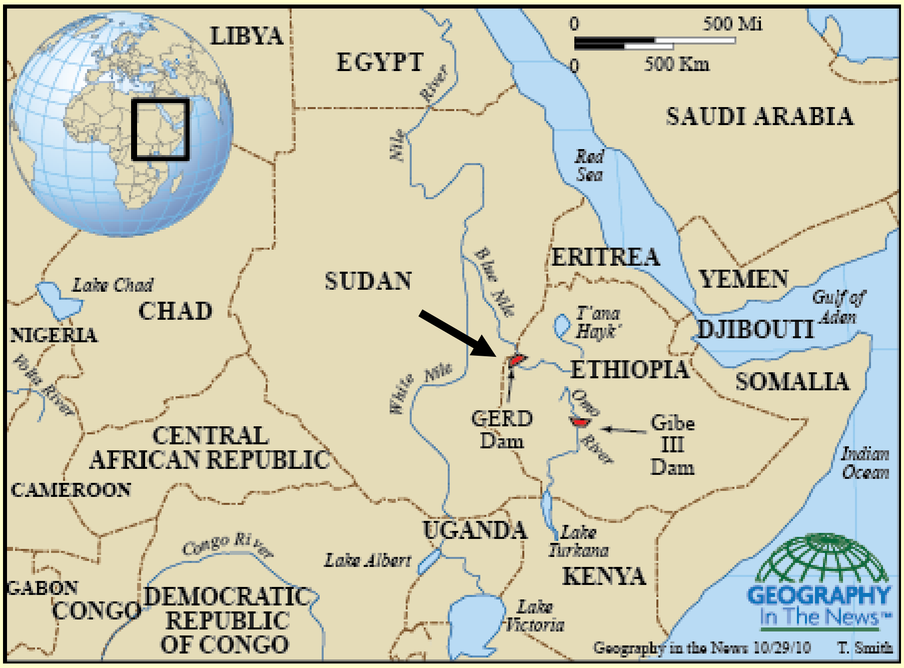
A study in the *Journal of the American Water Works Association* (AWWA) reports that countries already experiencing water stress or far worse include Egypt, Jordan, Turkey, Iraq, Israel, Syria, Yemen, India, and China. Many of these countries are experiencing civil unrest and lack of access to water is playing a major role in sectarian violence.

Before Syria's civil war began, 60 percent of the country experienced a drought that led over a million mostly Sunni farmers to migrate to coastal cities dominated by the Alawite sect. The migration fueled tensions that eventually contributed to the current cycle of civil unrest and violence. Water security experts have also noted water scarcity as a key driver in the inter-tribal and sectarian conflicts in Yemen.

Water management expert Roger Patrick, author of the AWWA study, observes that Yemen is consuming water faster than it is being replenished. He notes that even the 2011 uprising in Egypt was partly initiated by spikes in grain prices caused by "droughts in major grain-exporting countries" like Australia, triggered by climate change.

TURKEY
CASPIAN SEA
SYRIA
IRAN
Euphrates
Tigris
IRAQ
PERSIAN GULF

Furthermore, **the construction of the Grand Ethiopian Renaissance Dam (GERD) could threaten Egypt's access to the Nile River, which supplies 98 percent of the country's water supply.** As Egypt's population is estimated to double to 150 million by 2050, future unrest and conflict between Ethiopia and Egypt over access to the Nile seems inevitable, especially since Ethiopia's dam would reduce the capacity of Egypt's Aswan Dam by 40 percent.



With proper management and cooperation with regional partners, governments facing water scarcity can avoid conflict. The Israeli government has been able successfully to cooperate with Jordan on their shared water resources for years through a combination of efficient water management methods and desalination technologies. Neighboring Gaza, however, could become "unlivable" according to the UN, due to its worsening water crisis, amplified by discriminatory policies, including Israel's effective forced privatization of the Palestinian water supply. The Israel-Gaza case shows that while efficient water management and distribution methods can offset water crises, inequalities and repressive government policies "can be a precursor to social breakdown and violent conflict."

— Read more in Roger Patrick, "When the Well Runs Dry: The Slow Train Wreck of Global Water Scarcity," Journal of the American Water Works Association 107, no. 3 (March 2015): 65-76

California imposes first mandatory water restrictions in state history

Source: http://www.homelandsecuritynewswire.com/dr20150402-california-imposes-first-mandatory-water-restrictions-in-state-history

Apr 02 – **Standing on a patch of brown grass in the Sierra Nevada mountains, which is usually covered with several feet of snow at this time of the year, California governor Jerry Brown announced the first mandatory water restrictions in state history.** "Today we are standing on dry grass where there should be five feet of snow," Brown said yesterday. "It's a different world… we have to act differently."

Brown directed the state Water Resources Control Boardto implement rules which would reduce water usage by 25 percent. The savings would amount to 1.5 million acre-feet of water over the next nine months. **According to the *Los Angeles Times*, Brown's orders would:**

- Require golf courses, cemeteries, and other large landscaped spaces to reduce water consumption.
- Replace fifty million square feet of lawn statewide with drought-tolerant landscaping as part of a partnership with local governments.
- Create a statewide rebate program to replace old appliances with more water- and energy-efficient ones.
- Require new homes to have water-efficient drip irrigation if developers want to use potable water for landscaping.
- Ban the watering of ornamental grass on public street medians.

- Call on water agencies to implement new pricing models that discourage excessive water use.
- Require the agriculture sector to report more water usage information to the state so that regulators can better find waste and improper activities.
- Create a mechanism to enforce requirements that water districts report usage numbers to the state.

The Sierra Nevada Mountains collect snow during the winter and release water or moisture during the spring as snow melts. The water is then collected in lakes and ponds which are controlled with dams. *The Washington Post* reports that the snow levels in the Sierra Nevada have declined each month since manual surveying began on 30 December 2014. That first reading showed the snow's water content was 50 percent of normal for the date. Thirty days later, the water content was 25 percent of normal, and in March it was 19 percent of normal. Electronic readings taken earlier this week across the Sierra Nevada show the snow's water content at about 5 percent of normal levels.

Thirty percent of California's water supply comes from the snowpack, so less snow means less snowmelt, which means less water. "It is such an unprecedented lack of snow," said Frank Gehrke, chief of snow surveys for the California Department of Water Resources (DWR).

Other water sources, including reservoirs and rainfall totals, have improved, but the state's snowpack replenishes California's reservoirs, so no snow means there will be no runoff this spring or summer when the rain stops and temperatures rise.

"This is sort of uncharted territory," said DWR spokesman Doug Carlson, calling the situation "dismal."

California's rainfall since the current water year began in October 2014 has helped refill the state's reservoirs. Lake Oroville delivers water from Northern California to the south and as of Monday was at 51 percent capacity, from 49 percent a year ago. Lake Shasta, the state's largest reservoir, had 150 billion gallons more water in it Monday than it did a year ago.

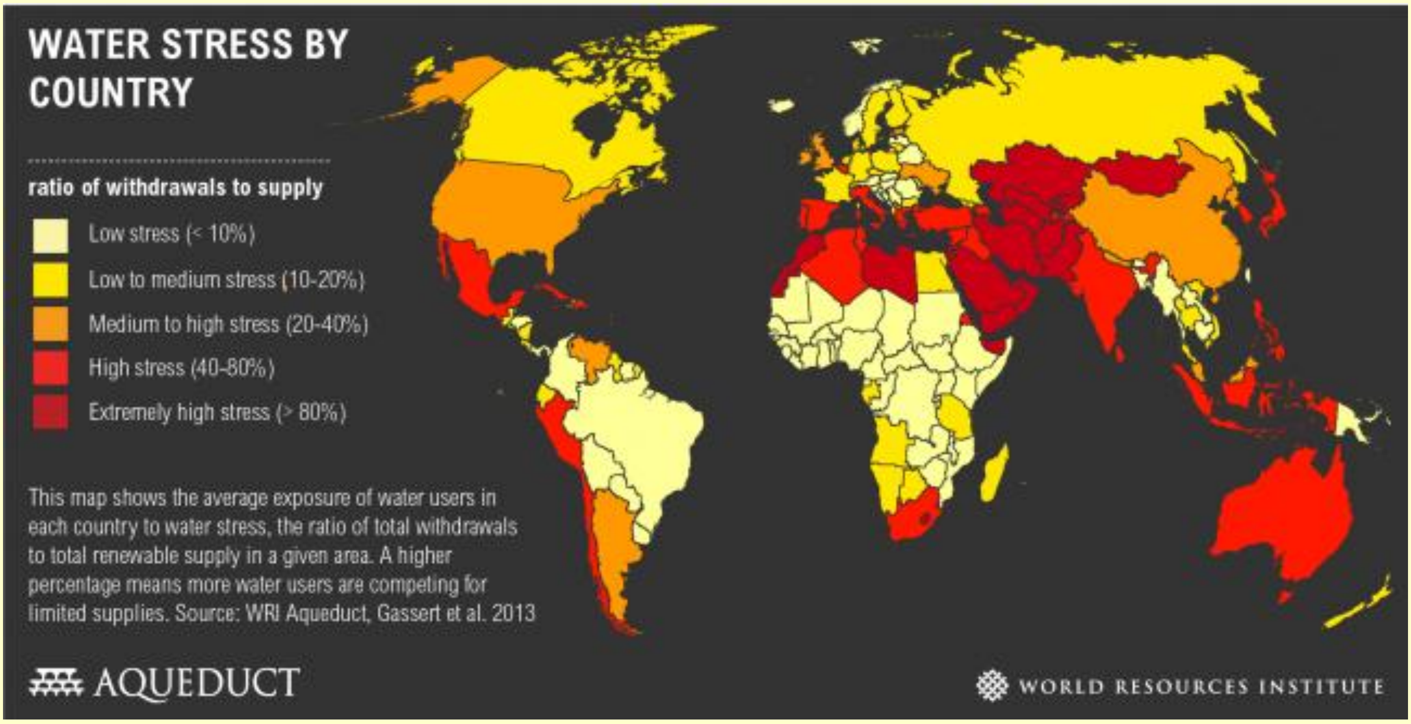
This unpredictable situation might offer a glimpse of California's new normal, with the current drought expected to worsen, along with the effects of climate change. "It does leave questions about where the water will come from," Carlson said. "Will there be enough of it? It will probably have to come from groundwater again … and that brings in a whole other set of problems and complications since the groundwater seems to be over-tapped."

Animated map of what Earth would look like if all the ice melted

Source: http://www.businessinsider.com/what-earth-would-look-like-if-ice-melted-world-map-animation-2015-2#ixzz3XAOGwW00

Water Stress by Country

Source: http://www.wri.org/resources/charts-graphs/water-stress-country



WATER STRESS BY COUNTRY

ratio of withdrawals to supply
Low stress (< 10%)
Low to medium stress (10-20%)
Medium to high stress (20-40%)
High stress (40-80%)
Extremely high stress (> 80%)
AQUEDUCT
WORLD RESOURCES INSTITUTE

This map shows the average exposure of water users in each country to water stress, the ratio of total withdrawals to total renewable supply in a given area. A higher percentage means more water users are competing for limited supplies. Source: WRI Aqueduct, Gassert et al. 2013

This map shows the average exposure of water users in each country to baseline water stress, the ratio of total withdrawals to total renewable supply in a given area. A higher percentage means more water users are competing for limited water supplies.

Our analysis finds that 37 countries currently face "extremely high" levels of water stress, meaning that more than 80 percent of the water available to agricultural, domestic, and industrial users is withdrawn annually.

EDITOR'S COMMENT: California (US) is already in red!

San Diego to build largest ocean desalination plant in Western Hemisphere

Source: http://www.homelandsecuritynewswire.com/dr20150416-san-diego-to-build-largest-ocean-desalination-plant-in-western-hemisphere

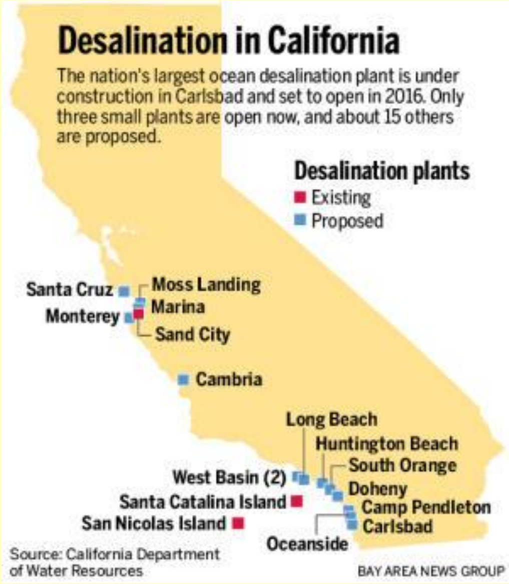
Apr 16 – San Diego County, California will soon become home to a $1 billion desalination plant which would supply drinking water to residents currently having to cut their water consumption by as much as 25 percent in response to the state's current drought. Small ocean desalination plants already operate throughout the state, but the facility being built in San Diego will be the largest ocean desalination plant in the Western Hemisphere, producing roughly fifty million gallons of drinking water a day.

Supporters of desalination say the technology has improved over the past twenty years. Desalinated water can cost twice as much as conventionally treated water, but it is still less than a penny a gallon.

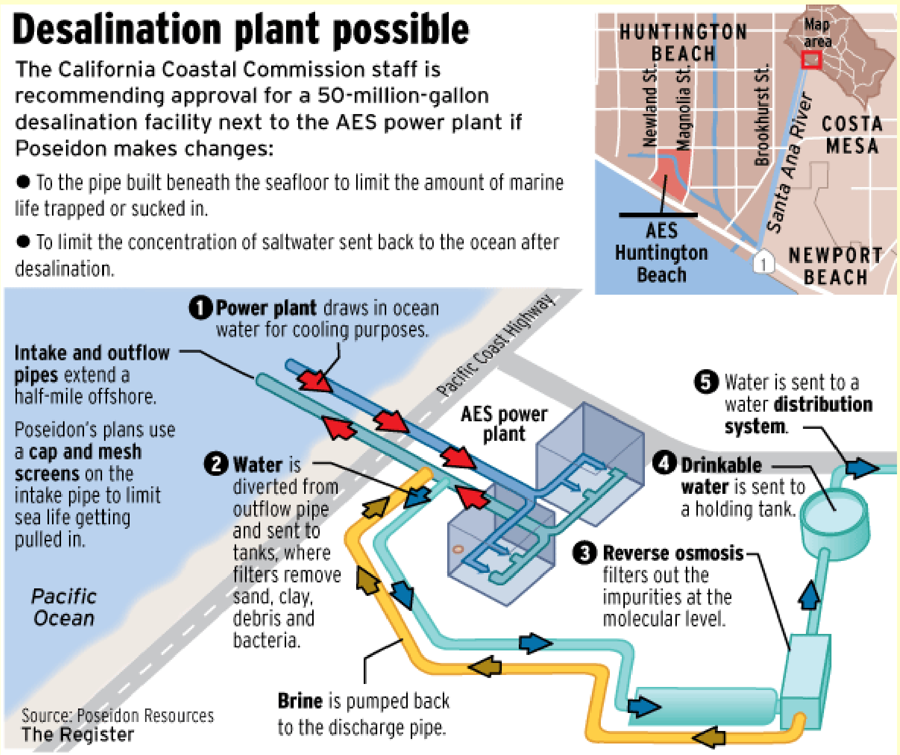
According to the *New York Times*, there are more than 15,000 desalination plants around the world, though many are small and treat brackish groundwater. Large plants focused on seawater are rare, but a few exist in the Middle East. Israel will soon get half its water from desalination. Israeli engineers have actually become sought-after partners in many desalination projects and are involved in the San Diego facility.

"It was not an easy decision to build this plant," said Mark Weston, chairman of the San

Diego County Water Authority. "But it is turning out to be a spectacular choice. What we thought was on the expensive side ten years ago is now affordable."


Desalination in California
The nation's largest ocean desalination plant is under construction in Carlsbad and set to open in 2016. Only three small plants are open now, and about 15 others are proposed.
Desalination plants
🟥 Existing
🟦 Proposed
Santa Cruz
Monterey
Moss Landing
Marina
Sand City
Cambria
Long Beach
Huntington Beach
South Orange
West Basin (2)
Doheny
Santa Catalina Island
Camp Pendleton
San Nicolas Island
Carlsbad
Oceanside
Source: California Department of Water Resources
BAY AREA NEWS GROUP

San Diego County currently depends on imported freshwater supplies from the Colorado River and Northern California. Water bills average about $75 a month, and the new plant is estimated to increase monthly bills by $5 to secure a new supply equal to about 7 or 8 percent of San Diego County's water consumption. The technology being implemented in San Diego is called reverse osmosis, which involves forcing seawater through a membrane with holes small enough that the water molecules can pass through but large salt molecules cannot.


Desalination plant possible
The California Coastal Commission staff is recommending approval for a 50-million-gallon desalination facility next to the AES power plant if Poseidon makes changes:
● To the pipe built beneath the seafloor to limit the amount of marine life trapped or sucked in.
● To limit the concentration of saltwater sent back to the ocean after desalination.
HUNTINGTON BEACH
Map area
Newland St.
Magnolia St.
Brookhurst St.
Santa Ana River
COSTA MESA
AES Huntington Beach
1
NEWPORT BEACH
1 Power plant draws in ocean water for cooling purposes.
Pacific Coast Highway
Intake and outflow pipes extend a half-mile offshore.
Poseidon's plans use a cap and mesh screens on the intake pipe to limit sea life getting pulled in.
AES power plant
5 Water is sent to a water distribution system.
2 Water is diverted from outflow pipe and sent to tanks, where filters remove sand, clay, debris and bacteria.
4 Drinkable water is sent to a holding tank.
3 Reverse osmosis filters out the impurities at the molecular level.
Pacific Ocean
Brine is pumped back to the discharge pipe.
Source: Poseidon Resources
The Register

An enormous amount of energy is required to create enough pressure to shove the water through the membranes. The energy use of desalination plants have been cut in half from twenty years ago, but operating the San Diego plant will still require large amounts of electricity, which will increase the carbon dioxide emissions that cause global warming, further straining existing fresh water supplies. Poseidon Water is developing the plant and has promised to counter the environmental damage by paying into a California program that finances projects to offset emissions of greenhouse gases.

Still, some environmental groups and scientists remain skeptical, saying that should California's drought conditions end, the desalination plant would become useless. They point to a desalination plant built in Santa Barbara about twenty-five years ago that promptly shut down when rains returned to the region. Australia has built six large desalination plants during a drought period and four of them remain idle, leaving customers with several billion dollars' worth of construction bills.

"Our position is that seawater desalination should be the option of last resort," said Sean Bothwell, an attorney with the California Coastkeeper Alliance, an environmental coalition that has battled California's turn toward desalination. "We need to fully use all the sustainable supplies that we have available to us first."

Other environmental concerns include the intake of saltwater and the disposal of excess salt into the Pacific Ocean, both harmful to sea life. Collecting large amounts of seawater, for example, can kill fish eggs and larvae by the billions. Embracing desalination, environmentalists argue, represents a failure to manage freshwater supplies effectively. They want the San Diego water agency to stress water conservation and the reuse of existing supplies.

Weston, the head of the local water authority, said since 1990, says his agency has cut county water use by 12 percent, even as population has increased by 30 percent. The region helped pioneer water conservation measures including low-flow bathroom fixtures and more efficient washing machines.

Conservation alone is not enough, Weston said. His agency decided years ago, before the current drought began, to move forward on the desalination plant.

Peter MacLaggan, a vice president of Poseidon Water who is overseeing the project, said the desalination plant has been of interest to locals. “Every time California has a drought, we get letters to the editor pointing out that there’s a lot of water in the Pacific Ocean,” he said. “They say, ‘Hey, guys, what are we waiting for?’”

7 Risks That Are Making Climate Change Into One of the Biggest Security Threats of the 21st Century

Source: http://www.huffingtonpost.com/lukas-ruettinger/7-risks-that-are-making-climate-change-into-one-of-the-biggest-security-threats-of-the-21st-century_b_7078826.html

Climate change is advancing. Its effects can be felt already today and will increase significantly in the coming decades even if the global community sets ambitious targets for reducing emissions at the end-of-year climate change negotiations in Paris.

On behalf of the G7 foreign ministries, an international research consortium from Germany, France, Great Britain and the USA, led by the Berlin-based think tank adelphi, analysed what this means for global security and the fragility of states and communities. The findings were published in the report "A New Climate for Peace -- Taking Action on Climate and Fragility Risks."

Climate impacts are intensifying crises and conflicts around the world

One central finding is that there are no "climate wars," as some experts claim. Not today and, as far as we know, not tomorrow. Instead of wars directly caused by climate change, we are increasingly being confronted with crises and conflicts that are intensified by climate change.

In particular, states that lack legitimacy and are struggling with weak government institutions will find it difficult to manage the combined and increasing pressure of climate change, population growth, uncontrolled urbanisation, increasing resource consumption, unequal economic development, and environmental degradation.

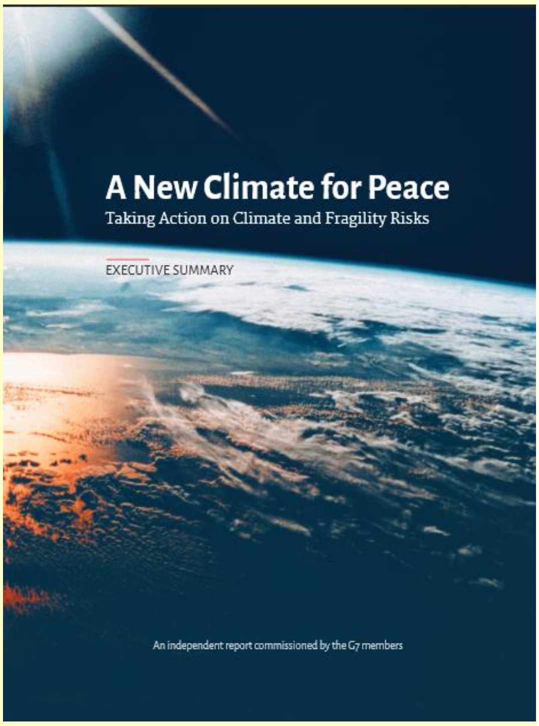
These combined stressors and pressures can lead to political instability and conflicts. The breakdown of states and societies threatens to cause a downward spiral of increasing fragility. Although the exact strength of the current effects of climate change is a hotly debated topic, the following examples give an indication of what the future could look like:

Syria: Between 2006 and 2011 Syria suffered a serious drought destroying many people's livelihood, especially in rural areas: Almost 75 percent of Syria's farmers lost their harvest. Many fled to the cities and the government failed to respond to the resulting humanitarian crisis. Pressures bubbled over as a result of the influence of the Arab Spring, combined with grievances towards the authoritarian regime that had built up over the years.

Thailand: Heavy monsoon rains in 2011 led to flooding in 26 provinces, which affected two million people. The political landscape was already fragile after violent protests between 2008 and 2010. Many considered the government's attempts at managing the disaster to be misguided and inequitable. Hundreds of people protested the unfair distribution of aid supplies and the protests continued until a military coup occurred in 2013.

At the foundation of these and many similar examples are seven compound risks. These risks have been expounded on in detail in the report and are meant to bring future crises into sharper focus for foreign policy makers:

1. **Local resource competition:** As the pressure on natural resources increases, competition can lead to instability and even violent conflict in the absence of effective dispute resolution.
2. **Livelihood insecurity and migration:** Climate changes will increase the human insecurity of people who depend on natural resources for their livelihoods, which could push them to migrate or turn to illegal sources of income.
3. **Extreme weather events and disasters** will exacerbate fragility challenges and can increase people's vulnerability and grievances, especially in conflict-affected situations.
4. **Volatile food prices and provision:** Climate change is highly likely to disrupt food production in many regions, increasing prices and market volatility, and heightening the risk of protests, rioting, and civil conflict.
5. **Transboundary water management:** Transboundary waters are frequently a source of tension; as demand grows and climate impacts affect availability and quality, competition over water use will likely ncrease the pressure on existing governance structures.
6. **Sea-level rise and coastal degradation:** Rising sea levels will threaten the viability of low-lying areas even before they are submerged, leading to social disruption, displacement, and migration, while disagreements over maritime boundaries and ocean resources may increase.
7. **Unintended effects of climate policies:** As climate adaptation and mitigation policies are more broadly implemented, the risks of unintended negative effects - particularly in fragile contexts - will also increase.


A New Climate for Peace
Taking Action on Climate and Fragility Risks
EXECUTIVE SUMMARY
An independent report commissioned by the G7 members

These seven compound risk factors interact in complex ways and extend across borders: for example transboundary water conflicts can disrupt local livelihoods and extreme weather events in the USA and Russia can lead to food insecurity in Egypt. It is therefore not sufficient to address these risks separately. Moreover, when policies and problem-solving approaches ignore the interdependent and systemic nature of climate-fragility risks, they can even exacerbate these risks.

nterdependent risks require cross-sectoral and integrated answers that break out of the silos of climate, development and peace policy.

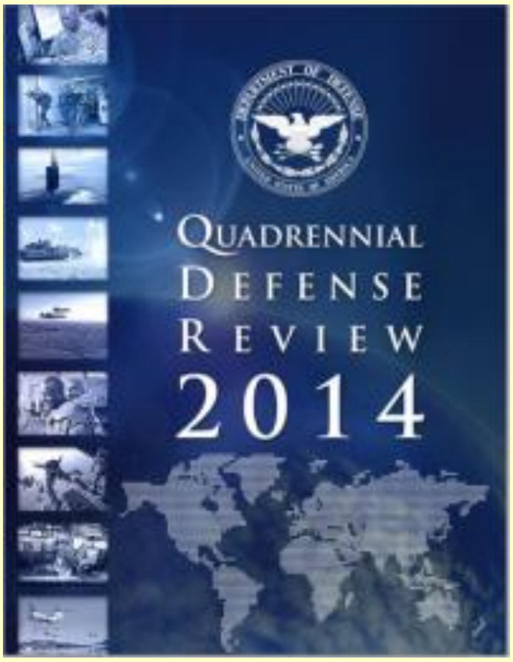
▶ **Read the report at:** http://www.newclimateforpeace.org/sites/default/files/NewClimateforPeace_ExecutiveSummary.pdf

The New Sponsor of Terrorism: Climate Change

By Jon Soltz

Source: http://www.huffingtonpost.com/jon-soltz/the-new-sponsor-of-terrorism-climate-change_b_7108492.html

For years, we have been warned that climate change would lead to a less stable world, with some very serious implications for the United States, its military, and its security. Beginning in 2010, in its Quadrennial Defense Review, the Pentagon warned that while climate change "alone does not cause conflict, it may act as an accelerant of instability or conflict, placing a burden to respond on civilian institutions and militaries around the world."



This was followed up in 2014, when the Pentagon once again warned that the effects of climate change are "threat multipliers that will aggravate stressors abroad such as poverty, environmental degradation, political instability, and social tensions - conditions that can enable terrorist activity and other forms of violence."

Finally, this year, a groundbreaking study concluded that the Zero Hour had come. Climate change, indeed, contributed to conditions that hastened the rise of extremism, in the form of ISIS, in Syria.

From the *Scientific American* article covering the study:

"Drying and drought in Syria from 2006 to 2011--the worst on record there--destroyed agriculture, causing many farm families to migrate to cities. The influx added to social stresses already created by refugees pouring in from the war in Iraq, explains Richard Seager, a climate scientist at Columbia University's Lamont-Doherty Earth Observatory who co-authored the study. The drought also pushed up food prices, aggravating poverty. "We're not saying the drought caused the war," Seager said. "We're saying that added to all the other stressors, it helped kick things over the threshold into open conflict. And a drought of that severity was made much more likely by the ongoing human-driven drying of that region."

It isn't that tough to imagine other potential hot spots. We already have documented evidence of increased migration from Pakistanis, who are moving from ground that has become less fertile due to climate change. **The 2014 QDR found that,** "the pressures caused by climate change will influence resource competition while placing additional burdens on economies, societies, and governance institutions around the world." Indeed. What happens when areas of Pakistan continue to dry up? Already home to terrorist activity, resource shortages and tensions with India could hasten the growth of terror networks. Think it sounds like some environmentalist scare tactic?

It's already happening: "Extremist groups, of which there is no dearth in Pakistan, have also weighed in on the matter, using it as an opportunity to garner support for their movement. Hafiz Saeed, the founder of the militant group, Lakshar-e-Taiba--the organization behind the 2008 Mumbai attacks--has unequivocally blamed India for Pakistan's water crunch, accusing its government of committing "water terrorism." By evoking an issue that is sensitive to millions of Pakistanis, Saeed's rhetoric demonstrates the potential of militant groups to exploit this issue."

As someone who has served in the Iraq war, and has had to help fight terrorists there, I can tell you unequivocally, this is not a path we want to go down. We have the best military in the world, but as we saw, it became strained by fighting two wars at once. I have seen what three, four, and five deployments have done to our force structure, and readiness, and it is not good. If terror networks accelerate their growth, aided by climate change, our military may reach its breaking point, trying to contain the spread of terrorism and upheaval it causes. This doesn't even take into account all of the humanitarian aid our military would have to provide to the millions who would be suffering.

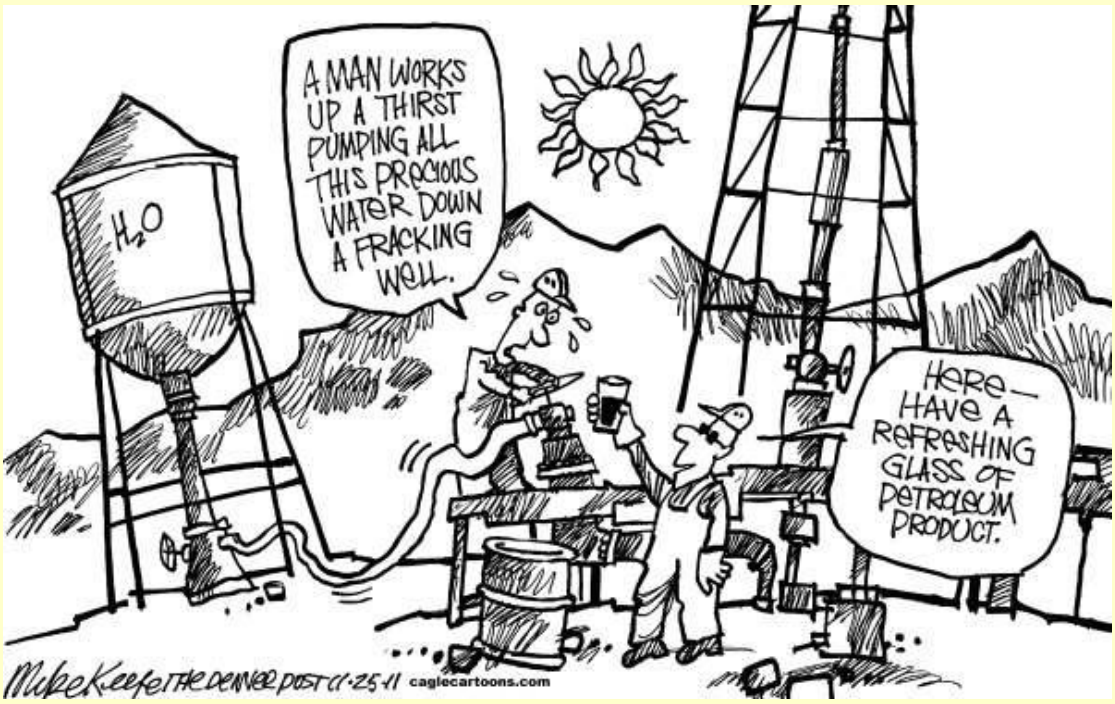
And, with every bit of terrorist growth, America would become more at risk of attack.

Still, we have another choice. To slow the pace of climate change, with an eye towards stopping it, in the long run. That will mean serious, drastic action. It will mean expanding the use of carbon-free forms of energy, from wind and solar, to better hybrid and electric vehicles, and protecting the Renewable Fuel Standard, used in our current fuel supply, which lessens the amount of money that flows to terrorist groups, who shoot at our troops. It will not be easy. And it will not be cheap.

But think of it this way. When we find out someone is sponsoring terrorism, we act. We freeze funds. We sanction them. And, rightly or wrongly, we sometimes even strike at them with drones. We act, and we act decisively. Why wouldn't we act the same way against this foe?

Today, on Earth Day, let's continue to protect ourselves, and ask our politicians to vote for policies that protect us. Included in that is a campaign to defeat the newest sponsor of terrorism -- climate change.

***Jon Soltz** is the Co-Founder and Chairman of the 400,000+ supporter veterans group, VoteVets.org. He served twice in Iraq -- in 2011 as a Major, helping train the Iraqi Army prior to the removal of US Troops, and in 2003, as a Captain during Operation Iraqi Freedom, deploying logistics convoys with the 1st Armored Division. In 2000 he served as a tank Platoon Leader in the Kosovo Conflict. Soltz is a graduate of Washington & Jefferson College with a dual degree in Political Science and History and a 2010 graduate of the University of Pittsburgh's Graduate School of Public and International Affairs.*


A MAN WORKS UP A THIRST PUMPING ALL THIS PRECIOUS WATER DOWN A FRACKING WELL.
HERE— HAVE A REFRESHING GLASS OF PETROLEUM PRODUCT.
H₂O
MikeKeefe THE DENVER POST 11·25·11 caglecartoons.com

Frequently asked questions on Business Continuity Management

Source: http://www.resilienceguard.ch/faq/

What is Business Continuity Management (BCM)?

Business continuity management (BCM) is the holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause. It provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. *(Source: ISO 22301:2012)*

Truly effective business continuity management will go beyond organisational boundaries to encompass the supply chain and ensure a key supplier's failure does not affect your own business in terms of service interruption or reputational damage.

How will it benefit my business?

An effective business continuity management programme will result in many proven business benefits including the ability to:

- Identify and manage current and future threats to your business
- Take a proactive approach to minimising the impact of incidents
- Keep critical functions up and running during times of crisis
- Minimise downtime during incidents and improve recovery times
- Demonstrate resilience to customers, suppliers and for tender requests

Why isn't Risk Management enough?

Risk management is a complementary discipline to business continuity management (BCM) and in some cases the two can overlap.

Having said that, there is a huge difference in what each discipline achieves. For example, while risk management involves mapping risks into a risk matrix and developing a mitigation plan and strategy for each threat, business continuity goes further. Critical activities are objectively identified, planned for and tested so that when a potential risk identified in the matrix materialises your organisation knows what to do about it. A BCM programme ensures the organisation has tried and tested procedures in place that will keep the business running, from the point the issue is identified through crisis management and successful recovery of affected operations.

In short, business continuity builds upon the foundation of risk management, hugely enhancing your response to incidents and helping to make your organisation resilient.

What is the difference between a Business Continuity plan (BCP) and a Business Continuity Management System (BCMS)?

First of all, a plan is just a piece of paper – if not acted upon it is worthless. That is why people are at the very heart of a business continuity management system (BCMS).

A business continuity plan (BCP) is the first step towards resilience whereas a well-established and certified BCMS is an ongoing management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Implementing a BCMS is a decision that will affect every single area of the organisation and, as such, requires senior management commitment and support.

I already have Disaster Recovery arrangements in place. Is my business safe?

The short answer is 'no'. That's because disaster recovery is the process by which an organisation resumes business *after* a disruptive event. The event might be something huge-like an earthquake, tsunami or major terrorist attack – or something small and localised like malfunctioning software caused by a computer virus or a power failure.

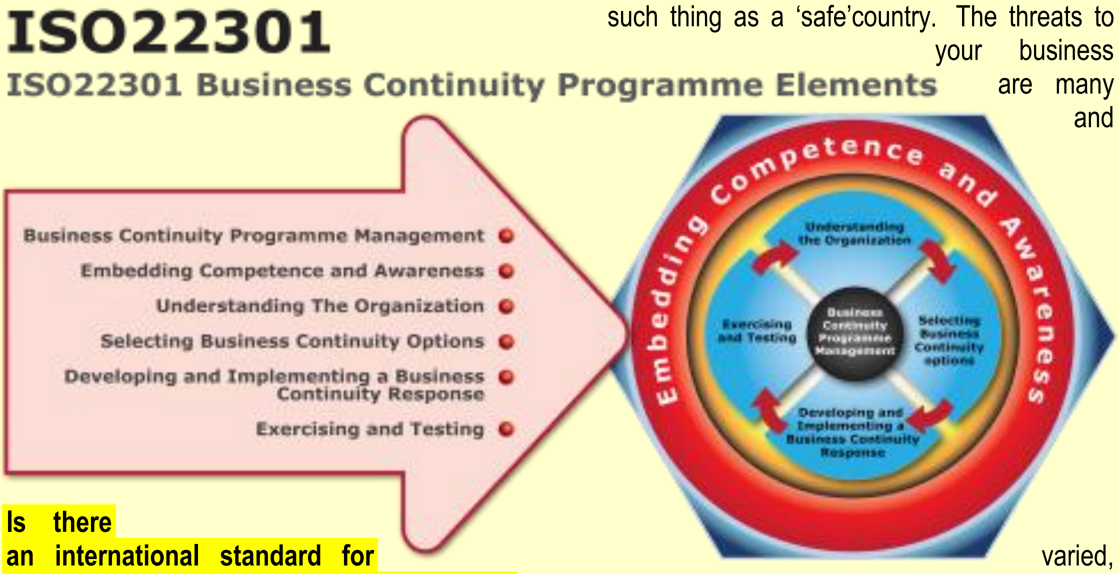
If you have adequate disaster recovery provision in place and are able to get back to business as usual fairly quickly you are likely to survive without too much lost business, too many customers defecting to competitors and too much harm to your reputation. However, this isnot the same as resilience, which means having the ability to withstand potentially disruptive events without any interruption to services in the first place.

Do I have to implement everything in one go?

Obviously, the sooner you are able to implement any business continuity recommendations that have been made, the sooner your business will be protected. However, in the real world budgetary and resource constraints mean it is not always possible to achieve everything in one hit. For this reason, Resilience Guard takes a phased approach, prioritising the work to be done in terms of urgency and available budget.

How much time will I need to implement a full scale Business Continuity Management System (BCMS)?

The timescale will very much depend on the complexity and size of the organisation. Typically, SMEs that do not have a dedicated BCM team but contract professional consultancy support, should be in a position to apply for certification within around 12-18 months, while for medium-sized and large international organisations with visible senior management commitment this could extend to 18-24 months.


ISO22301
ISO22301 Business Continuity Programme Elements
Business Continuity Programme Management
Embedding Competence and Awareness
Understanding The Organization
Selecting Business Continuity Options
Developing and Implementing a Business Continuity Response
Exercising and Testing
Embedding Competence and Awareness
Understanding the Organization
Exercising and Testing
Business Continuity Programme Management
Selecting Business Continuity options
Developing and Implementing a Business Continuity Response

Is there an international standard for Business Continuity Management (BCM)?

Yes. ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements is the internationally recognised standard and builds on the success of the British Standard BS 25999 and other regional standards. It's designed to protect organisations from potential disruption. This includes extreme weather, fire, flood, natural disaster, theft, IT outage, staff illness or terrorist attack. The ISO 22301 management system helps organisations identify threats relevant to their business and the critical business functions they could impact. And it allows you to put plans in place ahead of time to ensure the business doesn't come to a standstill.

Can I get a certification for my Business Continuity Management System?

The publication of ISO 22301 in May 2012 enables organisations to gain an independent seal of approval for their business continuity management system. This shows customers, suppliers, employees, investors and all other stakeholders they can be confident your company can successfully manage incidents and minimise business disruption.

Commercially, it can give your organisation a competitive advantage, demonstrating to your valuable customers that the products and services they rely on will always be available when they need them.

My business is located in a safe country. So why do I need Business Continuity Management?

In today's interconnected world, there is no such thing as a 'safe'country. The threats to your business are many and varied, and only some are geographic risks. Even if you can be absolutely confident that the country in which you're located has plentiful supplies of energy, skilled workers and reliable infrastructure, there is still the threat of staff shortages, denial of access to your premises, a natural disaster, human error or failure of a key supplier to consider.

In conclusion, while certain areas of risk may be lower than for businesses in high risk countries, you will almost certainly benefit from a business continuity plan that addresses your organisation and country-specific threats.

Isn't Business Continuity Management something only big companies need to worry about?

The need to be 'always-on' is something that's vital for all businesses, regardless of size or sector. Threats range from hardware failure, power outages and being let down by a key supplier all the way through to major disruptions caused by challenges such as flooding, severe weather and flu pandemics.

We recognise that smaller businesses may not have the money, time and resources to prepare for disruptions, yet the cost of dealing with them when they arise can be significant. It's never too early in the life of an organisation to build in resilience, robustness and availability. This is far easier to do as the business grows, rather than attempt to retrofit measures later on.

Do you speak 'Business Continuity'?

Source: http://www.resilienceguard.ch/blog/

SO I'M LIKE, "PM ME," AND SHE'S ALL, "182," SO I HACKED THE ADMIN LOG AND RICKROLLED HER, AND NOW EVERYBODY IS LIKE, "ROTFLMAO, DUDE, YOU'RE AWESOME!"
TIMMY IS SPEAKING IN TONGUES!

For those who are new to business continuity, it can seem that at times experienced practitioners are almost speaking a different language. Like most disciplines, an array of mystifying acronyms and bewildering terminology has developed over time. Industry veterans toss these terms around with apparent ease and clearly they mean something as those 'in the club' understand them perfectly but we appreciate it can all seem baffling to those who aren't in the know.

So in an effort to break down barriers to understanding, here is Resilience Guard's guide to some of the more commonly used business continuity and crisis management terminology. While far from being an exhaustive list, we hope you will find it a good starting point:

Business continuity jargon buster

- **ALARP (or risk)**
  A risk management term meaning 'As low a risk as reasonably practical'.
- **Assurance**
  The process by which an organisation verifies its business continuity management capability.
- **AToD**
  Shorthand for 'At time of disaster'.
- **Battle box**
  Often literally a box used to store vital information (such as employee contact details, third party recovery providers) and equipment (such as pens, torches, spare batteries) that may prove useful in a disaster.
- **BAU**
  Business as usual – quite literally meaning the normal course of business and commonly used to describe activities returning to normal following a business interruption.
- **BC**
  Business continuity – Defined as the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

- **BCM**
  Business continuity management – A holistic management process that identifies potential threats to an organisation and the impact on business operations that those threats—if realised—might cause. BC provides a framework for building what's known as organisational resilience: the capability of an organisation to respond effectively, safeguarding the interests of its key stakeholders and reputation.
- **BCP**
  Business continuity plan – A documented collection of procedures and information that is developed, and kept up-to-date in readiness for use in a potentially disruptive event to enable the organisation to continue to deliver its critical products and services as usual.
- **BCMS**
  Business continuity management system – An overall management system that implements, operates, monitors, reviews and improves an organisation's business continuity.
- **BIA**
  Business impact analysis – the process of analysing business functions and the effect a business disruption might have on them.
- **Blue light services**
  Predominantly used in the UK, this term is used informally to refer to the emergency services of police, fire and ambulance.
- **Campus**
  A set of buildings that are geographically grouped together and might form one interconnected set of business continuity plans.
- **Cold site**
  A data centre or work area equipped with the appropriate environmental conditioning, electrical connectivity, communications access, configurable space and access to accommmodate the installation of equipment by key workers tasked with resuming operations.
- **CMT**
  - Crisis management team – A group of designated individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.
  - Whereas in most countries 'crisis' and 'incident' are used interchangeably in the UK the term 'crisis' generally refers to wide area incidents involving the emergency services with 'incident management' used for normal BCM.
- **Dedicated work area**
  Workspace provided for sole use by a single organisation and configured ready for use.
- **Desktop Exercise (also known as a tabletop exercise)**
  Technique for rehearsing emergency teams in which participants review and discuss the actions they would take according to their plans, but do not actually perform any of these actions. Such an exercise can be conducted with a single team or multiple teams, typically under the guidance of exercise facilitators.
- **Disaster declaration**
  Nominated staff should be familiar with the list of assessment criteria of an incident versus disaster situation established by the BCM or DR Steering Committee and the notification procedure when a disaster occurs. Usually, to invoke third party services or make an insurance claim there will be a need for a formal disaster declaration to have been made.
- **DR**
  Disaster recovery – the process of recovering IT systems following an incident.
- **Exercise**
  Term used to describe rehearsing the roles of team members and staff and test the recovery of an organisation's systems – including technology, telephony and administration – to demonstrate the effectiveness of a business continuity plan.

- **Hot site**
A facility equipped with IT, telecoms and infrastructure that can be used to restore IT and telephony capabilities. When the facility is designed to accommodate business users it is more commonly referred to as a work area recovery site.
- **IMT**
Incident management team – A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.
- **Invocation**
A formal declaration that an organisation's business continuity plan needs to be activated to continue to deliver key products and services in the event of a business interruption.
- **ITDR**
Refers to the pure IT aspects of disaster recovery, specifically restoring IT to the level required to support an organisation's critical business functions to acceptable levels within a pre-determined period of time following a disruption.
- **KPI**
Key performance indicators – Benchmark measurements based on the organisation's objectives, targets and industry practice.
- **MTDL**
Maximum tolerable data loss – The maximum loss of information (electronic and other data) that an organisation can tolerate. The age of the data could make operational recovery impossible or the value of the lost data is so substantial as to put business viability at risk.
- **MTPoD**
Maximum tolerable period of disruption – the amount of downtime an organisation can withstand in the event disaster strikes after which its viability will be threatened if product or service delivery cannot be resumed.
- **Outage**
A period of time in which IT services and systems are out of commission. For other plant and equipment the term 'downtime' is commonly used.
- **PDCA**
Abbreviation for Plan, Do, Check, Act – This is the model used as a framework for all management systems including business continuity management systems.
- **Residual risk**
The level of risk remaining after all cost-effective actions have been taken to lessen the impact, probability and consequences of a specific risk according to an organisation's risk appetite.
- **Risk appetite**
The degree of risk an organisation is prepared to accept being exposed to at any point in time.
- **RPO**
Recovery point objective – The target set for the status and availability of data (electronic and paper) at the start of the recovery process. In purely ITDR terms it can be seen as the precise time to which data and transactions have to be restored, for example close of business or last backup.
- **RTO**
Recovery time objective – The target time for resuming the delivery of a product or service to an acceptable level – either full or partial – following its disruption.
- **SLA**
Service Level Agreement – An agreement between a service provider and a customer defining the scope, quality and timeliness of service delivery.
- **Simulation**
Simulation is a process whereby recovery team members perform all of the actions they would take in the event of a crisis plan activation. It may involve one or more of the recovery teams and is performed under conditions that simulate a real world business interruption.
- **SPOF**
Single point of failure – A service, activity or process to which there is no alternative meaning that loss of that element could lead to total failure of a mission-critical activity.

- **Syndicated service**
  A workspace shared by a limited number of organisations, set-up for general use rather than any one organisation.
- **Syndication ratio**
  The number of times that a particular work area is sold by a third party provider. This is an important figure as a work area's availability at the time of an incident could be allocated on a first come, first served basis or on a reduced allocation basis.
- **Virtual battle box**
  An electronic form of a storage location held on the internet, intranet or cloud so that data and information is immediately available post incident and accessible by the Incident Management Team.
- **WAR**
  Work area recovery – Restoration of office activities at an alternative location that provides desks, telephony, office systems and networking capability.
- **Warm site**
  A designated standby site equipped and serviced to a level which will allow the organisation to resume essential operations before their non-availability threatens business viability. However, there is no definitive distinction between a warm and a hot site, although clearly recovery at a hot site could be almost immediate whereas at a warm site it might take several hours to accomplish.
- **Wide area disaster**
  A catastrophic event such as a terror attack or industrial accident that impacts a large geographic area and requires emergency services (or even the military) to take control.
- **WRC**
  Workplace recovery centre – a fully-equipped alternative workspace for use by employees in the event their normal premises or the technology and communications they need to do their jobs are unavailable for any reason.

Four Essential Skills for Building a Risk Management Team

Source: http://levelhundred.com/four-essential-skills-for-building-a-risk-management-team/

As firms in the financial services arena better understand the significant risks they face, many are deciding to build or grow their risk management teams. Firms all across North America, Europe, and Asia added risk management staff in 2004. Coupled with the explosive growth of economies in Asia, this trend is expected to continue for the next decade. However, as the risk management field continues to mature, senior executives are becoming more selective as they look to hire these individuals who, in many cases, are relied upon to ensure the future existence of the firm.

Risk management departments are called upon to set and monitor risk limits; build, validate, stress test and back-test data and models; work with regulators to provide assurance that financial markets and stockholders are being protected; and to assist the business units in looking at the next deal in light of the risks involved. **Who are these essential people, and what backgrounds are firms looking for when filling risk management roles?**

Four Essential Skills

1) Academic Credentials in Finance

First, firms seek risk managers who have strong academic finance credentials. While many quantitative risk managers have PhD's in physics, statistics, and computer science, the top firms seek individuals with strong academic credentials in finance. MBA's in finance, with rigorous course loads in quantitative finance, from the University of Chicago, Wharton, and NYU, for example, get the attention of hiring managers. Doctorates in finance and econometrics from top US finance institutions are also preferred to non-finance degrees. **One top risk professional told me, "I wouldn't expect to run a**

nuclear facility, so why would I want a nuclear physicist running my portfolio analytics?"

2) Market Experience

Second, firms seek individuals who understand trading and how the global financial markets operate. Ex-traders, or individuals who have hands-on experience on the trading floor, are regarded quite favorably by senior risk managers. Why? Because risk management does not operate in a static environment – new products or trading strategies are introduced and new deals are structured routinely. Risk managers must be able to quickly understand the trade or the deal, as well as the motivation of the traders/portfolio managers so that the risks of the deal are properly and fully understood. Individuals who have trading experience are highly valued at capital markets firms, as well as hedge funds, where the pace is fast and the risks are significant.

3) Strategic

Third, the leading risk managers need to be forward-looking and strategic minded, with an eye to understanding potential risks, rather than reporting on yesterday's VaR levels. The strongest risk management teams are able to keep pace with the evolving and volatile nature of the financial markets, and in more and more cases, assist the front office, portfolio managers and chief investment officers reach a solution that satisfies the investment objectives as well as the risk parameters. This is especially true in the area of credit risk and structured products, where credit risk managers are often involved in the structuring process to ensure that risks are adequately quantified and hedged so that the deal will pass exposure limit tests.

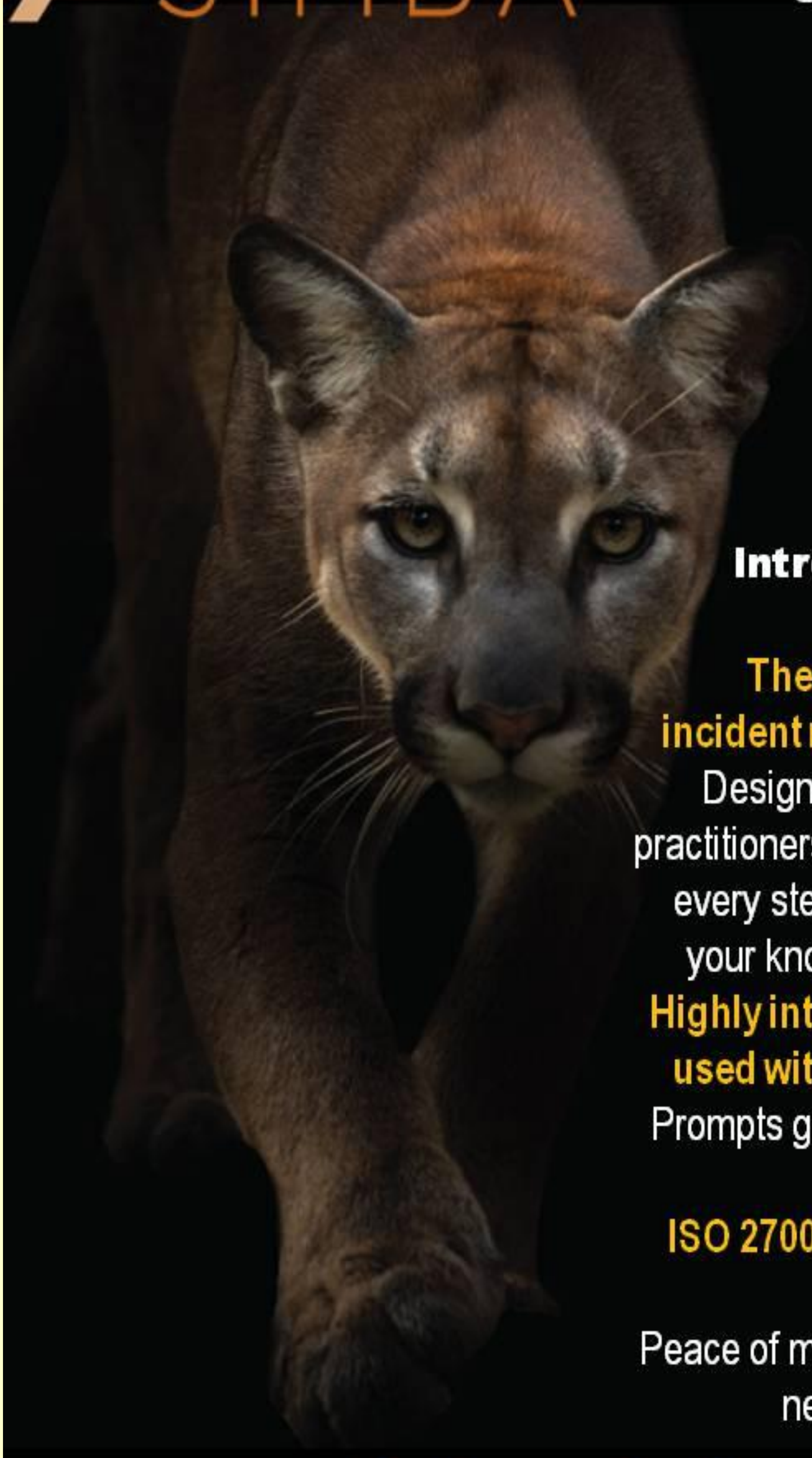
4) Communication Skills

Finally, firms have determined that not only must risk managers be educated in quantitative finance, experienced in trading, and forward-looking, but that they also be able to translate complex financial products and risk management concepts, practices, and processes into language understood and appreciated by the front office, management and board personnel. In many cases, risk managers are called upon to summarize the myriad of risks that financial firms face, and to translate this into actionable concepts that can be addressed at the executive committee level. Strong interpersonal, general business and communication skills are imperative for risk managers to be successful.

New risk managers starting their career should first choose a finance degree from a top quantitative program, and then select an opportunity close to the trading desk. An avid interest and thorough understanding of the financial press is also highly recommended. Risk managers should be able to grasp the relationships between global events and the financial markets, and failures such as LTCM, China Asian Aviation, Enron, and so on. Hiring managers in this field should clearly understand the skills they desire and need within the risk group. They should not settle for someone who does not have the proper balance of quantitative, market savvy, strategic and communication skills required for success.

While these fours skills are difficult to find in one person, they do exist. As the market appreciates the value of exceptional risk management and this skill set, firms are compensating top risk managers – those key individuals who are one or two levels below the CRO level – with annual packages in the $500,000 to $1.2 million range. As one might imagine, this provides ample incentive for individuals to select risk management as a rewarding career.

EDITOR'S COMMENT: Although the article comments on a "Risk Management Team" it ends up with the conclusion that "While these four skills are difficult to find in one person, they do exist". Despite this, what is missing in #1 skill is an "intelligence analyst" coupled with an "asymmetric threats analyst". If you do know what is going on in the planet how can you calculate risks?

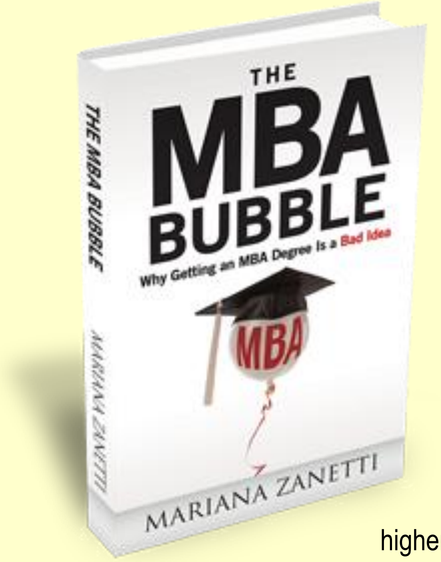


The MBA Bubble

Source: http://www.thembabubble.com/

If you think an MBA from a "top" Business School is a sure step to a high salary, then you need to read The MBA Bubble.

It contains the REAL secrets to reach your professional, financial, and life goals without mortgaging your life on an MBA program.



YOU'LL FIND OUT

- The worst mistakes young professionals make when investing in their education;
- Why MBAs are NOT worth and DON'T lead to higher salaries;
- How MBAs are a leftover product of the industrial age…and don't teach the skills required to thrive in today's business world;
- How Business Schools use deceitful marketing strategies to take credit for your success and lure in more unsuspecting students;
- Why you could be wasting over $100,000 on an MBA…even if you have a full scholarship.

Author **Mariana Zanetti** pens an eye-opening expose into the world of higher business education that will appeal to all those who have, or are contemplating getting, their master of business administration (MBA) degree. The MBA Bubble is nothing short of revolutionary in a world where young professionals are increasingly encouraged to mortgage their futures for little return.

After earning her MBA from one of the world's top business schools, Zanetti embarked on a successful international marketing career, meeting all of her professional goals and more. Yet she admits in The MBA Bubble that choosing to pursue this particular degree was one of the worst mistakes of her entire career.

In her straightforward and honest prose, Zanetti reveals the truth about the role of MBAs in today's world. Created one hundred years ago for an age that no longer exists, these degrees have become **ruinous investments** for the hoards of young professionals who have been convinced by business schools that they are necessary. Zanetti explains that, despite the common belief, MBAs do not actually enhance salaries and discusses the deceit behind business schools' marketing tactics, including their manipulation of rankings and statistics.

While the popularity of MBA degrees is undeniable, Zanetti argues that much of the hype surrounding these degrees comes from the fact that business schools tend to only admit highly motivated people who are likely to become successful anyway. The schools simply take the credit from extremely driven professionals, likely to achieve their professional goals in the first place, and attribute their success to the degree.

In addition to the presentation of exhaustive research, Zanetti demonstrates how to meet one's professional goals without plummeting into massive debt. MBA programs often tout the networking channels, higher salaries, career improvements, new skills, and business training as benefits of a higher degree. The author, however, offers alternative resources and profitable strategies that will help readers reach those same exact goals minus the wasted years and money. Ultimately, she teaches readers how to think critically and how to challenge the faulty mental models that most people accept without question.

The MBA Bubble is a must read for all those who have, or are considering, a higher business education degree. Armed with facts and alternative resources, readers will walk away from Zanetti's book with a new found understanding of the way business schools really work.

Analyze your education investment

Most MBA applicants do not evaluate the Return Of Investment (ROI) of their education properly. Many of them take for granted that they will get a six-figure job after graduation, as if the average wages published by the business school are guaranteed. They are not, and the data the statistics show can be easily manipulated.

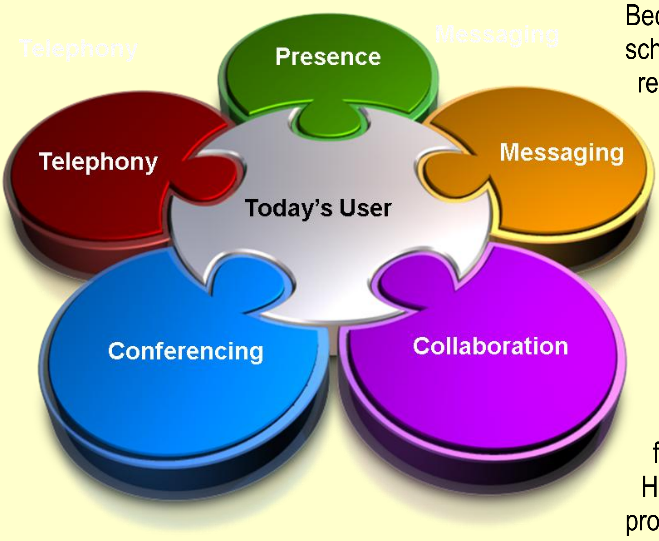
To analyze the ROI of your education investment, you should calculate the value of the money you spend on the MBA program over time, including the risk of not finding a good job immediately and of not fulfilling your salary expectations. Additionally, you should not forget that you would not have a static career if you had not gotten an MBA. Your salary would have increased anyway, as a consequence of your career's natural evolution. Any investment should be evaluated only in contrast with its alternative, so you should only take into account the differential income increase you expect by pursuing an MBA program.

Use the calculator below to estimate the Net Present Value (NPV) of your education investment
http://www.thembabubble.com/npv-calculator/

How Unified Communications promote Humanism through Disaster Risk Reduction

Dr. Alexandros E. Soulahakis

Apr 19 – Unified Communications (UC) today is defined as the number of technologies involved within a single platform, which offers user-friendly communications tools for corporate users. It is a fact that today, more than a billion employees are remote users. Unified Communications today offer a new communication experience. Virtual teams are organized through a collaboration platform, presence, voice and video capabilities, in order to increase their productivity and efficiency.



So why should we adopt UC? Unified Communications is not just the next trend. UC is not the new way of selling VoIP products. The vision behind UC is a lot bigger than selling, making money or present new technological achievements. What is the secret behind the success story? UC unintentionally, transfers incredible knowledge and skills to its users. Even if the employees do not have the skills the collaboration platform helps them to organize and prioritize their work. How? Because they can visually follow the time schedule and get the full picture of the remaining tasks related to the deadline. Organizing the progress within visual environments help people to have a better understanding of the goal and a better sense of time. It is not a coincidence that the adage "a picture is worth thousand words" refers to complex idea that can be easily understood by watching a single picture. This is why we humans visualize things. This is how we understand the magnetic field by drawing flux lines; Time is represented on the x-axis; Humans focus on organized actions and progress through visualization. But what is relationship of those discussed with Unified Communications and how does this related with Disaster Risk Reduction DRR?

The idea of Unified Communications is not a new concept. It is a primordial need. How many movies have you watched, in which the war (incident) will start after they light up the beacons? That is the signal that danger is close (beginning of the incident).

So how does UC contribute to DRR? The Beacon on the movies is a part of UC system, which uses no technology, but utilizes the presence, a well-known characteristic of modern UC systems. Furthermore the visual effect of fire can be seen from miles away. Does it rings a bell? How many corporate systems today can broadcast a unique message simultaneously to thousands or maybe millions of users, ensuring immediate & reliable transmission? What if the collaboration platform, videoconference and media integration can be easily used as the beacon? In case of an incident (as for example fire at the front entrance), a picture, or even better a live video feed will minimize the risk of accident, as people watching it are now aware that there is a fire and they must stay away of it. At the same time the same media offers a visual of the situation to the emergency services, before they arrive at the place of the incident. This is not only a time saver but also gives control (and visual) of the situation even before the start of fire extinguishing.

It is a fact that a UC solution is not the new "fancy toy" for enterprises; It is not a luxury. It is a need. It organizes humans to a unified force and helps them achieve targets progressively by using all means of communications. Employees not confident with their organizational soft skills or teamwork are benefit of the UC, because they can now get organized and progress a lot faster, towards their target. Now visualize what happens when this platform is getting combined with mobility. What if a user turns the camera of the tablet facing the fire through a window of a nearby building? I am sure that a programmatically magic button could easily pass the feed to any monitor of the intranet, through the corridors of the nearby buildings. Can you visualize the impact of that action? People watching the event through monitors are aware of the danger, but they are also calm, as they know three very important facts.

- They are far away from the fire so **they know** they are not in danger.
- **They may choose** easily alternative emergency exits to get away of the building, while they maintain their composure.
- As they walk their way to the exit **they can still watch** the incident from other monitors around, which gives them constant information (even while running) of the progress and the current state of the incident.

So Unified Communications help humans use most of their senses to communicate. Such a platform introduces awareness to the users (**they know**). Decision-making skills (**they may choose**) and observation (**they can still watch**), which means they can change their decision in real-time whenever they feel there is a reason to do so. Moreover the use of a collaboration platform helps employees to focus on work and not on how to handle data. The logic is already implemented in the platform for them. That helps the employee to become more productive. But how is this happening and why is this related to risk reduction?

Most visionary people today already have those skills. They like to develop others, pass their experience to them and create a better, "upgraded" image of themselves. Leaders are the people thinking more about risks and how to help others to avoid pitfalls. Subconsciously those people pass their experience and skills to the employees without even knowing it by implementing their logic to the UC platform. This is happening because the logic behind the UC functionality is directly affected by their initial purpose. To create humanized communication systems. Their love for humans has been transferred through their passion for telecoms to the platform itself. This is why UC is not just a trend.

This is the reason such systems succeed. Employees using a collaboration platform feel the responsibility to inform others of an upcoming incident more than those using the old-fashion way of working. When we see a stranger trying to cross the road while a vehicle in approaching fast, instinctively we will try to pull that person back. This is happening because we have been built to help each other. This is why we leave in societies. We ensure living while we minimize the risks of extinction. This is exactly what is happening with Unified Communications. The fact that UC users behave with a more protective/informative way is not happening because they are better people than others. It happens because they train themselves unconsciously to work in a more humanized environment and this boosts their disaster risk reduction skills. Subconsciously every each one of us has the risk management skill developed. But humans are getting better through training.

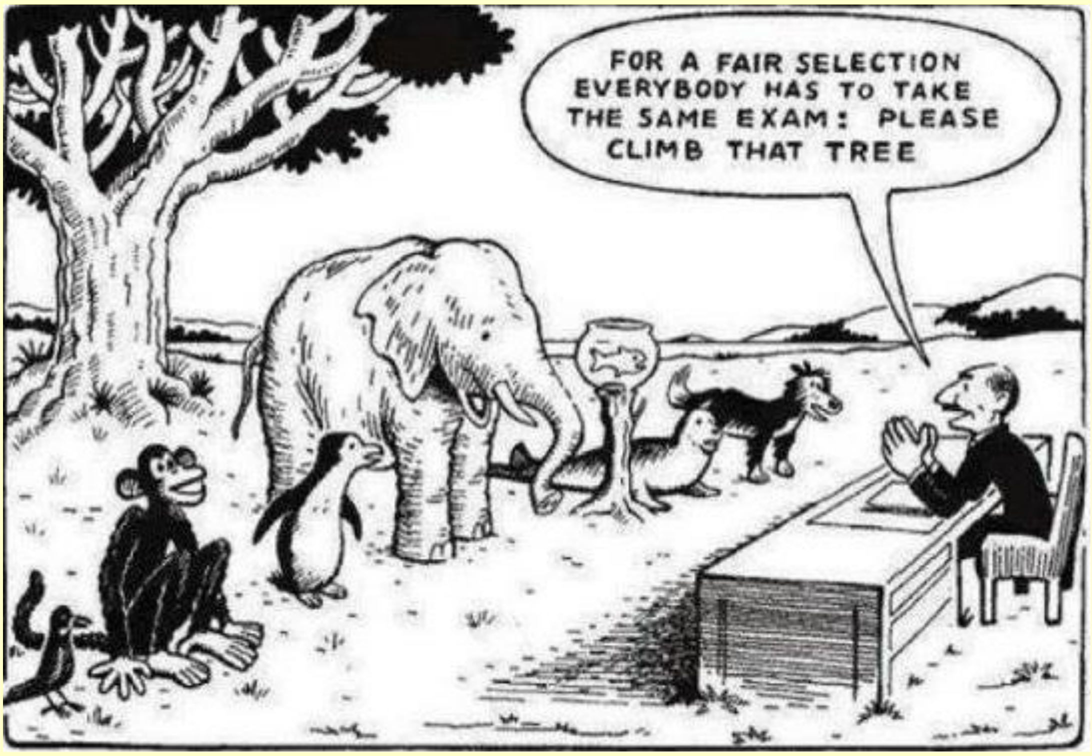
The difference between people using the UC and people not, is that those working in a UC environment train their brain models. That helps them to activate and develop those skills as a part of their everyday life.

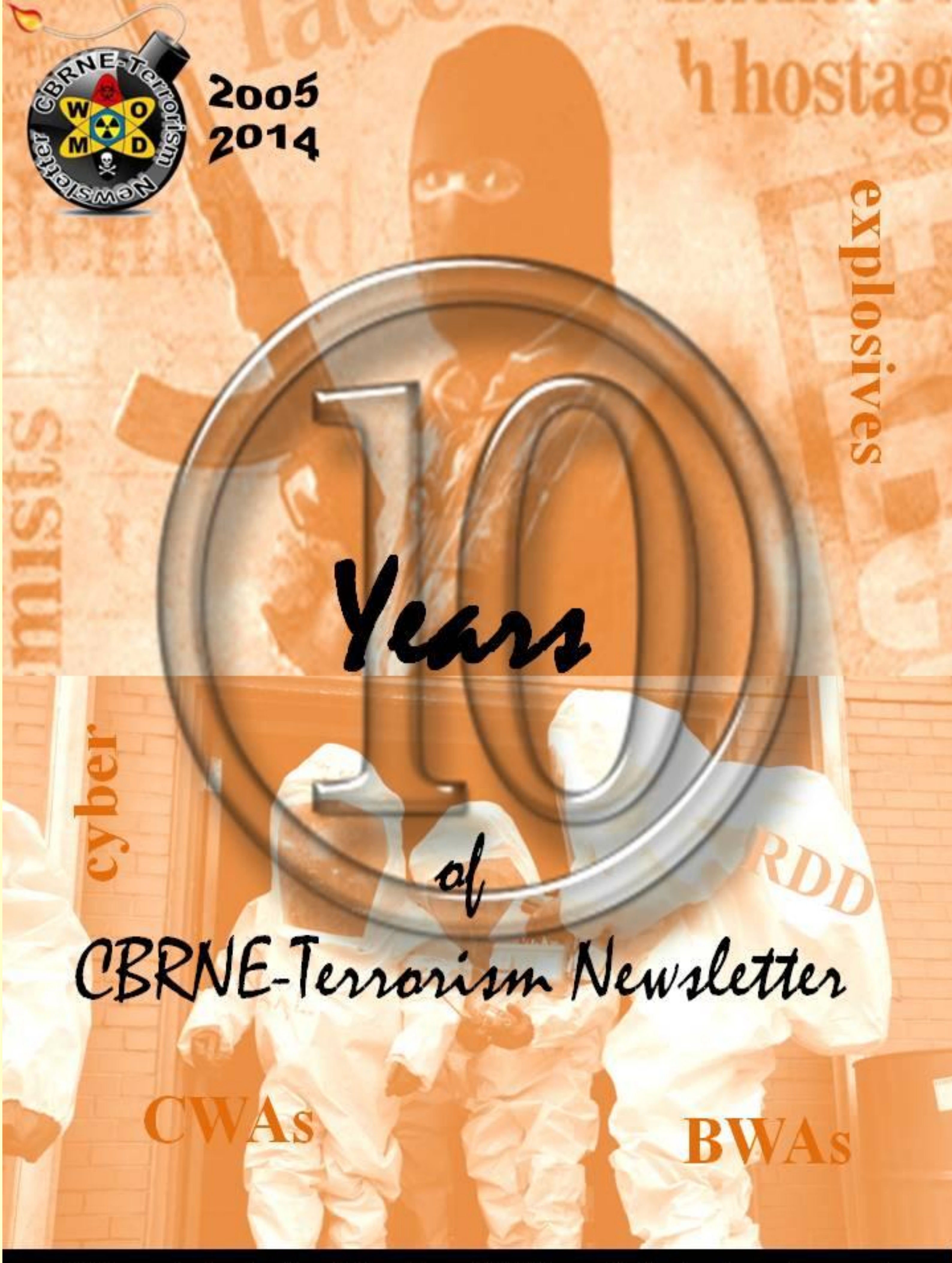
Summarizing this (not so philosophical) approach, Unified Communications:

- Offer socializing in virtual teams.
- Promote teamwork through a virtual society.
- Reintroduce interpersonal relationships between employees.
- Train hidden skills inside our brain.
- Share valuable knowledge through experience.
- Favor awareness and disaster risk reduction.

Concluding our story, UC is not the new way of calling. It has been used back in times when humanity decided that the only way to survive is to create societies. Today this idea is still imprinted deep into our brain, but since we have managed to greatly reduce the risk of extinction, we are using it in the form of prevention. This unwritten code is minimizing risks that may be a threat. And this is the reason why unified communications promote humanism.

***Dr. Alexandros E. Soulahakis is** Associate Consultant at Resilience Guard GmbH (Zurich, Switzerland). He is a self-driven engineer with strong technical background and hands-on ability to work in fast paced environments, such as maritime and hospitality industries. Deep understanding of telecommunication systems, computer science and electrical/electronic engineering that allows innovative resolution of highly complex problems. Ability to design and oversee the installation of telecommunications equipment and facilities, complex PBX scalable systems & VPN secure VoIP networks. Experience with IT administration in real or simulated environments (storage, antivirus solutions, IDS/IPS).*


FOR A FAIR SELECTION EVERYBODY HAS TO TAKE THE SAME EXAM: PLEASE CLIMB THAT TREE



2005
2014

10 Years of CBRNE-Terrorism Newsletter

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