

July 2015

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders



10 years



E-terrorism

www.cbrne-terrorism-newsletter.com

Iran stored nuclear equipment in Sudanese arms factory destroyed by Israel in October 2012: Saudi memo

Source: <http://www.homelandsecuritynewswire.com/dr20150624-iran-stored-nuclear-equipment-in-sudanese-arms-factory-destroyed-by-israel-in-october-2012-saudi-memo>

June 24 – In early October 2012 Israeli planes destroyed the Yarmouk arms factory near Khartoum, Sudan's capital – 1,300 miles from Israel. In 1998 the plant was suspected of holding Iraqi chemical weapons which Saddam Hussein wanted to conceal from the UN

to officials in the Saudi embassy in Khartoum, Iran, in early 2012, shipped advanced nuclear equipment to Sudan.

Business Insider reports that the Saudi embassy memo, dated February 2012 and marked as "very secret," was leaked last week



2

inspectors. Sudan had become a major corridor of arms for Hamas, and Israel has conducted several military operations inside Sudan aiming to disrupt shipments of arms to Hamas. In April 2011, for example, Israeli special forces, ferried by helicopters into Sudan, ambushed and killed two high-level Hamas officials who were on their way to Libya to finalize a deal, financed by Iran, to buy about 800 chemical munitions from anti-Qaddafi rebels who had taken over a couple of chemical weapons depots from the pro-Qaddafi forces.

It now appears that the October 2012 Israeli attack targeted more than chemical weapons Iran was trying to supply to Hamas. According

by the WikiLeaks groups along with what the group claimed were 60,000 other official Saudi communications.

"The embassy's sources advised that Iranian containers arrived this week at Khartoum airport containing sensitive technical equipment in the form of fast centrifuges for enriching uranium, and a second shipment is expected to arrive this week," the document read, according to a Reuters report.

The Saudi embassy cable does not offer any details about the source of the information, or about the nuclear devices or materials Iran was storing at the site.



Sudan does not have a nuclear power industry or a nuclear research program, and with the exception of the Saudi message, there were no other indications that Iran was using Sudan to store nuclear materials. There were no comments on the revelations from Sudan, Iran, Saudi Arabia, or Israel.

The October 2012 Israeli strike caused massive explosions which destroyed a sprawling arms factory and weapons depots south of Khartoum. The air strikes wiped out the complex and killed four people.

Germany's oldest nuclear power plant goes offline, part of move to shut reactors by 2022

Source: <http://www.startribune.com/germany-s-oldest-remaining-nuclear-plant-shuts-down/310440251/>



June 28 – Germany's oldest remaining nuclear reactor has been shut down, part of a move initiated four years ago to switch off all its nuclear plants by the end of 2022. The Grafenrheinfeld reactor in the southern state of Bavaria was taken offline as scheduled overnight, authorities and operator E.ON said Sunday. Grafenrheinfeld went into service in 1981. It is the first reactor to close

since Germany switched off the oldest eight of its 17 nuclear reactors in 2011, just after Japan's Fukushima nuclear plant disaster. The next to close will be one of two reactors at the Gundremmingen plant in Bavaria, which is set to shut by the end of 2017. The rest will be closed by the end of 2022. Environment Minister Barbara Hendricks said the Grafenrheinfeld shutdown is "a visible signal that the nuclear exit is moving forward." "Every nuclear power station that goes offline reduces the so-called residual risk that is linked to the use of nuclear power plants and moves us a step forward in the reorganization of our energy supply," she said. Germany aims to generate 80 percent of its electricity from renewable sources by 2050.

3

GERMANY'S NUCLEAR REACTORS

(https://en.wikipedia.org/wiki/List_of_power_stations_in_Germany)

Name	Location	Geographical Coordinates	Type	Capacity (MWe)	Operational	Notes
VAK	Kahl am Main	50.0591294°N 8.9871812°E	BWR	15	1960–1985	
MZFR	Leopoldshafen	49.1043102°N 8.4325862°E	PHWR	52	1965–1984	
AVR	Jülich	50.9030599°N 6.4213693°E	HTGR	13	1966–1988	
KKR	Rheinsberg	53.1472465°N 12.9903674°E	VVER	62	1966–1990	GDR plant, shut down after German reunification
KRB Unit A	Gundremmingen	48.513264°N 10.4020357°E	BWR	238	1966–1977	



Name	Location	Geographical Coordinates	Type	Capacity (MWe)	Operational	Notes
KRB Unit B	Gundremmingen	 48.5148276°N 10.402379°E	BWR	1284	1984–present	Scheduled for shut down: Dec. 31, 2017 [1]
KRB Unit C	Gundremmingen	 48.5155383°N 10.4020786°E	BWR	1288	1985–present	Scheduled for shut down on 31 December 2021 [1]
KWO	Obrigheim	 49.364503°N 9.076252°E	PWR	340	1968–2005	
KWL	Lingen	 52.4831853°N 7.3005223°E	BWR	250	1968-1977	
HDR	Grosswelzheim	 50.0551446°N 8.9848691°E	BWR	23	1969–1971	
KKS	Stade	 53.6200685°N 9.5306289°E	PWR	640	1972–2003	
KKN	Niederaichbach	 48.6058015°N 12.3000848°E	HWCGR	100	1973–1974	
KGR Unit 1	Greifswald	 54.1417497°N 13.6583877°E	VVER	408	1974–1990	GDR plant, shut down after German reunification
KGR Unit 2	Greifswald	 54.1417623°N 13.6597395°E	VVER	408	1975–1990	
KGR Unit 3	Greifswald	 54.1415235°N 13.6624217°E	VVER	408	1978–1990	
KGR Unit 4	Greifswald	 54.1414229°N 13.663644°E	VVER	408	1979–1990	
KGR Unit 5	Greifswald	 54.140631°N 13.6664128°E	VVER	408	1989–1990	
KWB Unit A	Biblis	 49.709331°N 8.415865°E	PWR	1176	1975–2011	[2]
KWB Unit B	Biblis	 49.7089474°N 8.413285°E	PWR	1240	1977-2011	
KWW	Würgassen	 51.6396481°N 9.3915617°E	BWR	640	1975–1994	
GKN Unit 1	Neckarwestheim	 49.0401151°N 9.1721088°E	PWR	785	1976–2011	capacity including traction current
GKN Unit 2	Neckarwestheim	 49.0406214°N 9.1755903°E	PWR	1269	1989–present	Scheduled for shut down: Dec. 31, 2022 [1]
KKB	Brunsbüttel	 53.8913533°N 9.2005777°E	BWR	771	1977–2011	
KKI Isar Unit 1	Essenbach	 48.6044748°N 12.2972095°E	BWR	870	1979-2011	
KKI Isar Unit 2	Essenbach	 48.6055532°N 12.2931647°E	PWR	1365	1988–present	Scheduled for shut down: Dec. 31, 2022 [1]
KKU Unterweser	Stadland	 53.4293465°N 8.4774649°E	PWR	1285	1979–2011	



Name	Location	Geographical Coordinates	Type	Capacity (MWe)	Operational	Notes
KNK-I/II	Leopoldshafen	49.0973279°N 8.4327739°E	FBR	21	1979–1991	fast sodium-cooled research reactor ^[3]
KKP Unit 1	Philippsburg	49.2513078°N 8.4356761°E	BWR	890	1980–2011	
KKP Unit 2	Philippsburg	49.2513078°N 8.4356761°E	PWR	1358	1985–present	Scheduled for shut down: Dec. 31, 2019 ^[4]
KKG	Grafenrheinfeld	49.9841308°N 10.1846373°E	PWR	1275	1982–present	Scheduled for shut down: end of May, 2015 ^[4]
KKK Krümmel	Geesthacht	53.4104656°N 10.4091597°E	BWR	1260	1984–2011	
KWG	Grohnde	52.0348748°N 9.4097793°E	PWR	1360	1985–present	Scheduled for shut down: Dec. 31, 2021 ^[4]
KBR	Brokdorf	53.850666°N 9.3457603°E	PWR	1326	1986–present	Scheduled for shut down: Dec. 31, 2021 ^[4]
KMK	Mülheim-Kärlich	50.408791°N 7.4861956°E	PWR	1219	1987–1988	
THTR	Hamm-Uentrop	51.6786228°N 7.9700232°E	HTGR	296	1987–1988	
KKE	Emsland	52.4716974°N 7.3206389°E	PWR	1290	1988–present	Scheduled for shut down: Dec. 31, 2022 ^[4]

Legend:

Reactor is currently operational Decommissioned reactor

Types:

BWR = Boiling water reactor, FBR = Fast breeder reactor, HTGR = High-temperature gas-cooled reactor, HWCGR = ?, PHWR = Pressurized heavy-water reactor, PWR = Pressurized water reactor, VVER = Water-water energetic reactor

Fukushima Daiichi Status Updates

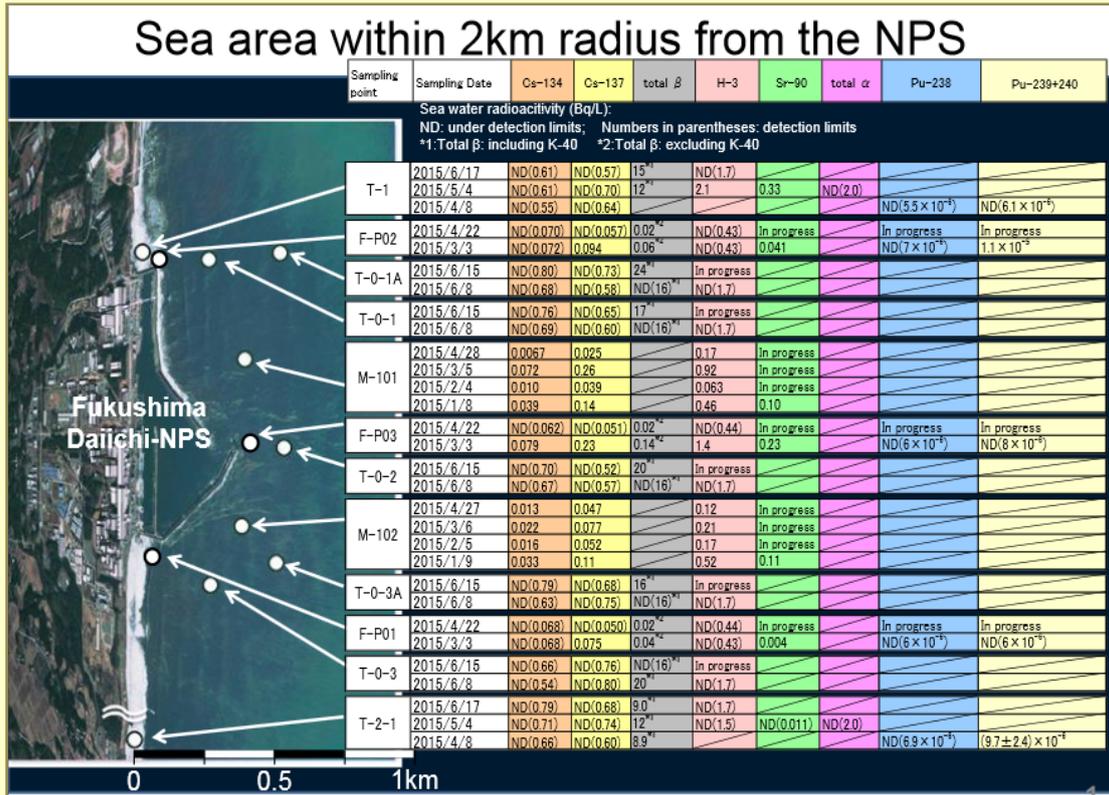
Source: <https://www.iaea.org/node/11410>



Radioactivity in water near the Fukushima Daiichi nuclear power plant has remained low and stable from 21 to 27 June 2015, according to the [regular update](#) and [sea area monitoring results](#) provided by Japan's Nuclear Regulation Authority (NRA) to the IAEA. Tokyo Electric Power Corporation announced that removal of the highly contaminated water into an underground tunnel housing pipes and cables outside the Unit 2 turbine has been completed. Removal of the remaining water at Unit 3 will begin shortly pending

government approval.





A new look for nuclear power

By Nancy W. Stauffer

Source: <http://www.homelandsecuritynewswire.com/dr20150701-a-new-look-for-nuclear-power>

July 01 – **Many experts cite nuclear power as a critical component of a low-carbon energy future. Nuclear plants are steady, reliable sources of large amounts of power; they run on inexpensive and abundant fuel; and they emit no carbon dioxide (CO₂).**

A novel nuclear power plant that will float eight or more miles out to sea promises to be safer, cheaper, and easier to deploy than today's land-based plants. In a concept developed by MIT researchers, the floating plant combines two well-established technologies — a nuclear reactor and a deep-sea oil platform. It is built and decommissioned in a shipyard, saving time and money at both ends of its life. Once deployed, it is situated in a relatively deep water well away from coastal populations, linked to land only by an underwater power transmission line. At the specified depth, the seawater protects the plant from earthquakes and tsunamis and can serve as an infinite source of cooling water in case of emergency — no pumping needed. An analysis of potential markets has identified many sites

worldwide with physical and economic conditions suitable for deployment of a floating plant.

“More than 70 new nuclear reactors are now under construction, but that’s not nearly enough to make a strong dent in CO₂ emissions worldwide,” says Jacopo Buongiorno, professor of nuclear science and engineering (NSE) at MIT. “So the question is, why aren’t we building more?”

The offshore floating nuclear plant

The researchers’ vision for an Offshore Floating Nuclear Plant (OFNP) includes a main structure about 45 meters in diameter that will house a plant generating 300 megawatts of electricity. An alternative design for a 1,100-MW plant calls for a structure about 75 meters in diameter. In both cases, the structures include living quarters and helipads for transporting personnel — similar to offshore oil drilling platforms.

Buongiorno cites several challenges to this vision. First, while the fuel is



cheap, building a nuclear plant is a long and expensive process often beset by delays and uncertainties. Second, siting any new power plant is difficult: Land near sources of cooling water is valuable, and local objection to construction may be strenuous. And third, the public in several important countries has lost confidence in nuclear power. Many people still clearly remember the 2011 accident at the Fukushima nuclear complex in Japan, when an earthquake created a tsunami that inundated the facility. Power to the cooling pumps was cut, fuel in the reactor cores melted, radiation leaked out, and more than 100,000 people were evacuated from the region.

In light of such concerns, Buongiorno and his team — Michael Golay, professor of NSE; Neil Todreas, the KEPCO Professor of Nuclear Science and Engineering and Mechanical Engineering; and their NSE and mechanical

conventional nuclear reactor on a floating platform similar to those used in offshore oil and gas drilling, and mooring it about 10 miles out to sea.

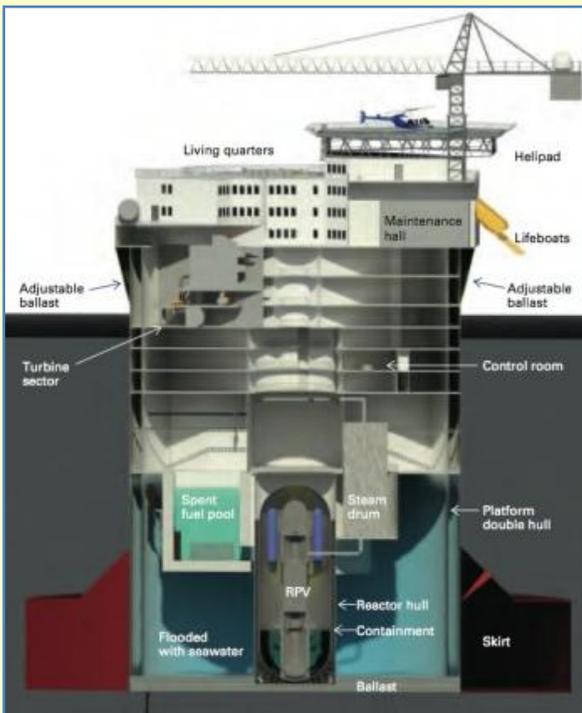
The OFNP integrates two well-established technologies with already robust global supply chains. “There are shipyards that build large cylindrical platforms of the type we need and companies that build nuclear reactors of the type we need,” Buongiorno says. “So we’re just combining those two. In my opinion, that’s a big advantage.” By sticking with known technologies, the researchers are minimizing costly and time-consuming development tasks and licensing procedures. Yet they are making changes they think could revolutionize the nuclear option.

Advantages of shipyard construction, offshore siting

According to the researchers’ plan, OFNPs will be built entirely in shipyards, many of which already regularly deal with both oil and gas platforms and large nuclear-powered vessels. The OFNP structure — platform and all — will be built upright on movable skids, loaded onto a transportation ship, and carried out to its site. There, it will be floated off the ship, moored to the seafloor, and connected to the onshore power grid by an underwater power transmission cable. At the end of its life, it will be towed back to the shipyard to be decommissioned — just as nuclear-powered submarines and aircraft carriers are now.

The proposed Offshore Floating Nuclear Plant structure is about 45 meters in diameter, and the plant will generate 300 megawatts of electricity. An alternative design for a 1,100 MW plant calls for a structure about 75 meters in diameter. In both cases, the structures include living quarters and helipads for transporting personnel, similar to offshore oil drilling platforms.

Compared with deploying terrestrial nuclear plants, this process should provide enhanced quality control, standardization, and efficiency. There’s no need to transport personnel, materials, and heavy equipment to a building site — or to clean up after the plant has been retired. The plan also reduces the need for site evaluation and preparation, which contribute uncertainty and delays. Finally, the OFNP is made mostly of steel, with virtually no need to deal with structural



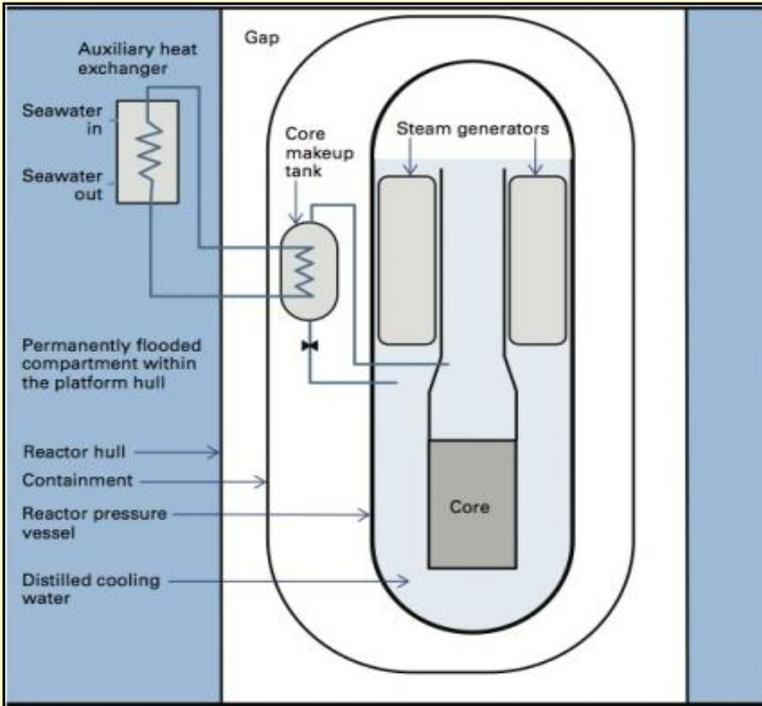
engineering students — have been investigating a novel idea: mounting a



concrete, which, according to Buongiorno, is typically responsible for significant cost overruns and construction delays as well as the emission of substantial quantities of CO₂. Taken together, these factors mean that the OFNP can be deployed with unprecedented speed — an important benefit for a project that

any pumping and without any seawater contamination. “We won’t lose the ultimate heat sink,” Buongiorno says. “The decay heat, which is generated by the nuclear fuel even after the reactor is shut down, can be removed indefinitely.”

The OFNP thus addresses the three main takeaways from Fukushima cited by Buongiorno: Stay away from dense populations, protect against earthquakes and tsunamis, and never lose cooling to the fuel.



The reactor core and steam generators are immersed in fresh, distilled cooling water inside the reactor pressure vessel (RPV). If operation of the cooling pumps is interrupted, cooling water flows passively through an auxiliary heat exchanger immersed in seawater. If a more serious problem occurs, cooling water is released from inside the RPV into the containment structure, and seawater can enter the empty space around the containment. Heat from the cooling water will pass through the containment wall to the seawater. Seawater flows naturally through the structure, so it is constantly renewed, providing an infinite source of cooling.

Designed for efficient operation, enhanced safety

Illustrations in the slideshow above present a view of the OFNP in its ocean setting as well as the plant’s key features. The overall structure is upright, cylindrical in shape, and divided into many floors, most of them split into compartments separated by watertight bulkheads. The upper levels house noncritical components such as the living quarters and a helipad. As on oil and gas platforms, workers are brought out by boat or helicopter for three- or four-week shifts. Food, fuel, and equipment and materials for minor maintenance activities are brought out by supply boat, and heavy loads are lifted off by crane.

The nuclear reactor (either a 300-MW or a 1,100-MW unit) and its related safety systems are located in watertight compartments low in the structure to enhance security and safety, provide easy access to ocean water, and give the overall structure a low center of gravity for increased stability. The reactor core and associated critical components are housed within a reactor pressure vessel (RPV), which is located inside a compact structure called the containment. Surrounding the containment — but separated by a

is highly capital-intensive. “You don’t want to have a large investment lingering out there for eight or 10 years without starting to generate electricity,” Buongiorno says.

The planned site of the floating plant offers other benefits. The OFNP will be situated eight to 12 miles offshore — within the limit of territorial waters — and in water at least 100 meters deep. Thus, it will be far from coastal populations (its only onshore presence will be a small switchyard and a staff and materials management facility), and the deep water beneath it will reduce threats from earthquakes and tsunamis: At that depth, the water absorbs any motion of the ocean floor during earthquakes, and tsunami waves are small. Tsunamis become large and destructive only when they hit the shallow water at the coastline — a concern for nuclear plants built on the shore.

Finally, the open ocean will provide the OFNP with an endless supply of cooling water. If accident conditions arise, seawater can be used to remove heat from the reactor; because the plant is well below the water line, the necessary flows will occur passively, without



gap — is a large chamber that extends to the edge of the cylindrical structure and is constantly flooded with seawater, which enters and exits freely through ports.

Specific design features allow for response to various types of interruptions in normal cooling operations. Generally, pumps bring in cool water from the low ocean layers and discharge the used, heated water to the warm surface layers, thereby preventing “thermal pollution” that can threaten the local ecosystem. If that cooling process is temporarily disrupted, heated water from the reactor is allowed to circulate naturally to a special heat exchanger within the flooded chamber. If a more serious problem (for example, a pipe break) threatens the core, distilled cooling water from inside the RPV is released into the containment (always keeping the core submerged), and seawater from the outside compartment fills the gap around the containment. Heat is efficiently transferred through the containment wall to the seawater, which is constantly and passively renewed. At all times, the cooling water and seawater are kept separate so that contaminants cannot flow from one to the other.

In the unlikely event that, despite continuous heat removal, pressure inside the containment builds up to dangerous levels, gases from within the containment can be vented into the ocean. However, the gases would first pass through filters to capture cesium, iodine, and other radioactive materials, minimizing their release. Current research is tracking the likely dispersion and dilution of such materials to ensure that any radioactivity in the water remains below acceptable limits even under such extreme circumstances.

Promising economics, abundant potential markets

The MIT team believes that the OFNP may be “a potential game changer” as far as the economics of nuclear power is concerned. It provides the economic advantage of “factory” production of multiple units, yet the units can be large enough to benefit from economies of scale. In addition, unlike any type of terrestrial plant, the OFNP is mobile. “If you build a power plant on land, it remains at the construction location for 40 or 50 years,” says Buongiorno. “But with the OFNP, if after a decade or two you need the generating capacity 100 miles

farther up the coast, you can unmoor your floating power plant and move it to the new location.”

The viability of the researchers’ idea depends, of course, on whether there are locations with the necessary physical attributes — deep water relatively near shore but away from busy shipping lanes and frequent massive storms — as well as economic and other incentives for adopting the OFNP.

A detailed analysis identified many potential sites. For example, regions of East and Southeast Asia have limited indigenous resources, a high risk for both earthquakes and tsunamis, and coastal populations in need of power. Countries in the Middle East could use OFNPs to fulfill their domestic needs, freeing up their valuable oil and gas resources for selling. Some countries in coastal Africa and South America rely on power supplied by generators running on imported diesel fuel — an expensive and highly polluting way to go. “Bringing in an OFNP, mooring it close to the coast, and setting up a small distribution system would make a lot of sense — with minimal need for infrastructure development,” says Buongiorno.

Continuing research

The researchers are continuing to work on various aspects of the OFNP. For example, they are developing optimal methods of refueling, a detailed design of the mooring system, and a more thorough model of the plant’s hydrodynamic response in storm waves. In addition, they are establishing a cohesive OFNP protection plan.

The plant design provides considerable security: The reactor is deep in the structure within multiple hulls; the high upper decks permit an unimpeded 360-degree view; and the physical layout minimizes approaches for attackers. Working with security experts, the researchers are now investigating additional strategies involving state-of-the-art sonar and radar systems, submarine netting and booms, and a team of armed security guards.

While much work remains, Buongiorno says, “We anticipate that the first OFNPs could be deployed in a decade and a half — in time to assist the massive growth in nuclear energy use required to combat climate change.”

This research was supported by the MIT Research Support Committee



— Read more in Jacopo Buongiorno et al., “Offshore Small Modular Reactor (OSMR): An Innovative Plant Design for Societally Acceptable and Economically Attractive Nuclear Energy in a Post-Fukushima, Post-9/11 World” (paper presented at the ASME 2014 Small Modular Reactors Symposium, Washington, D.C., 15-17 April 2014), [ASME Digital Collection](#), Paper No. SMR2014-3306, pp. V001T01A001

The military option against Iran: Not a single strike, but a sustained campaign

Source: <http://www.homelandsecuritynewswire.com/dr20150703-the-military-option-against-iran-not-a-single-strike-but-a-sustained-campaign>

July 03 – If negotiations in Vienna to curb Iran’s nuclear program fail, and if at some point a strike on Iran’s nuclear facilities would be deemed necessary, the U.S. Air Force’s new, 30,000-pound Massive Ordnance Penetrator bomb would likely be used to target nuclear facilities buried deep

ton bunker busting bombs – the largest non-nuclear ordnance ever created – developed for the purpose of destroying deeply buried targets.

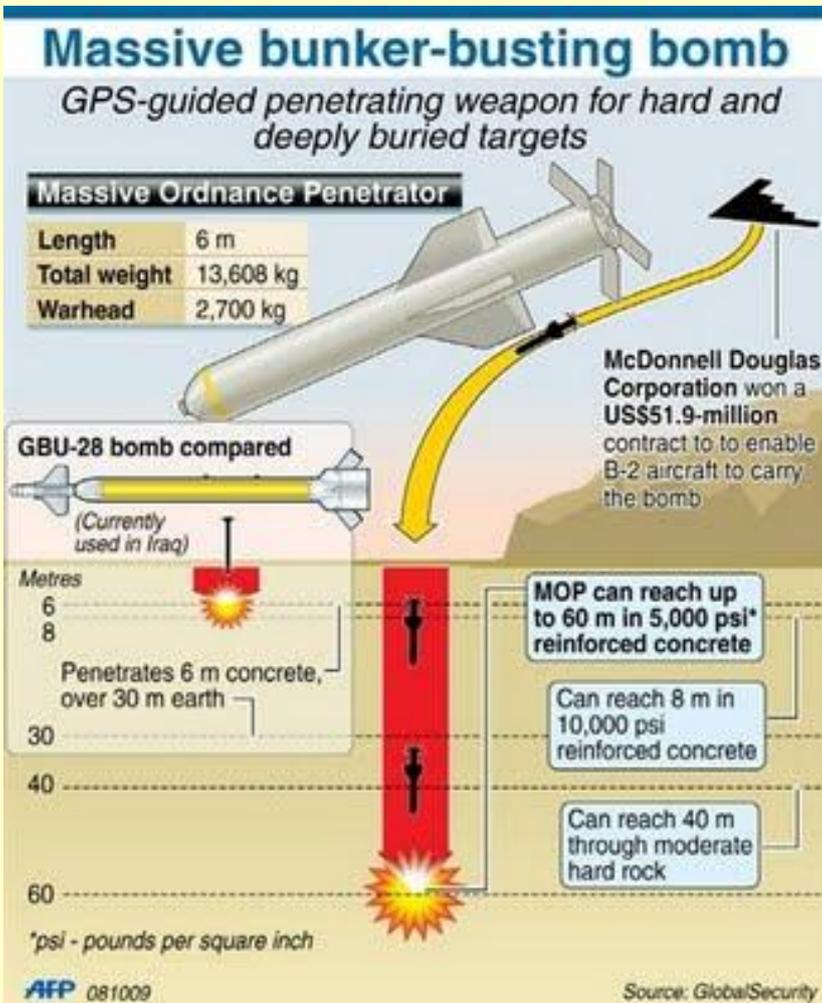
“The military option isn’t used once and set aside,” said Army General Martin Dempsey, chairman of the Joint Chiefs of Staff. “It remains in place, so we will always have options and the massive ordnance penetrator is just one of them.”

President Obama has frequently said that he is not ruling out any options for dealing with Iran’s nuclear program. Some hawks in the Senate argue that military action against Iran would take only a matter of days.

Some in the American intelligence community, however, have concluded that a military strike on Iran’s nuclear facilities would do little to halt the nuclear program for any length of time. “[The] U.S. strikes might set Iran’s program back two-to-four years, but it can’t destroy it,” said Senator Angus King (I-Maine). “You can’t bomb knowledge out of them, and probably all doubt would be erased that Iran would respond by pursuing a nuclear weapons program.”

Others agreed that a military strike would achieve little beyond a temporary disruption of Iran’s program. “A single military strike would only delay an Iranian drive for a finite period so a credible military option would have to envision a long-term campaign of repeated follow-up strikes

as facilities are rebuilt or new targets identified,” said Kenneth Katzman, a Middle East analyst for the Congressional Research Service. “This is within the U.S. capability, but would require



10

underground.. There are those, however, who question for how long such an attack would halt the Iranian programs.

As Bloomberg reports, the 509th Bomb Wing of the Air Force is now equipped to carry the 15-



policy consistency and sustained determination across several U.S. administrations. What is crucial is not the bomb, but a multiyear campaign of vigilance and precise intelligence of new targets.”

Former secretary of defense Robert Gates noted in April 2009 that air strikes “will only buy us time and send the program deeper and more covert.” Bombing “would also bring together a divided nation and make them absolutely committed to obtaining nuclear weapons.”

Among the potential targets would be a fuel enrichment complex in Natanz, a heavy water reactor facility near Arak, and a uranium conversion facility along with research reactors

east of the city of Esfahan. The toughest target, U.S. military and intelligence officials have said, is the Fordow site, buried deep beneath a mountain about twenty miles from the holy city of Qum.

While the threat of force is real, others see the bomb as more of a bargaining chip in the current negotiations.

“We have the capability to shut down, set back and destroy the Iranian nuclear program,” said Defense Secretary Ashton Carter. “And, I believe the Iranians know that and understand that.”

The talks in Vienna are expected to extend until 7 July, when diplomats are planning to draft a final agreement.

The EMP threat: is enough being done?

Source: http://www.army-technology.com/features/featurethe-emp-threat-is-enough-being-done-4605258/?WT.mc_id=WN_Feat

An open letter to US President Barack Obama from the EMP Task Force has outlined that the US should, as an urgent requirement, address the threat of an electromagnetic pulse (EMP) attack by protecting its critical infrastructure. So, how real is this threat and what are countries doing to counter it?

Signed by a number of military specialists, a letter from the EMP Task Force, delivered to the White House last month, claims that an EMP attack - a radio wave that damages and destroys electronic systems - would bring the US economy to a halt.

The signatories note: **“The consequent failure of critical infrastructure that sustains our lives is a major national security threat and would be catastrophic to our people and our nation.”** Hard-hitting words, indeed.

As well as this, a 2012 document from the US Intelligence Council, entitled Global Trends 2013, highlighted an EMP attack as one of eight 'Black Swan' events - in other words something that could irrevocably damage civilisation as we know it.

NASA has claimed that the chance of a geomagnetic storm - a form of natural EMP - hitting Earth is 12% per decade. In 2012 a similar storm narrowly missed Earth and the Carrington event of 1859 caused electrical currents to surge through telegraph systems.

On top of natural disasters is the threat of manmade nuclear weapons. If detonated in the

sky, the resultant explosion would produce electromagnetic radiation.

Such a scenario was first demonstrated in 1962 when the US detonated a bomb at a height of 240 miles in the Pacific Ocean. The after-effects caused telephone outages in Hawaii and damaged streetlights.

More recently, in 2013 it was reported that North Korea was developing an EMP weapon. The Task Force letter also states that Russia and China have nuclear EMP capabilities, with Russia actively developing a super-high-frequency gun that can deactivate unmanned aerial vehicles and precision weapons.

The threat was further highlighted in March, when a secret Iranian military document described a potential nuclear EMP attack in 20 different locations in the US.

However, one of the biggest players in the EMP game is the US itself, with the country's air force announcing in May that the Counter-electronics High-powered microwave Advanced Missile Project can be deployed using the Joint Air-to-Surface Standoff Missile-Extended Range.

Countering the threat

There is no doubting the seriousness with which the signatories believe in the threat and their recommendations, which include protecting nuclear reactors.

In an article for the Wall Street Journal last year, Dr Peter Vincent Pry, who



served on the EMP Commission - set up to study the nature and magnitude of potential high-altitude EMP threats, among other things - and James Woolsey, chairman of the Foundation for Defense of Democracies and a former director of the CIA, wrote that "literally millions of American lives could depend" on increased protection against EMPs. So what can be done?

One course of action is called hardening.

This involves designing, or modifying, electronic systems to cope with a pulse by using thicker conductors. The Task Force urges Obama to insist that such technology be used on the electrical grid, as it has been by the Department of Defense for nuclear systems and military installations. This includes surge arrestors and Faraday cages, as well as micro-grids.

The cost of these upgrades for the national grid was estimated at \$2bn in 2008 by the EMP Commission.

UK MPs warned in 2012 that the potential impact of an EMP weapon "could be devastating and long-lasting for UK

infrastructure", adding it was "vitally important that the work of hardening infrastructure is begun now and carried out as a matter of urgency".

In 2013 Republican Representative Trent Franks introduced the Critical Infrastructure Protection Act, but according to the US Congress website the last action of the bill was referral to the Committee on Homeland Security and Governmental Affairs.

In the same year the Fraunhofer Institute in Germany unveiled a device that detects the strength, frequency and location of an attack, but this would only be useful for small-scale attacks.

What this points to, however, is a general lack of forward planning when it comes to civilian infrastructure. While it could be claimed that the EMP Task Force letter is exaggerating the threat, the consequences of not protecting at least the critical elements such as nuclear reactors are vast.

The EMP catastrophe may never materialise, but it's wiser to plan as if it will rather than burying our heads in the sand.

Researchers pin down risks of low-dose radiation

Nature 523, 17–18 (02 July 2015)

Source: http://www.nature.com/news/researchers-pin-down-risks-of-low-dose-radiation-1.17876?utm_content=17377783&utm_medium=social&utm_source=linkedin

For decades, researchers have been trying to quantify the risks of very low doses of ionizing radiation — the kind that might be received from a medical scan, or from living within a few tens of kilometres of the damaged Fukushima nuclear reactors in Japan. So small are the effects on health — if they exist at all — that they seem barely possible to detect. A landmark international study has now provided the strongest support yet for the idea that

long-term exposure to low-dose radiation increases the risk of leukaemia, although the rise is only minuscule (K. Leuraud *et al. Lancet Haematol.* <http://doi.org/5s4>; 2015).

The finding will not change existing guidelines on exposure limits for workers in the nuclear and medical industries, because those policies already assume that each additional exposure to low-dose radiation brings with it a slight

increase in risk of cancer. But it scuppers the popular idea that there might be a threshold dose below which radiation is harmless — and provides scientists with some hard numbers to

quantify the risks of everyday exposures.

"The health risk of low-dose radiation is really very tiny, but the public is very concerned," says Bill Morgan, who heads a systems-biology programme in low-dose radiation at the Pacific Northwest National Laboratory in Richland, Washington, and chairs the

committee on radiation effects at the International Commission on Radiological Protection (ICRP) in Ottawa, Canada. That concern has driven a lot of investment in programmes trying to quantify the risk, he says. The European Commission, for example, has a 20-year road map



to assess the problem. “We don’t do a very good job of explaining ourselves to the public, which finds it hard to put radiation risks in context — some people go to radon spas to treat their rheumatism while others won’t board planes for fear of cosmic rays,” he adds.

Ionizing radiation — the kind that can pull electrons from atoms and molecules and break DNA bonds — has long been known to raise the risks of cancer; the higher the accumulated dose, the greater the damage. But it has proved extremely difficult to determine whether this relationship holds at low doses, because any increase in risk is so small that to detect it requires studies of large numbers of people for whom the dose received is known. A study of more than 300,000 nuclear-industry workers in France, the United States and the United Kingdom, all of whom wore dosimeter badges, has provided exactly these data. A consortium of researchers coordinated by the International Agency for Research on Cancer (IARC) in Lyon, France, examined causes of death in the workers (one-fifth of whom had died by the time of the study) and correlated this with exposure records, some of which went back 60 years.

The workers received on average just 1.1 millisieverts (mSv) per year above background radiation, which itself is about 2–3 mSv per year from sources such as cosmic rays and radon. The study confirmed that the risk of leukaemia does rise proportionately with higher doses, but also showed that this linear relationship is present at extremely low levels of radiation. (Other blood cancers also tended to rise with radiation doses, but the associations were not statistically significant.) The results were published on 21 June.

“The health risk of low-dose radiation is really very tiny, but the public is very concerned.”

“It is a solid, unusually large study of individuals exposed to very low doses of ionizing radiation,” says epidemiologist Jørgen Olsen, director of the Danish Cancer Society Research Center in Copenhagen. The finding implies that some cases of leukaemia will even be caused by a high level of natural background radiation, he adds, “though the increased risk for an individual is going to be vanishingly small”.

ICRP recommendations, which most national radiation-protection agencies follow, already call for monitoring of individuals whose annual exposure is likely to exceed 6 mSv. They

restrict exposure to 20 mSv annually over 5 years, with a maximum of 50 mSv in any one year. Researchers expected that 134 of the workers (4.3 per 10,000 people) would die from leukaemia as a result of the average 27 years they spent in the industry; in fact, 531 people died from the disease. Even in this large study, there was no direct evidence that workers who had accumulated extremely low doses of radiation (below a total of 50 mSv) had an increased risk of leukaemia, says Olsen. But a mathematical extrapolation of the data suggests that each accumulation of 10 mSv of exposure raises a worker’s risk of leukaemia by 0.002%.

The data also challenge an ICRP assumption that accumulated low-dose exposure gives a lower risk of leukaemia than does a single exposure to the same total dose (based on the idea that the body has time to recover if the assault comes in tiny, spread-out doses). But such details are unlikely to change the overall ICRP recommendations, which are deliberately conservative, says Thomas Jung, from Germany’s Federal Office for Radiation Protection in Munich.

Medical scans

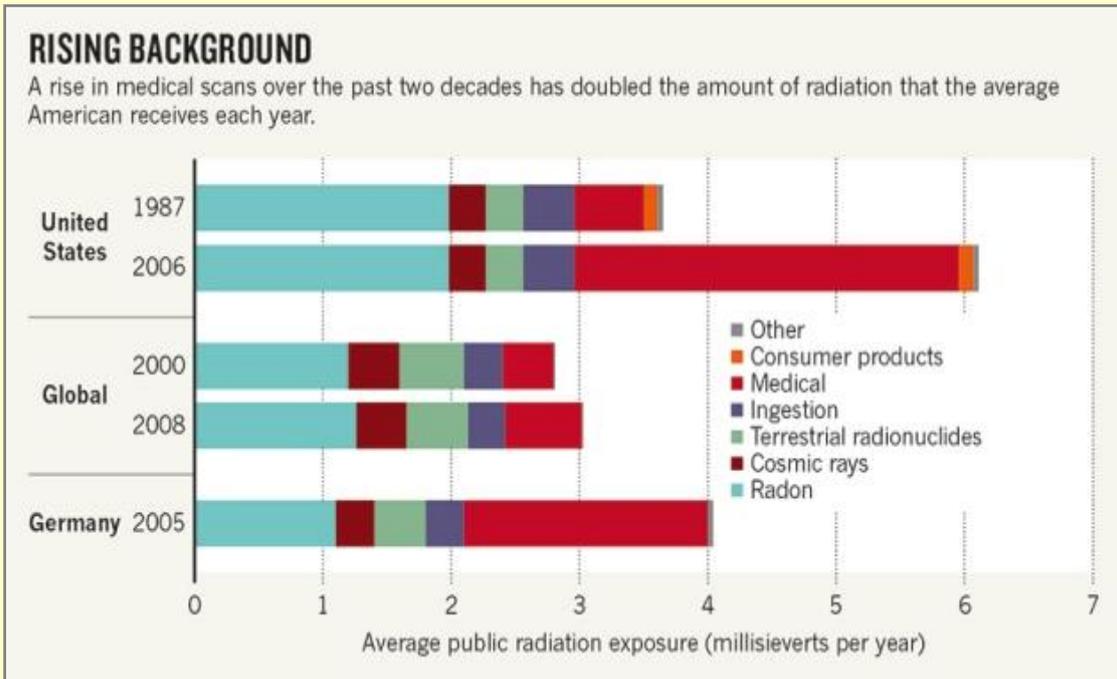
A major, and increasing, source of low-dose radiation comes from the medical world, says David Richardson, an epidemiologist at the University of North Carolina and an author of the study. “The amount of radiation a US person receives in a year on average has doubled, mostly because of medical procedures,” he says. Computed-tomography (CT) scans are to blame for most of the rise; a typical abdominal scan delivers more than 10 mSv. Radiologist David Brenner of Columbia University in New York has calculated that of the 25 million people having CT scans in a year, 1 million will have accumulated more than 250 mSv over the previous 20 years.

One group that needs to pay particular attention to the findings are the tens of thousands of health workers who use radiological imaging to guide catheters through blood vessels of patients to reach into their hearts and brains, says Martha Linet, at the US National Cancer Institute’s radiation epidemiology programme in Bethesda, Maryland. These minimally invasive operative procedures are used ever more frequently, she says.



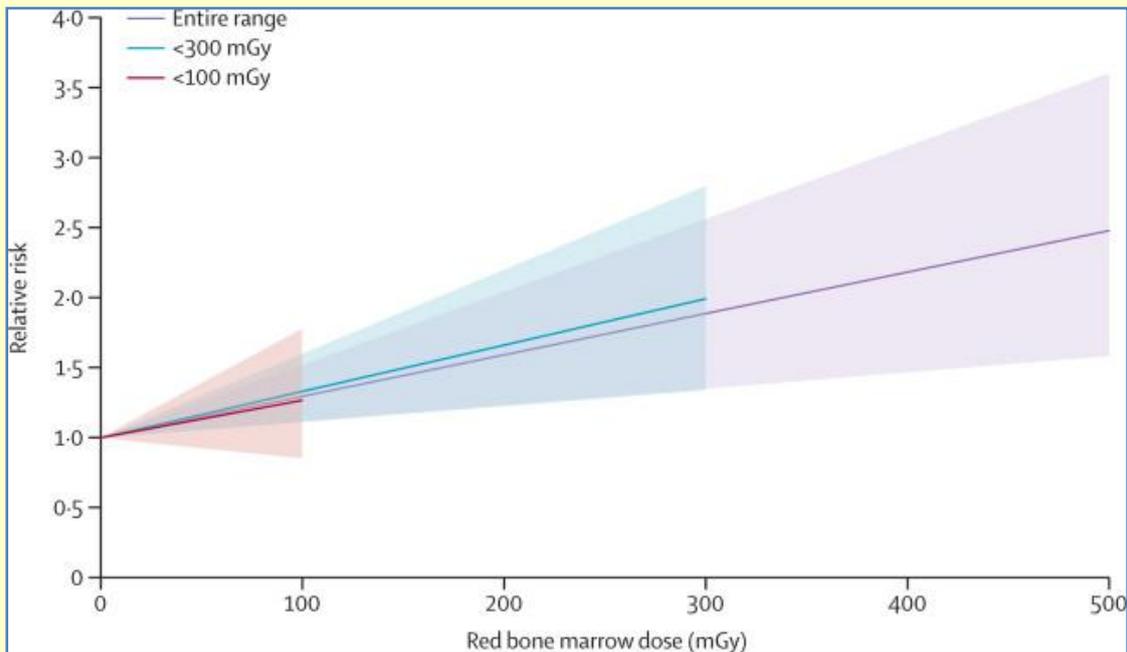
Epidemiological studies suggest that radiation exposure has health effects beyond cancer.

the Epi-CT study, is recruiting one million people from nine European countries who had



UN Scientific Committee on the Effects of Atomic Radiation

CT scans as children; its analysis will be complete by 2017. In another, the Helmholtz Center Munich is analysing heart tissue from



Relative risk of leukaemia excluding chronic lymphocytic leukaemia associated with 2-year lagged cumulative red bone marrow dose

workers who died in the Mayak uranium mines in the South Urals, Russia.

The IARC-led consortium is now looking at the effect on solid cancers, and also on diseases such as heart attack and stroke. Other studies are under way to study the long-term impact of low-dose radiation on different cohorts. One,

Although the European Commission has been funding research on low-dose radiation for some time, equivalent programmes in the United States have stalled. In 2013, scientists wrote an open letter to the White House Office of Science and Technology Policy calling for renewed



investment, and a bill is currently being debated in Congress calling for more work.

Getting funding for such studies is important, says Mike Atkinson, head of radiation biology at the Helmholtz Center Munich. Being able to quantify the effects of radiation will help doctors to balance risk against benefit when deciding

whether to put children in CT scanners, he says. And further understanding the health impacts of low-dose radiation might aid decisions about how much remedial activity is needed to clean up soil contaminated by radioactivity from accidents or nuclear-power works, says Morgan.

► Read also the comments for this article at source's URL.

Why the 'dirty bomb' scenario is a realistic threat for homeland terrorism

Source: <http://www.worldtribune.com/2015/07/03/why-the-dirty-bomb-scenario-is-a-realistic-threat-for-homeland-terrorism/>



As the U.S. enters the July 4 weekend and the summer travel season with numerous large public gatherings and celebrations, law enforcement and

intelligence officials this year are confronting many types of potential terrorist threats but perhaps the most unusual is a dirty bomb attack.

Some commentators such as Rep. Peter King during his July 1 appearance on a Fox News show made remarks that appeared to confuse a nuclear attack with a dirty bomb attack.

The differences are significant. A nuclear detonation would cause massive damage, the combination of blast, heat and radiation capable of killing tens of thousands depending on the size (yield) and location of the detonation.

Dirty bombs have qualities attractive to terrorists and thus present an immediate security threat at a time when the Islamic State of Iraq and Levant (ISIL) is mounting a global offensive using social media to recruit, groom and direct remote actors.

The good news — if that description fits — is that nuclear weapons in the U.S. are accorded extensive albeit far from perfect security. In addition, there are a series of technical barriers that must be crossed before a nuclear weapon can be detonated.

Dirty bombs are almost the polar opposite of the consequences of a nuclear blast.

In a dirty bomb attack there is virtually no physical destruction. One possible dirty bomb scenario would involve the use of



conventional explosives to disperse a small amount of radioactive material into the atmosphere, hoping winds would carry the radioactive material over some distance — one mile is a reasonable estimate — again depending on conditions.

There are hundreds if not thousands of radioactive sources that serve useful and even important roles in various commercial and medical settings. Many of those sources have little utility in making a dirty bomb but there are exceptions.

In the early part of the last decade the threat reduction program I was running at the Department of Energy received congressional funding to begin a radioactive security program. Our mandate was to work with overseas partners, beginning with Russia, which had a massive inventory of unprotected sources located in central repositories scattered around the country at what the Russians called Radon sites.

This was an era of cooperation with Russia and I directed our experts to move as quickly as possible to set in place a process to secure those sites.

Doing so required assistance from the Russian government and also the International Atomic Energy Agency which supported our efforts. Before so doing we wanted to understand more about the most deadly sources and asked our experts to assess the situation more closely to identify those sources of greatest concern.

A list of about two dozen radioactive sources was identified. Subsequently, in the open media some of those sources also were identified and can be found on various websites. Unfortunately, after my departure from the energy department



the program lagged badly for years due to bureaucratic mischief.

Today the situation is not much improved than when I found it. There also are security vulnerabilities within the U.S. that remain unaddressed.

The dirty bomb scenario described above is low cost and low-tech. It also achieves, through the spread of radioactivity, not only physical harm to those who may ingest some of the radioactive particles but potential broader panic in the area where the radioactive material was released. Publicity is the life blood for terrorists

and such an attack would generate global headlines.

Finally, the disruption caused by such an attack invariably would cause considerable and potentially lasting economic consequences. Few would want to shop or eat in an area known to have been involved in a dirty bomb attack.

For this reason areas such as the Mall and surrounding area in Washington, DC and central Manhattan in New York City would be attractive targets for such a dirty bomb attack.

iPIX - Ultra Portable Gamma-Ray Imaging System

Source: http://www.canberra.com/products/insitu_systems/gamma-imaging-systems.asp

iPIX is a unique gamma imager that quickly locates and identifies low level radioactive sources from a distance while estimating the dose rate at the measurement point in real time. It is the ideal tool to map a radioactive area before entering the zone, thus reducing the dose exposure (ALARA) during standard operation or decommissioning. iPIX is also the appropriate instrument to detect any suspicious radioactivity in security and safeguard applications, as well as for emergency situations such as Fukushima.



Technology

iPIX integrates the GAMPIX technology developed by the Atomic Energy Commission (CEA) in France. It is based on a 1 mm CdTe detector bonded to a pixilated CMOS chip – the Timepix sensor developed at the CERN research center – a coded mask and mini optical-camera.

The coded mask aperture allows for background noise subtraction by means of a technique called mask/anti-mask differentiation. This greatly contributes to the reduced size and weight of the gamma imager. The mask automatically rotates to the anti-mask position based on the measurement conditions (background and source activity). The radioactivity mapping is automatically superimposed onto the visible image of the scene of interest.

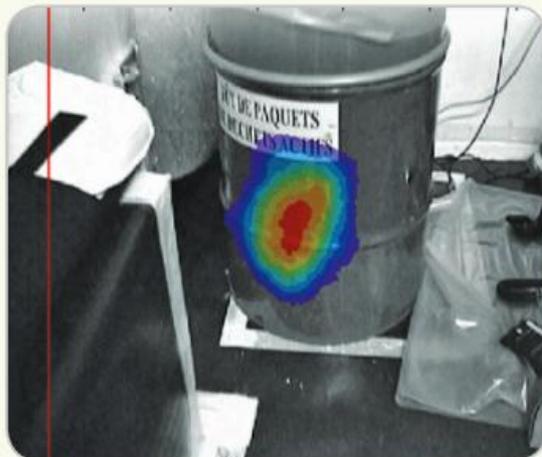
Application

iPIX is a real-time ultra-portable gamma-ray imaging system mostly designed for in situ

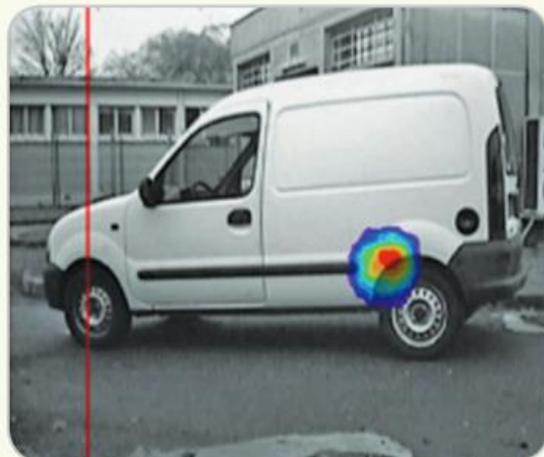
gamma measurements to locate radioactivity at nuclear sites. When planning for maintenance or decommissioning operations, it can be used to provide radiation intensity maps of the area. During radiological accidents, emergency situations, reactor outages or even routine area surveys where radiological conditions are subject to change (e.g., near piping), iPIX can help find radiological hot spot locations and quickly determine the boundaries of contaminated areas.



iPIX requires very little shielding while maintaining an excellent signal to noise ratio. This translates into



Waste measurement.



Illicit nuclear material trafficking.

a lightweight device (2.35 kg/5.5 lb) with a compact design (9 x 9 x 18.8 cm/3.5 x 3.5 x 7.4 in.) that can easily be deployed and transported in the field. The camera can be installed on a standard or motorized tripod that allows remote positioning of iPIX to focus on the area of interest.

Features

- Complete tool for in situ gamma imaging, saving time, cost and dose
- Real-time acquisition and immediate display
- 2.35 kg/5.5 lb camera
- Excellent spatial resolution for localization of gamma-ray emitters
- High detection sensitivity even at low energies
- IP65 rated, fully decontaminable
- Battery, POE or direct powered
- Remote control and operation
- Single Ethernet cable between tablet PC and camera (up to 80 m long)
- Three coded masks available for optimized response (optional)
- Fully rugged convertible notebook
- User-friendly software

Benefits

- Compact size and lightweight for ultra portability
- Best tool to track low energy emitters (safeguards, security, fuel cycle)
- Industrial design for use in harsh environments
- Fosters the ALARA principle: Can be operated remotely minimizing exposure to the operators.
- User friendly, with push button image acquisition
- Automatic parameter settings for non-expert users
- High performance to quickly and precisely locate hot spots
- Estimates dose rate at the measurement point
- Ideal for robotic applications

Concerns grow about Syria's nuclear materials

Source: <http://www.homelandsecuritynewswire.com/dr20150706-concerns-grow-about-syria-s-nuclear-materials>

July 06 – **The destroyed Al Kibar reactor site in Syria – it was destroyed by Israel in September 2007 — is now under the control of ISIS, which is apparently dismantling and possibly conducting excavation activities at the site. ISIS's intentions are unknown.** There is no new information about Syria's supply of uranium which would have been used in the destroyed reactor, although it is not believed to be at the reactor site or in the

hands of ISIS. New information adds support that Syria intended to build a plant to separate plutonium from the reactor's irradiated fuel. Researchers at the Washington, D.C.-based Institute for Science and International Security write that although Syria is no longer believed to have an active, secret nuclear reactor program at this time, it is believed to be hiding assets associated with its past undeclared nuclear efforts. These

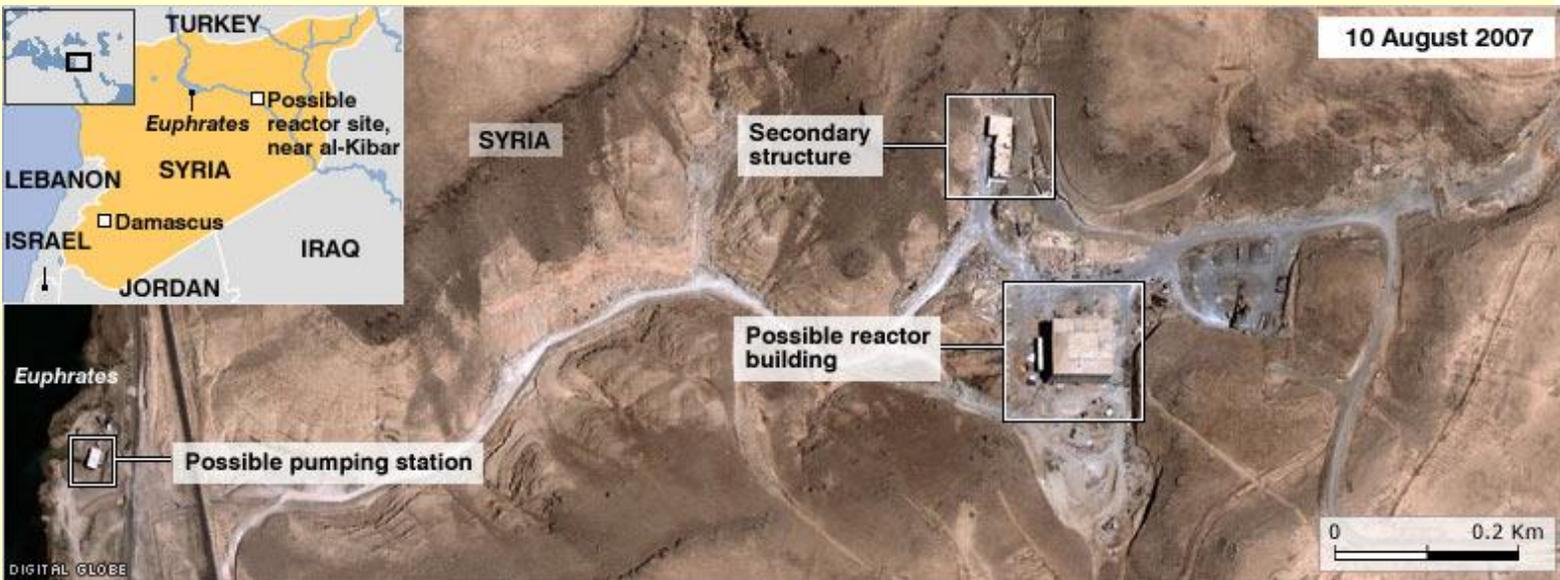


unresolved nuclear concerns, coupled with the deteriorating security situation in Syria caused by the on-going civil war and advances by ISIS, is a continued source of concern about the security of any nuclear materials, including an alleged large stock of natural uranium, nuclear-related equipment, and nuclear scientists and engineers still present in the country.

The researchers write that the natural uranium, believed to exceed 50,000 kilograms, is not as readily usable as Syria's past chemical weapons stockpile, because it requires further enriching to be usable in a nuclear weapon. This amount of natural uranium would be enough, if enriched to weapon-grade, for at least 3- 5 nuclear weapons.

did it have designs for a plutonium separation plant and some of the necessary equipment? Who controls the remains? What can the International Atomic Energy Agency (IAEA) do, other than providing its past assessment that the bombed site was likely a gas-graphite reactor large enough to support a small nuclear weapons program?

The remnants of Syria's undeclared nuclear program pose a proliferation risk. Albright et al. note that any known or suspected nuclear materials inside Syria are not as readily usable as a chemical weapons stockpile. For example, natural uranium is not readily usable in a nuclear weapon unless it is further enriched to highly enriched uranium (HEU) or put in a reactor to make plutonium and subsequently



Background

In September 2007 Israel destroyed the Al Kibar nuclear reactor in north-east Syria, which the Assad regime was building with the aid of North Korea. Nuclear experts say that although Syria is no longer believed to have an active, secret nuclear program, it is believed to be hiding and retaining assets associated with this past undeclared nuclear reactor effort. David Albright and colleagues at the Institute for Science and International Security write that such a reactor is accompanied by a range of nuclear and other materials, such as natural uranium, specialized equipment, expertise, and know-how. Where, then, are the remains of this program? Where is the natural uranium fuel for the reactor? What has become of the scientists and engineers assigned to the program? Was Syria planning to separate the plutonium? If so,

separated from the irradiated fuel. Natural uranium is a weak radioactive source and thus a poor choice for a dirty bomb. Nonetheless, the allegedly large stock of natural uranium, other nuclear-related materials, equipment, and other resources associated with the past nuclear program would be attractive to terrorists, certain states, and commodity traffickers. They may wish to sell these goods on the black market or otherwise seek to use them to extract concessions or cause damage. This material may also end up in undeclared nuclear programs of other states.

Albright and his colleagues have written a report to update the situation with new, albeit limited, information. It is a follow-on to earlier reports by the Institute for Science and International Security. The authors recommend that Syria's nuclear assets, particularly those that were



part of its undeclared nuclear efforts, need to be located and placed under international monitoring or removed from the country. The authors of the report conclude that regardless of the purpose of Syria's nuclear reactor program at Al Kibar, the deteriorating

situation in Syria raises serious concerns about the security of nuclear material, equipment, and scientists. It is extremely important that Syria's nuclear assets are located and placed under international monitoring or removed from the country.

— Read more in David Albright et al., “[Syria’s Unresolved Nuclear Issues Reemerge in Wake of ISIL Advance and Ongoing Civil War](#)” (Institute for Science and International Security, 30 June 2015); and David Albright et al., “[Syria’s Past, Secret Nuclear Program Poses Proliferation Risks](#)” (Institute for Science and International Security, 12 September 2013).

Mitchie Takeuchi and Miyako Taguchi: Second-generation survivors of the atomic bomb

Bulletin of the Atomic Scientists July/August 2015 vol. 71 no. 4 1-9
 Source: <http://bos.sagepub.com/content/71/4/1.abstract>

Abstract

Mitchie Takeuchi’s mother and grandfather survived the atomic bombing of Hiroshima 70 years ago. Miyako Taguchi’s parents survived the bombing of Nagasaki three days later. Takeuchi and Taguchi both are part of the second generation (and in Takeuchi’s case also the third generation) of **hibakusha**—the Japanese term for people who were exposed directly to one of the two bombings or their radioactive fallout or who were exposed while still in their mothers’ wombs. Although many *hibakusha* have been reluctant or unwilling to discuss the bombings with their children, some have not only talked about their experiences with family members but also become active in groups such as Hibakusha Stories—which brings survivors into New York City schools to discuss their experiences with students. In this pair of interviews, Takeuchi and Taguchi talk about what it’s like to be the child of a survivor and why they feel a responsibility to share their family stories and to speak out about nuclear weapons.



Statement by President Donald Tusk on the agreement on Iran's nuclear programme

European Council: 14/07/2015
 Source: <http://www.consilium.europa.eu/en/press/press-releases/2015/07/14-tusk-statement-agreement-iran/>

The agreement reached today in Vienna represents a breakthrough, bringing to an end a 13-year nuclear standoff.



If fully implemented, the agreement could be a turning point in relations between Iran and the international community, paving the way to new avenues of cooperation between the EU and Iran. Geopolitically, it has the potential to be a game changer. All the parties who worked so hard to achieve this agreement deserve our congratulations, in particular High Representative

Federica Mogherini, whose relentless facilitation of the talks among the three EU partners, the US, Russia and China is evidence of the constructive role the European Union plays in global affairs. The text of the agreement is precise; we must now join forces to see it through, taking into account regional sensitivities.



How Will Inspections Work in Iran under the Nuclear Deal?

Source: <http://www.iranwatch.org/our-publications/nuclear-iran-weekly/how-will-inspections-work-iran-under-nuclear-deal>

President Barack Obama, speaking this morning from the White House after the successful conclusion of talks in Vienna, declared that the nuclear agreement with Iran “is not built on trust; it is built on verification.” Addressing an issue that had been a key sticking point in the negotiations, President Obama said that inspectors from the International Atomic Energy Agency (IAEA) will “be able to access any suspicious location. Put simply [...] the IAEA will have access where necessary, when necessary. That arrangement is permanent.”[1]

But what does “where necessary, when necessary” mean in practice? How will inspections work under the nuclear deal described in today’s Joint Comprehensive Plan of Action? And will this inspections regime actually be “permanent”?

IAEA-led Inspections Teams

- The IAEA will have the responsibility of monitoring and verifying the nuclear-related provisions of the agreement. The Agency will provide regular updates to the IAEA Board of Governors and to the U.N. Security Council.[2]
- The IAEA will have a team of 130-150 designated inspectors for Iran. According to the agreement, Iran “will generally allow the designation of inspectors from nations that have diplomatic relations with Iran”—meaning Iran would bar inspectors from the United States and could also wield limited veto power over certain inspectors.[3]
- IAEA inspectors will have access to “modern technologies,” including automated data collection, electronic seals, on-line enrichment measurement, and other advanced surveillance equipment for real-time monitoring.[4] Inspectors will no longer have to rely upon older technologies, such as metallic seals, and the manual gathering and transmission of data to IAEA headquarters in Vienna—a process that takes days.[5]
- IAEA inspection teams will be able to access “locations of intended use of all items, materials, equipment, goods and technology” imported through a dedicated nuclear procurement channel.[6]

20

How will routine inspections work in Iran?

- Inspections will be governed by Iran’s standard Safeguards Agreement with the IAEA, as well as the Additional Protocol, which Iran has agreed to “provisionally apply.” Iran is not required to “seek ratification” of the Additional Protocol for up-to 8 years.[7] The Additional Protocol allows for broader access to nuclear-relevant sites, such as uranium mines and heavy water production plants.
- Iran has agreed to fully implement the IAEA’s modified Code 3.1, which requires countries to submit design information for new nuclear facilities as soon as the decision is made to construct or authorize construction of the facility.[8]
- Iran has also agreed to further “transparency measures” that go beyond the Additional Protocol, including: IAEA monitoring of uranium ore concentrate produced at all uranium mills for 25 years and containment and surveillance of centrifuge rotors and bellows for 20 years. All existing and newly produced rotors and bellows will be inventoried and verified. In addition, Iran will declare and the IAEA will continuously monitor equipment used for centrifuge production.[9]

How will the IAEA access suspicious, undeclared sites in Iran?

One of the most contentious issues in the talks was the authority the IAEA would have to access suspicious sites in Iran not officially declared as part of the country’s nuclear program—including military sites.

In practice, under the terms of deal, inspections “where necessary, when necessary” translates to: inspections where necessary, within 24 days, if five of the parties to the deal agree, for a period of 15 years.

Here are the steps for the inspections process related to undeclared sites[10]:



- “Request for clarification” (Day 0): If the IAEA has concerns about undeclared nuclear activities or sites, or any potential violations of the agreement, it will first “provide Iran the basis for such concerns and request clarification.”
- “Request for access” (Days 1-14): If Iran’s explanations do not satisfy the IAEA, the Agency may submit a request to access the suspicious sites in question. The IAEA “will provide the reasons for access in writing and make available any relevant information.” Within 14 days, Iran and the IAEA must either 1) agree on the procedures to inspect the sites in question, or 2) resolve the IAEA’s concerns by alternative arrangements without inspections.
- “Dispute resolution” (Days 15-21): If Iran and the IAEA cannot reach a resolution within 14 days of the IAEA’s request for access, the issue will be brought before the Joint Commission established by the agreement for dispute resolution. A consensus of 5 of the 8 members of the Joint Commission (the P5+1 nations, plus Iran, plus the EU High Representative) would issue a ruling and determine the course of action within 7 days. This means, Iran, China, and Russia could not block a consensus without the support of one Western country.
- “Implementation” (Days 22-24): Following the determination of the Joint Commission, Iran would have 3 additional days to implement the decision.

Will this inspections regime be permanent?

It appears not. The section of the agreement summarizing the “transparency measures” that Iran will implement includes: “a reliable mechanism to ensure speedy resolution of IAEA access concerns for 15 years”[11]—the mechanism described above. In describing IAEA inspections as “permanent,” President Obama could have been referring to the implementation of the IAEA’s Additional Protocol, which is not time-limited by the agreement, but does not include the same dispute resolution mechanism for inspections.

What about the IAEA’s investigation of “possible military dimensions” to Iran’s nuclear program?

These questions are meant to be resolved by the IAEA, with Iran’s cooperation, before the end of the year.

According to a [“road map”](#) signed today by the IAEA Director General and the head of Iran’s Atomic Energy Organization:[12]

- Iran will submit a written explanation to the IAEA by August 15. This submission will address all 12 allegations of military-nuclear work described by the Agency in its November 2011 report.
- The IAEA will then review Iran’s explanations and submit questions by September 15, after which both sides will meet and discuss ways to resolved remaining “ambiguities.”
- The road map refers to a “separate arrangement” regarding access to the controversial Parchin site, a military complex linked to nuclear explosive testing.
- All questions must be resolved by October 15, after which the IAEA will prepare a “final assessment” of PMD issues, which the Agency’s director will present by December 15.

Iran’s compliance with the IAEA’s investigation, according to the timeframe set forth today’s road map, is listed as one of the “transparency and confidence-building measures” in the nuclear agreement.

Footnotes

[1] Full text of President Obama’s remarks, July 14, 2015: <http://www.iranwatch.org/library/governments/United-states/executive-branch/white-house/statement-president-joint-comprehensive-plan-action>

[2] Joint Comprehensive Plan of Action (JCPOA), Preamble and General Provisions, July 14, 2015: <http://www.iranwatch.org/library/multilateral-organizations/european-union/joint-comprehensive-plan-action>

[3] JCPOA, Annex I, Section N, July 14, 2015.

[4] JCPOA, Annex I, Section N, July 14, 2015.

[5] For background on IAEA technology in Iran, see David E. Sanger and William J. Broad, “Awaiting Iran Deal, Nuclear Sleuths Gather Sophisticated Tools,” *New York Times*, July 6, 2015, http://www.nytimes.com/2015/07/07/world/middleeast/nuclear-inspectors-await-chance-to-use-modern-tools-in-iran.html?_r=0

[6] JCPOA , Annex IV, Section 6.7, July 14, 2015.

[7] JCPOA, Annex V, Section D, July 14, 2015.

[8] JCPOA, Annex I, Section L, July 14, 2015.



[9] JCPOA, Annex I, Sections O and R, July 14, 2015.

[10] JCPOA, Annex I, Section Q, July 14, 2015.

[11] JCPOA, Section C.15, July 14, 2015.

[12] IAEA Director General's Statement and Road-map for the Clarification of Past and Present Outstanding Issues regarding Iran's Nuclear Program, July 14, 2015: <http://www.iranwatch.org/library/multilateral-organizations/international-atomic-energy-agency/iaea-director-generals-statement-road-map-clarification-past-present-outstanding>.



The Deal with Iran: How to Make Lemonade out of Lemons

By Alexander H. Joffe

Source: <http://www.meforum.org/5380/iran-deal-lemonade>

July 14 – It is always perilous to predict what future historians will say. But regarding the nuclear deal with Iran, it is likely historians will observe the remarkable fact that at the moment of its greatest weakness, Iran's enemies suddenly reversed course. In the name of enticing it not to build nuclear weapons, they



dismantled years of carefully built economic and political sanctions, saved its crumbling economy, and empowered the regime against its domestic and foreign enemies, including the West itself.

Doing so they accepted Iran's attacks and insults, left its nuclear enrichment program intact and under minimal supervision, guaranteed Iranian threats to neighboring countries and efforts to expand regional hegemony, and did nothing to help the Iranian people, who struggled under harsh repression. Whether it will have succeeded in preventing Iran from building a nuclear weapon is unlikely. What is certain is that a new period of instability will have been created — that period is already upon us.

It is an extraordinary moment in world history, perhaps a turning point, based, as many such moments are, on an extraordinary convergence of lies and self-delusions. But for those interested in the two goals of an Iran free of nuclear weapons and free of religious fascism, perhaps it is also a moment of opportunity. **Iran is about to undergo a kind of opening to the world. Taking advantage of that is now a vital goal for Western intelligence and**

public diplomacy. It is the art of the making lemonade out of lemons.

Western businessmen are already flooding into Iran seeking deals, selling all manner of wares in exchange for Iranian cash. Those businessmen, the various branch offices they will establish, and the goods they will sell, represent an important opportunity for Western intelligence agencies to gather information and to subvert the Iranian regime.

One simple method are thumb drives, containing viruses to disrupt computer networks, encryption tools to evade official Iranian surveillance and firewalls, and perhaps even Western music, literature, and movies to subvert repressive traditional values, and classics of Western political thought to inspire Iranian society toward a liberal democratic



future. Jazz and rock, blue jeans and samizdat literature played roles in the collapse of communism; their 21st century analogs should be enlisted to help Iranian society reform itself.

In reality, this sort of 'subversion' should have been an important goal for Western public diplomacy and intelligence work all along. But there is no evidence that significant efforts have been made, especially under the Obama administration. Iranian jamming of Western broadcasts and Internet censorship have been extensive and have gone unopposed



by the West, as has repression of dissidents and even the imprisonment of American citizens.

New access in Iran means new opportunities to introduce cyber weapons such as Stuxnet into Iran's strategic computer systems. Stuxnet and its variants were designed to slow and damage computer controlled systems in Iran's nuclear centrifuges, apparently with success. But they were eventually detected, and bizarrely, the Obama administration leaked information that led the trail back to the US. Iran's computers were hardened against attack.



New cyber weapons aimed at Iran's nuclear program, along with missiles, military radars and aviation, regime communications and record-keeping, and much more, are all likely under development in the West — or should be. Certainly Iran is developing its own cyber weapons, and has virtually unlimited access points to introduce them. But its weapons are aimed Western banks and critical infrastructure, such as electric grids. It is in everyone's interest that more targeted cyber attacks on the Iranian regime and its weapons systems succeed first.

More access to Iran increases its vulnerability, as will more trade. Iran has long acquired items legally and illegally, including computers, industrial machinery, and materials for its weapons programs. With increased trade come more opportunities to sabotage equipment by introducing computer viruses, contaminating materials used in specific industries, and delivering products that do not meet stated specifications. One result may be that nuclear weapons programs can be slowed and that computer and communications systems can be monitored and disrupted. Another is that all imported trade goods become suspect, requiring expensive counterintelligence

monitoring and testing. Openness should have a high price for Iran, both real and imagined.

Human intelligence opportunities directed against Iran will also increase, albeit slowly.

Businessmen and academics have always been spies, and opportunities to recruit spies and saboteurs. More fundamentally it will increase the opportunity to innocently distribute information about the West through direct contacts. Keeping track of Westerners will in turn require more Iranian counterintelligence efforts. Here, too, the costs of Iran's opening to the West should be made as high as possible.

Access to Iran's people also raises the potential to eventually inspire them to overthrow the repressive theocratic fascist regime. Iran's vulnerability to ethnic uprisings is often underestimated.

The Persian-led regime rightly fears Ahwaz Arab tribes in the southwest, ethnic Baluch and Pashtun in the east, and Azeris and Kurds in the northwest. All these have

long histories of rebellion against the Persians, and the regime is highly sensitive to the West stirring dissent.

More access will not easily bring such dissent about, much less the arming of ethnic dissidents.

Indeed, such activities seem utterly antithetical to the Obama administration, which could not even be moved to support the Green movement that arose after Iran's corrupt 2009 elections. But putting the regime under stress is an important means to bring about its transformation or demise. At the very least more broadcasts and translations should be aimed at these minorities, bringing them the news that they have not been forgotten by the West.

Even if the territorial integrity of Iran is somehow taken for granted by the West, the values of the regime cannot.

The rights of ethnic minorities in Iran, and human rights generally should become a Western demand, supported by tough negotiations and public diplomacy. Such demands featured prominently in American relations with the Soviet Union and should have an equally central place in dealings with Iran. Of course, they will not under Obama, but



perhaps they will under the next president. In all this, Iran's paranoia should be exploited to the fullest. The opening to the West is — or should be — a counterintelligence nightmare for Iran and they should be forced to devote scarce resources and increase internal repression to try and stay one step ahead. Iran's youth are already deeply alienated against the regime and to some extent Islam

itself. How to increase alienation is a paramount strategic goal for the West. More positively, the opening to Iran must be seen as an opportunity for the West to promote its own values, of openness, tolerance, liberty and human dignity. If it does not, then those values no longer exist in the West, just as they do not in Iran.

Alexander H. Joffe, a historian and archaeologist, is a Shillman-Ginsburg fellow at the Middle East Forum.

EDITOR'S COMMENT: Trade is one thing – and it is good. Changing a nation is another – and it is not good. Attempt to change Iraq – failed. Attempt to change Afghanistan – failed. Arab Spring – failed. And the last paragraph: openness, tolerance, liberty and human dignity (democracy is missing from the list): are we definitely sure that we still have these core values (on both sides of the ocean)?

Sensors can help railways detect, cope with electromagnetic attacks

Source: <http://www.homelandsecuritynewswire.com/dr20150715-sensors-can-help-railways-detect-cope-with-electromagnetic-attacks>

July 15 – Eleven years ago the Madrid train bombings proved how much European railway security still needed to be improved. Now that rail equipment — like in most other industries — is increasingly standardized and connected, however, another, more insidious type of offensive has become likely: electromagnetic (EM) attacks. An EU-funded project has developed detection technologies that can help the sector face this new threat.

Did you know that soon, there will be as many connected devices as there are humans on Earth? Five billion of these devices are now in use and this number is expected to reach twenty-five billion in 2020. Sure, each new type of connected device brings us closer to the advent of smart cities and all of their foreseen benefits. But on the other hand, as recent news has shown, it makes hackers and other tech enthusiasts with bad intentions a growing threat to security.

CORDIS reports that in the European railway sector for instance, the homogenization of network technologies and the increasing use of wireless communications have made the

scenario of an EM attack very likely. Communication jammers are easy to use and available for anyone to purchase on the Internet, which means that communications could potentially be jammed, with trains being delayed, blocked or even diverted.

To get the sector ready to face this new threat, the [SECRET](#) (SECurity of Railways against Electromagnetic aTtacks) project has developed a set of detection sensors capable of identifying EM attacks as they occur, so that rail equipment operators can switch the network to a “safe mode” immune to the specific type of EM attack being used.

Virginie Deniau, coordinator of SECRET, discusses with *research*eu results magazine* the likelihood of the EM attack scenario, the devices developed by her team and how the sector will soon need to adapt to this new reality.

How likely would you say is the EM attack scenario?

The definition of an EM attack evolves with the multitude of the applications based on wireless communication technologies. In the past, the EM attacks were based on the generation of high power intentional interferences (Electromagnetic pulse or high-power



microwaves) able to disrupt or damage electronic equipment. Today, the functions of this equipment can be triggered by a command or information transmitted by wireless links, which means it is now easier to disrupt the transmitted information and damage the equipment. Such attacks require a less powerful signal which can be generated by mobiles and other discrete devices.

So, from a technological point of view, the likelihood of an attack increases with the vulnerability of the infrastructures. However, it is difficult to establish a clear probability because today it is impossible to distinguish a technical failure from an EM attack. EM attacks based on relatively 'low' power signal involve disruptions but no permanent damage.

You mentioned mobile devices. Does that mean anyone is virtually capable of conducting such attacks?

The knowledge of the target is essential to define the means needed to perform an EM attack. Nowadays public communication jammers can easily be bought on the public market but their power and action are limited.

Now if we consider professional or security communication services, specific devices are generally required for such attacks. These devices are usually restricted to the professional market or have to be developed from scratch. While possible, this requires a certain level of skill and knowledge.

However, when these professional applications are supported by public wireless services, they can be disrupted by common jammers. So there is a real issue coming up, and the security and criticality of wireless services have to be seriously considered.

SECRET focuses on railway security. What could be the consequences of EM attacks in this sector?

The main direct risk is a perturbation of rail network traffic. It may be possible to prevent the departure of trains, force train stops and cause significant financial losses and unmanageable situations. However, it is difficult to accurately assess cascading risks, as they depend on the characteristics of each railway network (exploitation, infrastructure, applications, etc.).

Can you tell us more about the tools you developed?

SECRET's vision is that if we are able to detect an EM attack with certainty, we can imagine switching to a safe railway mode perfectly

adapted to the situation and allowing operators to regain control. The challenge is therefore to develop fast and reliable detection solutions. With this in mind several solutions have been studied under SECRET. Some could be implemented directly within the communication terminals and other would require dedicated devices but offer the advantage of being able to monitor multiple communication links.

In order to reach resilience, our detection sensors were coupled with an acquisition and decision terminal which was charged with analyzing the output of these detection sensors and commanding a reconfigurable telecommunication platform. According to sensors' output, the decision terminal directs the messages to be transmitted towards the communication link that's most resilient to the EM attack. Obviously, such an approach requires the deployment of several communication networks.

When do you expect SECRET's technology to reach the market?

Due to the mobility and the large spectrum of electromagnetic railway environments, the robustness and the total absence of fault of the detection solutions is difficult to demonstrate aboard a train. However, when the train is not moving, SECRET technologies can be really efficient. So we can envisage reaching the market relatively quickly with these technologies to protect train stations or other critical infrastructures.

In parallel, SECRET's technologies can contribute to the evolution of telecommunication standards employed in critical infrastructure. Instead of improving performance in terms of data rate, the standards can evolve to provide real-time information about the quality of services or the presence of jamming signals (intentional or unintentional). They could then provide relevant diagnostics and activate the adequate intervention process.

European railways are already under high economic and security-related pressure. Do you think the sector can bear the extra cost which the implementation of SECRET's solutions would involve?

I think that with this growing threat, it will be necessary to guarantee the resilience of the railway network against such attacks. Usually wireless communication systems only represent a small percentage of the budget of a railway project. However,



these systems are essential in operational and security plans. EM attacks can have dramatic consequences in terms of cost, and if they are easy to implement, they can also become frequent malicious actions. So a solution against EM attacks should be considered while balancing risks, impacts and investments.

What are your plans now that the project is close to its end?

We would like to test our analysis of EM attacks with other types of attacks such as physical or other cyberattacks. In fact, jamming

attacks can easily be employed in support of other malicious actions in order to avoid video or alarm transmissions. As a consequence, the risks analyses have to take into account potentially coupled physical and jamming attacks. We also think that the detection architecture for EM attacks proposed in SECRET should be coupled with other monitoring tools for infrastructure in order get a better grasp of what's happening on the network in real time.

Iran Nuclear Deal Makes War More Likely

By Efraim Inbar

Source: <http://www.meforum.org/5381/israel-iran-war>



There are (at least) six significant and immediate bad results from the agreement reached yesterday between the Western powers and Iran.

1. America the weak: The way in which the negotiations were conducted underscored the weakness of the US. The Obama administration was willing to offer almost unlimited concessions to the skillful Iranian negotiators, ignoring all its own deadlines and red lines. It is clear that President Obama was desperate for a deal in order to leave office with a "legacy."

While Washington congratulates itself on a "successful" result, what counts is the perceptions of the countries in the region. Alas, all countries in the region can only conclude that America is indeed weak. America has capitulated to Iran.

2. Nuclear legitimacy: Instead of insisting on the dismantling of all uranium enrichment facilities in Iran, as was accomplished in Libya,

the US actually accorded international legitimacy to a large-scale Iranian nuclear infrastructure, including thousands of centrifuges. The deal leaves almost intact all central components of the Iranian nuclear program. ... [T]he US has totally ignored UN Security Council Resolution 1696 of July 2006, which demanded that Iran suspend enrichment

activities, as well as American demands for the dismantlement of the nuclear facilities.

3. Proliferation: This agreement is a stimulus for nuclear proliferation. Indeed, Saudi Arabia has announced its desire for "the same type of infrastructure" that has been allowed to Iran. It is to be expected that countries such as Egypt and Turkey will emulate Saudi Arabia. These states share Iranian ambitions for a leadership role in the region and it is highly unlikely they will refrain from acquiring capabilities that match Iran's. Actually, the regional nuclear race has already begun and a multi-polar nuclear Middle East is on the way. This is a strategic nightmare.

An American attempt to provide a nuclear umbrella ("extended deterrence") to the Gulf States in order to forestall nuclear proliferation already has failed. Saudi King Salman refused to attend the US-Gulf State summit. This reflects disappointment with what Washington had to offer, and signals



Saudi intentions to try to take care of itself on its own.

4. Force projection and terrorism: The international sanctions regime against Iran already has eroded. States and businesses already are lining up to capitalize on the economic opportunities emerging in the Iranian market. The unfreezing of Iranian bank accounts and the projected increase in oil production will enrich the coffers of the Iranian regime with more than \$100 billion. This will allow the diversion of many resources to an Iranian arms build-up, and will buttress Tehran's aspiration to project force far beyond its borders. Moreover, the cash influx enhances Iranian capability for supporting proxies, such as the Shiite-controlled government in Iraq, Assad's regime in Syria, Hizballah in Lebanon, Hamas in Gaza, and the Houthis in Yemen. The Iranian capacity for subversion and for exporting terror will be greatly magnified.

5. Balance of power: The American decision to accept Iran as a nuclear-threshold state, and Obama's statements in favor of a "responsible Iranian role" in the region, accompanied by an inflated American threat perception of ISIS – signal a most significant change in American Middle East foreign policy. This accord marks an end to Iran's regional isolation. Instead, America seems to be siding with the Shiites

against Sunnis. This move changes dramatically the regional balance of power, instilling even greater uncertainty in regional politics.

The naïve American belief that Iran can become a "normal" state – will backfire. While cautious, Iran is nevertheless a "revisionist" power trying to undermine the status quo. It does not hide its hegemonic aspirations. Its subversive activities in Shiite Bahrain and the Shiite eastern province of Saudi Arabia (where most of the oil is), and in other Gulf countries, might create an unbearable situation for the West. Eventually, Iran might even attain its declared goal of putting an end to the American presence in the Persian Gulf.

6. Conflict with Israel: American policy is now on a collision course with Israel. The consensus in Israel is that Obama signed a very bad deal, which is dangerous for the Middle East and well beyond it. Israelis, as well as most Middle Easterners, do not buy the promise of a moderate Iran. They know better. Israelis take seriously the calls of the Iranian mobs "Death to America. Death to Israel."

Thus, an Israeli military strike on Iran has become more likely, and in the near future – before the US puts the brakes on military supplies to the Israeli army.

Efraim Inbar, a professor of political studies at Bar-Ilan University, is the director of the Begin-Sadat Center for Strategic Studies and a fellow at the Middle East Forum.

Japan's 17,000 Tons of Nuclear Waste in Search of a Home

Source: <http://www.bloomberg.com/news/articles/2015-07-10/japan-s-17-000-tons-of-nuclear-waste-in-search-of-a-home>

Welcome to Japan, land of cherry blossoms, sushi and sake, and 17,000 metric tons of highly radioactive waste.

That's what the country has in temporary storage from its nuclear plants. Supporters of atomic power say it's cleaner than fossil fuels for generating electricity. Detractors say there's nothing clean about what's left behind, some of which remains a deadly environmental toxin for thousands of years.

Since atomic power was first harnessed more than 70 years ago, the industry has been trying to solve the problem of safe disposal of the waste. Japan has been thrown into the center of the conundrum by its decision in recent months to retire five reactors after the

Fukushima disaster in 2011. It also decided this week to begin the restart process of one reactor despite public opposition.

"It's part of the price of nuclear energy," Allison Macfarlane, a former chief of the U.S. Nuclear Regulatory Commission, said in an interview in Tokyo on atomic waste. "Now, especially with the decommissioning of sites, there will be more pressure to do something with this material. Because you have to."

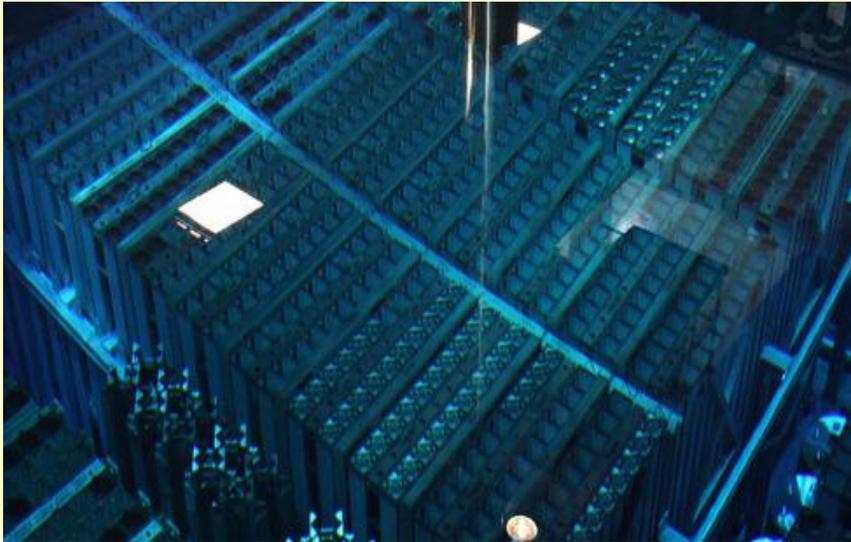
For more than half a century, nuclear plants in more than 30 countries have been humming away -- lighting up Tokyo's Ginza, putting the twinkle into New York's Broadway and keeping the elevators running up the Eiffel Tower. Plus powering



appliances in countless households, factories and offices around the world.

In the process, the world's 437 operating reactors now produce about 12,000 tons of high-level waste a year, or the equivalent of 100 double-decker buses, according to the World Nuclear Association.

Fukushima Disaster



Most countries now agree burying atomic waste deep underground is the best option. Other ideas like firing it into space or tossing it inside a volcano came and went.

The U.S., with the most reactors, spent an estimated \$15 billion on a site for nuclear refuse in Yucca Mountain, Nevada. Local opposition derailed the plan, meaning about 49,000 tons of spent fuel sits in cooling pools at nuclear plants around the country.

Japan faces another challenge. Four years ago, the country had a nuclear accident unlike anything seen before. An earthquake and tsunami ripped through the engineering defenses at the Fukushima plant north of Tokyo and caused the meltdown of three reactors.

It will need billions of dollars and technology not yet invented to clean up Fukushima. How long that will take is disputed. The operator, Tokyo Electric Power Co., estimates 40 years. Greenpeace says it could take twice that time.

'Ethical Responsibility'

All Japan's 43 operational reactors have been offline since September 2013 for safety checks after the disaster. The government has said atomic power is essential to energy supply and

reactors that meet safety standards will be allowed to restart.

The first in line belongs to Kyushu Electric Power Co., which today said it has finished refueling one of its units in southern Japan. It plans to restart the plant in August, which means generation of more nuclear waste.

It will be a "failure in our ethical responsibility to future generations," to restart reactors without a clear plan for waste storage, the Science Council of Japan said in April.

No Thanks

Japan's Nuclear Waste Management Organization, known as NUMO, has been searching for a permanent storage site for years, initially inviting districts to apply as a host.

In 2007, it got one when the mayor of a town called Toyo submitted interest. Like the residents near Yucca Mountain in the U.S., Toyo's citizens didn't like the idea and voted him out of office. His successor canceled the plan.

Now facing the accelerated shutdown of some reactors post-Fukushima, NUMO in May ditched the idea of waiting for a volunteer. Instead, scientists will nominate suitable regions.

"We'd like all citizens to be aware and feel ownership of this situation," said Takao Kinoshita, a NUMO official. "We should feel grateful for the community that's doing something for the benefit of the whole country and respect their bravery."

Deep Underground

NUMO's plan for a final underground repository was drawn up in 2007 and would cost 3.5 trillion yen (\$29 billion).

It would contain about 40,000 canisters, each weighing half a ton and holding waste at temperatures above 200 degrees Celsius (392 Fahrenheit). The contents would give off 1,500 sieverts of radiation an hour, a level that would instantly kill a human being.

The canisters need to cool in interim storage for as long as 50 years before heading 300 meters below ground. Their stainless steel inner layer is wrapped in bentonite clay to make sure water can't leak inside.

"That's the biggest risk we see, water leaking through," said Kinoshita.

Finland and Sweden are the only two countries so far to have selected and



reached a public agreement on a final site and storage technology for high-level nuclear waste. Finland's is expected to open in 2020. Taking apart a reactor, known as decommissioning, produces a few tons of highly radioactive material, usually the used fuel and coolant. The buildings and equipment account for thousands of tons of so-called low-level waste.

Disposal Confusion

Japan's government is responsible for dealing with the most radioactive waste. The plant operator handles the rest. "Even in the low-level category there is the relatively higher-level waste and the nation's technical solutions are not ready," Makoto Yagi, the president of Kansai Electric Power Co., said at a June briefing in Tokyo. Shaun Bernie, senior nuclear specialist with Greenpeace Germany, said this shows Japan's reactor program and high-level nuclear waste policy is "in a state of crisis."

Without a clear disposal strategy, costs to take apart the reactors can end up being double original estimate, said Colin Austin, senior vice president at Energy Solutions, which has worked on every decommissioning project in the U.S.

Another wrinkle in Japan for finding a final disposal site is that the country sits on a mesh of colliding tectonic plates that make it one of the most earthquake-prone countries in the world.

Former NRC chief Macfarlane, who is also a seismologist, said that doesn't make it impossible to bury the waste. A repository hundreds of meters underground is partly protected against quakes in the same way submarines are during high storms, she said.

Leaving nuclear waste on the surface indefinitely means it will get into the environment so Japan has to solve this, she said.

"An adequate place underground is better than waiting for the best possible place."

BiO-dOSimetric Tools for triagE to Responders



Project founded by the European Union under the Seventh Framework Programme (FP7)



Source:<http://www.booster-project.org/>

Since the beginning of the third millennium, security applications have been a challenging issue for all western societies. 9/11 attacks showed the reality and impact of a terrorist act against a western country. The threat of a new terrorist attack forced western societies to adapt and develop new technological solutions. Moreover, nuclear accidents in the past demonstrated the fear of people concerning nuclear risks. A terrorist attack, potentially involving a radiological risk, could have dramatic and long-standing consequences on the world population, from a sanitary and psychological point of view.

On these basis, crisis management (after the explosion of a dirty bomb, or an accident involving radioactive materials, for instance) is a main issue in the framework of security applications, in order to ensure the protection of citizens and prevent any radiological risks. The effective management of an incident involving exposure of large numbers of people to radioactive material requires a mechanism for rapid triage of exposed persons.

The BOOSTER Project addresses the requirement under Security Topic of Bios-dosimetric tools to manage radiological casualties (SEC-2009-4.3.2). The BOOSTER Project is a capability project designed to research and develop new bio-dosimetric tools in order to quickly evaluate the level of exposure of potential casualties, determine by appropriate sensors its consequences and allow an efficient triage of exposed people. These bio-dosimetric tools will be integrated to a useful and usable toolbox along with a prognostic toolkit based on radiation sensors. These approaches will allow an effective management of the situation. At the end of the project, civil protection operators and emergency services will be trained and commercial exploitation potentialities defined.



What is Multibiodose?

Multi-disciplinary biodosimetric tools to manage high scale radiological casualties (MULTIBIODOSE - 7th EU Framework Programme)

Source: http://multibiodose.eu/read_more.html

The MULTIBIODOSE project was launched on May 1st 2010, and it is planned to continue until April 2013. The purpose of this multi-disciplinary collaborative project is to analyse a variety of biodosimetric



tools and adapt them to different mass casualty scenarios. It is envisaged that the project will result in an establishment of a biodosimetric network that is fully functional and ready to respond in case of a mass casualty. In the event of a large scale radiological emergency, biological dosimetry is an essential tool that can provide timely assessment of radiation exposure to the general population and enable the identification of those exposed who should receive medical treatment. A number of biodosimetric

tools are potentially available, but they must be adapted and tested for a large-scale emergency scenario. These methods differ in their specificity and sensitivity to radiation, the stability of signal and speed of performance. A large scale radiological emergency can take different forms. Based on the emergency scenario, different biodosimetric tools should be applied so that the dosimetric information can be made available with optimal speed and precision.



The following biodosimetric tools will be validated and established: the dicentric assay, the micronucleus assay, the gamma-H2AX assay, the skin speckle assay, the blood serum protein expression assay and electron paramagnetic resonance (EPR)/optically stimulated luminescence (OSL) dosimetry in components of pocket electronic devices. These assays were chosen because they complement each other with respect to sensitivity, specificity to radiation and the exposure scenario, as well as speed of performance. Future training programmes will be developed for all the assays validated and established in the project, and automation and commercialisation will be pursued. An operational guidance that will address the multi-parametric approach for large scale human exposures will be developed and disseminated among emergency preparedness and radiation protection organisations.

30



SRI Awarded \$12.2 Million Contract for Radiation Exposure Screening Device

Source: <http://www.hstoday.us/single-article/sri-awarded-122-million-contract-for-radiation-exposure-screening-device/fbdb44375618b91eb037e6db4fec567a.html>

July 13 – With the possibility that terrorists and other criminals might obtain radioactive materials for malicious use, mitigating this threat to global security has become increasingly important. In response, **SRI International has been developing a diagnostic test for absorbed doses of radiation in the event of such an attack.**

SRI International, a nonprofit, independent research center serving government and industry, has been awarded a \$12.2 million contract from the Biomedical Advanced Research and Development Authority (BARDA)

to continue the development of the diagnostic test. BARDA, a division of the Department of Health and Human Services (HSS), is dedicated to developing medical countermeasures to protect civilians from adverse health effects resulting from exposure to chemical, biological, and radiological or radionuclide agents.

The project began more than five years ago when BARDA selected David Cooper, Ph.D., director of the Sensor Systems Laboratory, and his team at SRI to develop a radiation biodosimeter.



In an effort to prepare for an unanticipated radiological or nuclear incident in which large numbers of people may be exposed to radiation that could lead to severe health

assesses whether they have absorbed ionizing radiation or not."

Any living tissue in the human body can be damaged by ionizing radiation. This form of radiation has sufficient energy to strip away electrons from atoms (creating two charged ions) or to break some chemical bonds. The extent of damage depends on the dose of radiation received.

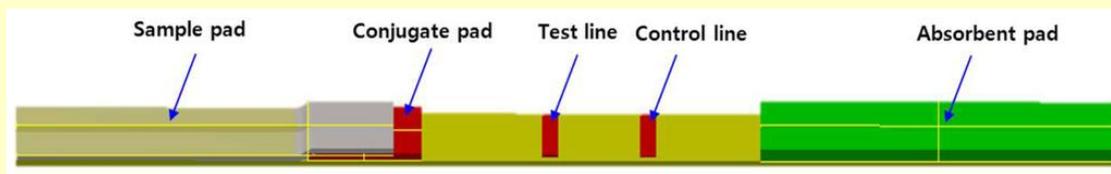
According to the Environmental Protection Agency, some of the early symptoms of radiation sickness are fairly nonspecific and include nausea, weakness, hair loss, skin burns or diminished organ function (especially bone marrow)—and can eventually cause death.

Currently, a wait-and see-approach is used to determine whether a person has absorbed a significant dose of ionizing radiation. Once symptoms develop, this roughly correlates to the exposure level but it is not a definitive diagnosis. The finger-prick blood test will solve the time delay and diagnostic concerns. In less than 30 minutes, the results will show whether a person has absorbed a clinically significant dose

The technology is based on a lateral flow immunoassay method, similar to home pregnancy test kits. Antibodies specific to a panel of radiation-responsive proteins and a proprietary phosphorescent reporter system



consequences, time is of the essence. To rapidly triage large numbers of people to determine who needs immediate treatment,



SRI developed a new and simple screening test.

"If you have hundreds of thousands of people potentially affected, you want to screen quickly and use medical resources efficiently," Cooper said. "Our goal is to develop a quick and simple point-of-care medical device that the government, first responders, hospitals and doctors can use in the field to determine a person's absorbed dose of ionizing radiation." Cooper and the SRI team are researching and developing a device with subcontractors from DCN Diagnostics, Evolve Manufacturing, and Stanford University School of Medicine. Cooper stated. "At this point, there is nothing else like it that takes a sample from an individual and

allow for quantitative measurement of protein concentrations in the patient's blood sample.

"Because our test actually measures biological response to radiation rather than a physical radiation dose, the information obtained is very important," Cooper explained.

Due to differences in individual sensitivities to radiation effects, each subject's response to the same physical dose may be different, therefore the immediate medical decision may be different.

This monetary award will support verification testing of the system, which puts the device one step closer to FDA clearance. SRI also feels infectious disease diagnostic testing can benefit from the



technology employed in the device, making it innovative and dual purpose. Ionized radiation

and infectious disease may just be the beginning of the diagnostic testing possibilities.

Iran's Nuclear Capabilities Fast Facts

Source: <http://www.wptz.com/national/irans-nuclear-capabilities-fast-facts/34222400>

Since 2003, worldwide concern over Iran's nuclear program has increased as Iran and the International Atomic Energy Agency (IAEA) spar over investigation and details of Iran's program. Iran's Supreme Leader Ayatollah Khamenei has repeatedly denied Iran is building a bomb and says weapons of mass destruction are forbidden under Islam.

Timeline

1957 - The United States signs a civil nuclear cooperation agreement with Iran.

1958 - Iran joins the International Atomic Energy Agency.

1967 - The Tehran Nuclear Research Center, which includes a small reactor supplied by the United States, opens.

1968 - Iran signs the Nuclear Non-Proliferation Treaty.

Mid-1970s - With United States' backing, Iran begins developing a nuclear power program.

1979 - Iran's Islamic revolution ends Western involvement in the country's nuclear program.

December 1984 - With the aid of China, Iran opens a nuclear research center in Isfahan.

February 23, 1998 - The United States announces concerns that Iran's nuclear energy program could lead to the development of nuclear weapons.

March 14, 2000 - U.S. President Bill Clinton signs a law that allows sanctions against people and organizations that provide aid to Iran's nuclear program.

February 21, 2003 - IAEA Director General Mohamed ElBaradei visits Iran to survey its nuclear facilities and to encourage Iran to sign a protocol allowing IAEA inspectors greater and faster access to nuclear sites. Iran declines to sign the protocol. ElBaradei says he must accept Iran's statement that its nuclear program is for producing power and not weapons, despite claims of the United States to the contrary.

June 19, 2003 - The IAEA issues a report saying that Iran appeared to be in compliance with the Non-Proliferation Treaty, but that it needed to be more open about its activities.

August 2003 - The IAEA announces that its inspectors in Iran have found traces of highly enriched uranium at the Natanz uranium enrichment plant. Iran claims the amounts are contamination from equipment bought from other countries. Iran agrees to sign a protocol of the Nuclear Non-Proliferation treaty that allows for unannounced visits to their nuclear facilities and signs it on December 18, 2003.

October 2003 - The Foreign Ministers of Britain, France and Germany visit Tehran, and all parties agree upon measures Iran will take to settle all outstanding issues with the IAEA. Under obligation to the IAEA, Iran releases a dossier on its nuclear activities. However, the report does not contain information on where Iran acquired components for centrifuges used to enrich uranium, a fact the IAEA considers important in determining whether the uranium is to be enriched for weapons.

November 2003 - Iran agrees to halt uranium enrichment as a confidence building measure and accepts IAEA verification of suspension.

December 2003 - Iran signs an Additional Protocol with the IAEA voluntarily agreeing to broader inspections of its nuclear facilities.

February 2004 - A.Q. Khan, "father" of Pakistan's nuclear weapons program, admits to having provided Iran and other countries with uranium-enrichment equipment.

June 1, 2004 - The IAEA states they have found traces of uranium that exceed the amount used for general energy production. Iran admits that it is importing parts for advanced centrifuges that can be used to enrich uranium, but is using the parts to generate electricity.

July 31, 2004 - Iran states that it has resumed production on centrifuge parts used for enriching uranium, but not enrichment activities.

August 8, 2005 - Iran restarts uranium conversion, a step on the way to enrichment, at a nuclear facility, saying it is for peaceful purposes only, and flatly rejects a European offer aimed at ensuring the nation does not seek nuclear weapons.



August 9, 2005 - Iran removes the IAEA seals from its Isfahan nuclear processing facility, opening the uranium conversion plant for full operation. IAEA spokesman Mark Gwozdecky states that the plant "is fully monitored by the IAEA" and "is not a uranium enrichment plant."

September 11, 2005 - Iran's new foreign minister, Manouchehr Mottaki, says the country won't suspend activities at its Isfahan uranium conversion facility and it plans to seek bids for the construction of two more nuclear plants.

January 10, 2006 - Iran resumes research at its Natanz uranium enrichment plant, arguing that doing so is within the terms of an agreement with the IAEA.

January 12, 2006 - Foreign ministers of the EU3 (Great Britain, France, Germany) recommend Iran's referral to the United Nations Security Council over its nuclear program.

January 13, 2006 - Iran's Foreign Minister, Manouchehr Mottaki, states that if Iran is referred, its government under law will be forced to stop some of its cooperation with the IAEA, including random inspections.

February 4, 2006 - President Ahmadinejad orders Iran to end its cooperation with the IAEA.

April 11, 2006 - Hashemi Rafsanjani, Iran's former president, states that Iran has increased the number of functioning centrifuges in its nuclear facilities in Natanz and has produced enriched uranium from them.

August 31, 2006 - The IAEA issues a report on Iran saying the Islamic republic "has not suspended its enrichment activities" despite this day's deadline to do so. Iran can possibly face economic sanctions.

December 23, 2006 - The U.N. Security Council votes unanimously to impose sanctions against Iran for failing to suspend its nuclear program.

February 22, 2007 - The IAEA issues a statement saying that Iran has not complied with U.N. Security Council for a freeze of all nuclear activity. Instead, Iran has expanded its uranium enrichment program.

March 24, 2007 - The U.N. adopts Resolution 1747 which toughens sanctions against Iran. The sanctions include the freezing of assets of 28 individuals and organizations involved in Iran's nuclear and missile programs. About a third of those are linked to the Iranian Revolutionary Guard, an elite military corps.

May 23, 2007 - The IAEA delivers its latest report to the United Nations on Iran's nuclear activities. The report states that not only has Iran failed to end its uranium enrichment program but has in fact expanded activity in that area.

June 21, 2007 - Iran's Interior Minister Mostapha PourMohamedi claims, "Now we have 3,000 centrifuges and have in our warehouses 100 kilograms of enriched uranium." ... "We also have more than 150 tons of raw materials for producing uranium gas."

December 2007 - A U.S. intelligence report finds that Iran abandoned a nuclear weapons program in 2003.

February 20, 2009 - The Institute for Science and International Security (ISIS) reports that Iranian scientists have reached "nuclear weapons breakout capability." The report concludes Iran does not yet have a nuclear weapon but does have enough low-enriched uranium for a single nuclear weapon. An official at the IAEA cautions about drawing such conclusions. The IAEA says Iran's stock of low-enriched uranium would have to be turned into highly enriched uranium (HEU) in order to be weapons-grade material.

February 25, 2009 - Iran runs tests at its Bushehr nuclear power plant using "dummy" fuel rods, loaded with lead in place of enriched uranium to simulate nuclear fuel. A news release distributed to reporters at the scene states the test measured the "pressure, temperature and flow rate" of the facility to make sure they were at appropriate levels. Officials say the next test will use enriched uranium, but it's not clear when the test will be held or when the facility will be fully operational.

September 21, 2009 - In a letter to the IAEA, Iran reveals the existence of a second nuclear facility. It is located underground at a military base, near the city of Qom.

October 25, 2009 - IAEA inspectors make their first visit to Iran's newly disclosed nuclear facility near Qom.

February 18, 2010 - In a statement, the IAEA reports that it believes Iran may be working in secret to develop a nuclear warhead for a missile.

August 21, 2010 - Iran begins fueling its first nuclear energy plant, in the city of Bushehr.



December 5, 2010 - Ali Akbar Salehi, Iran's atomic chief and acting foreign minister, announces that Iran's nuclear program is self-sufficient and that Iran has begun producing yellowcake, an intermediate stage in processing uranium.

January 8, 2011 - Ali Akbar Salehi reports that Iran can now create its own nuclear fuel plates and rods.

September 4, 2011 - Iran announces that its Bushehr nuclear power plant joined the electric grid September 3, making it the first Middle Eastern country to produce commercial electricity from atomic reactors.

September 5, 2011 - In response to Iran's nuclear chief stating that Iran will give the IAEA "full supervision" of its nuclear program for five years if U.N. sanctions are lifted, the European Union says that Iran must first comply with international obligations.

November 8, 2011 - The IAEA releases a report saying that it has "serious concerns" and "credible" information that Iran may be developing nuclear weapons.

January 9, 2012 - The IAEA confirms that uranium enrichment has begun at the Fordo nuclear facility in the Qom province in northern Iran.

January 23, 2012 - The European Union announces it will ban the import of Iranian crude oil and petroleum products.

January 29, 2012 - A six-member delegation from the IAEA arrives in Tehran for a three-day visit, shortly after the European Union imposes new sanctions aimed at cutting off funding to the nuclear program.

January 31, 2012 - In Senate testimony James Clapper, Director of National Intelligence, says there's no evidence Iran is building a nuclear bomb. CIA director David Petraeus agrees.

February 15, 2012 - Iran loads the first domestically-produced nuclear fuel rods into the Tehran research reactor.

February 21, 2012 - After two days of talks in Iran about the country's nuclear program, the IAEA expresses disappointment that no progress was made and that their request to visit the Parchin military base was denied.

March 28, 2012 - Discussions regarding Iran's nuclear future stall.

April 14, 2012 - Talks resume between Iran and six world powers over Iranian nuclear ambitions in Istanbul, Turkey.

May 25, 2012 - An IAEA report finds that environmental samples taken at the Fordo fuel enrichment plant near the city of Qom have enrichment levels of up to 27%, higher than the previous level of 20%.

June 18-19, 2012 - A meeting is held between Iran and the P5+1 (United States, France, Russia, China, Great Britain and Germany) in Moscow. No agreement is reached.

June 28, 2012 - Saeed Jalili writes to European Union foreign policy chief Catherine Ashton warning world powers to avoid "unconstructive measures" such as the oil embargo agreed upon by the EU in January draws near.

July 1, 2012 - A full embargo of Iranian oil from the European Union takes effect.

August 30, 2012 - A United Nations report finds that Iran has stepped up its production of high-grade enriched uranium and has re-landscaped Parchin, one of its military bases, in an apparent effort to hamper a U.N. inquiry into the country's nuclear program.

September 24, 2013 - At a speech at the U.N. General Assembly Iranian President Rouhani says "Nuclear weapons and other weapons of mass destruction have no place in Iran's security and defense doctrine, and contradict our fundamental religious and ethical convictions."

October 16, 2013 - The latest discussions between Iran and the six world powers center on a proposal put forth by Iran to recognize the peaceful nature of its nuclear energy pursuits. The meeting is described as "substantive and forward-looking."

November 24, 2013 - Six world powers and Iran reach an agreement over Iran's nuclear program. The deal calls on Iran to limit its nuclear activities in return for lighter sanctions.

January 12, 2014 - It is announced that Iran will begin eliminating some of its uranium stockpile on January 20.

January 20, 2014 - Iran's nuclear spokesman Behrouz Kamalvandi tells state-run news agency IRNA that Iran has started suspending high levels of uranium enrichment.

January 20, 2014 - The European Union announces that it has suspended certain sanctions against Iran for six months.



February 20, 2014 - Following talks in Vienna, EU foreign policy chief Catherine Ashton and Iranian Foreign Minister Mohammad Javad Zarif announce that a deal on the framework for comprehensive negotiations over Tehran's nuclear program has been reached.

November 24, 2014 - The deadline for a final nuclear agreement between Iran and the U.N. Security Council's P5+1 countries (the United States, Russia, China, France, Britain and Germany) has been set for July 1, 2015.

April 2, 2015 - Negotiators from Iran, the United States, China, Germany, France, Britain and Russia reach a framework for an agreement on Iran's nuclear capabilities, which includes reducing its stockpile of low-enriched uranium by 98%. The deadline for the complete agreement is July 1.

April 9, 2015 - Iranian President Hassan Rouhani announces that Iran will only sign a final nuclear agreement if economic sanctions are lifted on the first day of implementation.

July 14, 2015 - A deal is reached on Iran's nuclear program. The deal reduces the number of Iranian centrifuges by two-thirds. It places bans on enrichment at key facilities, and limits uranium research and development to the Natanz facility.

Sunni Arabs: Iran Deal Opens the 'Gates of Evil'

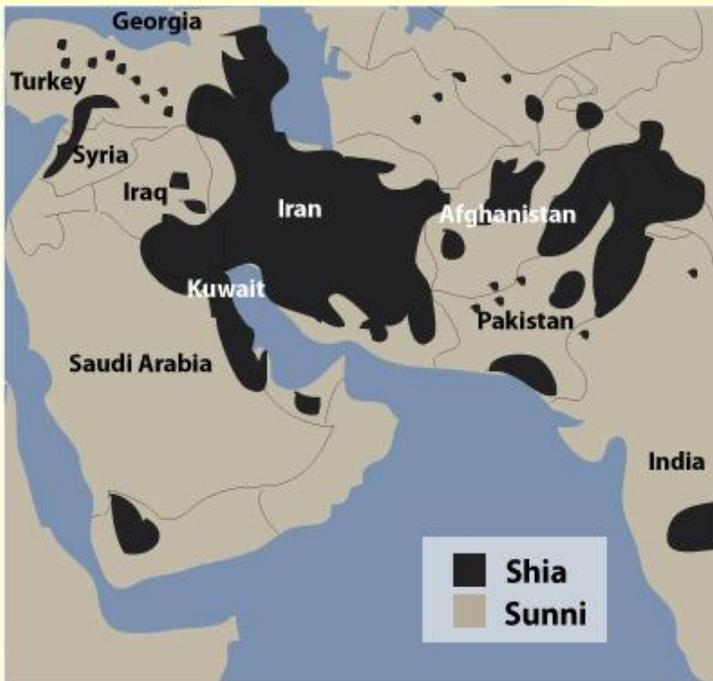
By Jonathan Spyer

Source: <http://www.meforum.org/5390/iran-gates-of-evil>

The response in the Arabic-speaking world to the conclusion of a deal between the P5+1 countries and the Islamic Republic of Iran over the latter's nuclear program has divided along familiar lines.

Among pro-Iranian elements, such as President Bashar Assad of Syria and

on the nuclear elements of the deal – that is, whether it will effectively halt Iran's march toward the bomb. Instead, attention has centered on the deal's implications for Iran's push for hegemony in the Middle East, and its interference in and subversion of regional states as part of this effort.



Hezbollah leader Hassan Nasrallah, the news of the deal has, predictably, been met with jubilation. Assad described the agreement as a "historic achievement" and a "great victory."

Among Sunni elements opposed to the advance of Iran, concerns have focused less

fighting terrorism with terrorism amid deafening silence from the West.

Saudi Arabia and the Gulf states can only welcome the nuclear deal, which in itself is supposed to close the gates of evil that Iran had opened in the region.



However, the real concern is that the deal will open other gates of evil, gates which Iran mastered knocking at for years even while Western sanctions were still in place.

From this perspective a particularly notable and dismaying aspect of the deal is its removal of the Iranian Revolutionary Guards Corps and its Quds Force commander, Maj.-Gen. Qasem Soleimani, from the list of those subject to sanctions by the West.

The ending of sanctions on the IRGC, and more broadly the likely imminent freeing of up to \$150 billion in frozen revenue, will enable Iran to massively increase its aid to its long list of regional clients and proxies. Iran today is heavily engaged in at least five conflict arenas in the region.

The Iranian creation and proxy Hezbollah in Lebanon is the dominant political and military force in that country. The organization depends on Iranian support, training and funding to maintain this position.

In Syria, beleaguered dictator and Iranian client Assad remains in control in the west and south largely because of Iranian support and assistance – up to \$1 billion per month, according to some estimates. For as long as Assad remains, the war remains, allowing such monstrous entities as Islamic State and al-Qaida to flourish.

Iran's Revolutionary Guards are unmatched in clandestine and proxy warfare, having effectively created an alternative armed force for Assad when his own army became unreliable in 2012. This force, the National Defense Forces, has plugged the gap in manpower which is the regime's greatest vulnerability. But in addition, Iran has channeled others of its proxies, including Hezbollah, Iraqi Shi'ite militias, and lately increasing numbers of Afghan Hazara Shi'ite "volunteers," toward the Syrian battlefield.

In Iraq, the Iranian-supported Shi'ite militias of the Hashd al-Shaabi are playing the key role in defending Baghdad from the advance of Islamic State. These militias are trained and financed by the Revolutionary Guards and organized by Soleimani and his Iraqi right-hand man, Abu Mahdi al-Muhandis, also thought to be an IRGC member.

In Yemen, the Iranians are offering arms and support to the Ansar Allah, or Houthi rebels, who are engaged in a bloody insurgency against the government of President Abd Rabbo Mansour Hadi.

Among the Palestinians, Tehran operates Palestinian Islamic Jihad as a client/proxy organization, and is in the process of rebuilding relations with the Izzadin Kassam, the powerful military wing of Hamas.

All this costs money. In a pattern familiar to the experience of totalitarian regimes under sanctions in the past, Iran has preferred to safeguard monies for use in service of its regional ambitions, while allowing its population – other than those connected to the regime – to suffer the consequent shortages.

Still, in recent months, things weren't going so well. Assad has been losing ground to the Sunni rebels. Hezbollah has been hemorrhaging men in Syria. The Shi'ite militias were holding Islamic State in Iraq but not advancing. Saudi intervention was holding back further advances by the Houthis in Yemen. Hamas was looking poverty-stricken and beleaguered in its Gaza redoubt.

The sanctions, plus these many commitments, were bringing the Iranian regime close to an economic crisis that would have confronted the regime with the hard choice of lessening its regional interference or facing the consequences.

No longer. The deal over the nuclear program is set to enable Tehran to shore up its investments, providing more money and guns to all its friends across the Middle East, who will as a result grow stronger, bolder and more ambitious. This, from the point of view of the main powers in the Sunni Arab world, is the key fallout (so to speak) from the deal concluded in Vienna. IRGC "outreach" to Shi'ite minorities in Saudi Arabia and Kuwait, and to the Shi'ite majority in Bahrain, is also likely to increase as a result of the windfall.

It has been felt in recent years in Riyadh, Cairo, Amman and other Sunni Arab capitals that the United States is determined to withdraw from active involvement in the region, and in pursuit of this goal is currently pursuing a dangerous path of appeasement of Iran.

This impression is compounded not only by the stance toward the Iranian nuclear program but also by the US response to Iran's activities across the Middle East. In Iraq, the US appears to be acting in tandem with Iranian goals, with no apparent awareness of the problems in this regard. Similarly, in Lebanon the West is supporting and equipping the Lebanese Armed Forces, without understanding that the Lebanese state



is largely a shell, within which Hezbollah is the living and directing force. In Syria, the US is pursuing a half-hearted campaign against Islamic State, while leaving the rest of the country to its internal dynamics.

The nuclear deal compounds and completes the picture. From the perspective of the Saudis and other Sunni Arabs, Iranian ruthlessness, clarity and advance combined with the flailing,

retreating US regional policy now so much in evidence spell potential disaster.

The Sunni Arabs, along with Israel and other regional opponents of Iran, will now develop strategies independent of the US to stem this advance and turn it back. The outcome of that struggle will determine the fate of the Middle East.

Jonathan Spyer, a fellow at the Middle East Forum, is director of the Rubin Center for Research in International Affairs and the author of The Transforming Fire: The Rise of the Israel-Islamist Conflict (Continuum, 2011).

CIA: Iran will focus on its economy, not terrorism, with sanctions money

Source: http://www.sentinelsource.com/news/national_world/cia-iran-will-focus-on-its-economy-not-terrorism-with/article_e45b7fe9-2a67-593b-b7cd-c7c2bb0df992.html

July 17 – A secret U.S. intelligence assessment predicts that Iran's government will pump most of an expected \$100 billion windfall from the lifting of international sanctions into the country's flagging economy and won't significantly boost funding for terrorist groups and sectarian militias it supports in the Middle East.

Intelligence officials have concluded that even if Tehran increases support for Hezbollah commanders in Lebanon, Houthi rebels in Yemen or President Bashar Assad's embattled government in Syria, the extra cash is unlikely to tip the balance of power in the world's most volatile region, according to two U.S. officials who spoke on condition of anonymity to discuss the intelligence document.

The controversial CIA report, which has been briefed to key members of Congress, thus provides ammunition to both sides in the battle brewing on Capitol Hill over President Barack Obama's signature foreign policy achievement, a sweeping deal to block Iran's ability to build nuclear weapons for at least a decade in exchange for the easing of sanctions that have hobbled the country's economy.

Under the deal sealed Tuesday in Vienna, once Iran completes a series of strict requirements, the U.S., the European Union and the United Nations will suspend the most damaging sanctions against Iran's financial and energy sectors, and Tehran will be given access to about \$100 billion from oil revenues frozen in overseas accounts. That could occur in early 2016.

The United States also will rescind most of its banking sanctions, allowing Iranian banks to reconnect to the global financial system, and will lift restrictions on Iran's automotive, shipping and insurance industries, as well as on trade in gold and precious metals. In all, 444 companies or individuals, 76 aircraft and 227 ships would be removed from U.S. blacklists.

Non-nuclear sanctions, including those related to human rights abuses and Iran's support for terrorism, will remain in place. A U.N. arms embargo would lift in five years, and restrictions on the transfer of ballistic missile technology remain for eight years, although administration officials said the U.S. and its Persian Gulf allies will step up efforts to interdict any Iranian military shipments to its proxies.

Republican lawmakers briefed on the CIA report have seized on the conclusion that Iran could increase support for terrorist groups and expand its military role in Yemen, Syria and other regional hot spots, describing it as a fatal flaw in the Vienna agreement.

"I don't know what information the Obama administration possesses that indicates this deal will actually prevent Iran from getting a nuclear weapon or will cause the mullahs to reduce their support for worldwide terrorism, but it sure isn't the same intelligence we're seeing in the Intelligence Committee," Rep. Devin Nunes, R-Calif., chairman of the House Intelligence Committee, said in a statement.



The Obama administration is banking, in part, on Iranian President Hassan Rouhani and other so-called moderates in Iran's leadership to steer most of the anticipated money into domestic infrastructure and other investments to quell increasing public frustration over a lack of jobs and business opportunities.

Rouhani was elected in 2013 on a campaign promise to improve Iran's economy, and U.S. intelligence analysts say his advisors determined early on that Iran's high inflation and moribund finances could not recover while biting sanctions were in place. The analysts believe that the impact of the sanctions kept the Iranians coming back to the negotiating table over the last 20 months.

For his part, Obama acknowledged Wednesday that some of the money could be siphoned off to fund Iranian proxies in the Middle East.

"Do we think that with the sanctions coming down, that Iran will have some additional resources for its military and for some of the activities in the region that are a threat to us and a threat to our allies? I think that is a likelihood that they've got some additional resources. Do I think it's a game-changer for them? No," Obama said a White House news conference the day after the deal was reached.

"The notion that they're just immediately going to turn over \$100 billion to the IRGC or the Quds Force I think runs contrary to all the intelligence that we've seen and the commitments that the Iranian government has made," Obama added, referring to the Iranian Revolutionary Guard Corps and its special forces units abroad.

Obama said it is a "mistake" to say his administration believes that Iran will only spend the money on "day care centers, and roads, and paying down debt." But he said preventing Iran from building a nuclear weapon is more important than releasing "incremental additional money" that Iran could use "to try to destabilize the region or send to their proxies."

Under the sanctions regime, Iran currently has about \$100 billion frozen in oil escrow accounts in banks in several countries that buy Iranian petroleum products, including China, India, Japan, South Korea, Turkey and Taiwan.

Iran would be able to withdraw funds from those accounts once it has complied with the initial terms of the nuclear deal, including taking out two-thirds of its centrifuges, reducing its enriched uranium stockpile by 98 percent, shutting down its plutonium facility and allowing International Atomic Energy Agency inspectors broad access for monitoring of operations.

EDITOR'S COMMENT: Let us see if (at least) this time CIA will be right in its forecasting!

The question of nuclear waste in the UAE

By Robert Matthews

Source: <http://www.thenational.ae/uae/technology/the-question-of-nuclear-waste-in-the-uae#full>

July 18 – It has gone so fast – and so far, so good. It's already the third anniversary of work starting on the UAE's first nuclear power plant at Barakah, near the border with Saudi Arabia. And it is still on budget and set to go live in late 2017, ultimately providing a quarter of the Emirates' energy needs.

But becoming the first new member to the global nuclear power club since the mid-1980s was never going to be straightforward, and the next 18 months will be the toughest so far.

Yet one huge challenge will remain even if the Barakah project is a triumphant success. It is the same one that has faced every member of the club since its first members signed up in the 1950s: what to do with radioactive waste.

Whatever one's view of the operational safety record of nuclear power, there is no doubting the scale of the waste problem.

Over the decades, **the world's 400-plus power reactors have generated about 270,000 tonnes of spent fuel. Laced with U-235 and other isotopes, it takes years to cool to the point where it can be processed, and another 1,000 years for most of its radioactivity to decay.**

Each year another 12,000 tonnes of the stuff is generated, and soon the UAE will join those nations faced with trying to deal with it.

The good news is that the UAE is joining the club at a time when some believe an acceptable solution may be starting to



emerge. What's unclear is whether the UAE will be in a position to exploit it. Over the decades ideas for dealing with nuclear waste have ranged from cavalier to

Now one may finally have emerged. It's not especially clever, and it's been around for years. But it requires a key ingredient so far found in few parts of the world: public trust.



Last month, a conference organised by the International Atomic Energy Agency in Vienna learnt of the latest progress with the technique, developed by Swedish engineers and known as KBS-3. It involves taking the HLW out of the pools once it's cooled off, encasing it in metal canisters and putting them in clay-filled tunnels about 500m underground.

To be fair, that somewhat underplays some of the technique's key features. For a start, the canisters are 25-tonne monsters made from 5cm-thick copper with cast-iron inserts.

literally out of this world.

During the 1940s, the United States and Britain began a programme of simply dumping radioactive waste into the ocean – including whole nuclear reactor vessels complete with fuel. Other countries joined the programme, which was only outlawed internationally in 1994.

During the 1970s, the US space agency Nasa looked at the possibility of using rockets to fire the nastiest and most concentrated high-level waste (HLW) into deep space.

This isn't just a theoretical possibility: many deep-space probes with small plutonium power plants have been successfully launched into space - among them the New Horizons mission that shot past Pluto last week.

Unsurprisingly, the idea crashed and burned in the face of concern about the rockets packed with HLW doing just that.

Since then, many more down-to-earth ideas have been explored, ranging from reprocessing and concentrating HLW to building special nuclear "incinerators". All have proved economically or technically problematic, and usually both.

As a result, most of the world's HLW remains sitting in huge water-filled pools or concrete casks, waiting for someone to come up with a better idea.

The clay is pretty special too: bentonite, which swells and self-seals when exposed to water but also cushions the canisters against any movement.

Not that there's likely to be much of that, as the tunnels themselves are carved out of solid granite bedrock.

Even so, KBS-3 still sounds like just another "out of sight, out of mind" approach of the sort that generates controversy, protests and delays.

Just ask the US government, which spent half a century trying to set up something similar for its own HLW.

In the 1970s it thought it had identified the perfect site: Yucca Mountain, in the Nevada desert, 150km from Las Vegas. But the plan quickly ran into huge public and political pressure, and ended up being abandoned in 2009.

What makes KBS-3 different is not the technology but where it is being used: Finland.

For over a decade, deep below the Olkiluoto nuclear power plant on the west coast of Finland, a vast access tunnel has been carved out of the granite. These will allow KBS-3 canisters to be taken down into storage once the site becomes operational in 2020.

And there seems little doubt that it will.



In February, Finland’s nuclear regulator backed the project with a safety assessment, and the Finns seem perfectly happy with that. As one of the national nuclear inspectors told Reuters last month: “The population has a high trust in regulators and policymakers.”

Other nations hoping to exploit the Finnish sangfroid and start shipping over their own HLW will be disappointed, however: the nation has banned importation of the stuff.

But that isn’t stopping others from trying to implement the central lesson of the Finnish experience: building trust is both possible and vital.

Sweden is now planning a similar project, and others countries across Europe are eyeing progress with keen interest.

On the face of it, the UAE has the luxury of being able to watch and wait for some time yet. Once operational, the four Barakah reactors will produce about 100 tonnes of spent fuel annually, and it will be years before a decision on its long-term fate is needed.

In reality, however, work on the waste problem has to begin immediately – by redoubling efforts to maintain trust in the UAE’s nascent nuclear programme.

Robert Matthews is Visiting Reader in Science at Aston University, Birmingham

Is your fear of radiation irrational?

By Geoff Watts

Source: <http://www.homelandsecuritynewswire.com/dr20150721-is-your-fear-of-radiation-irrational>

July 21 – Radioactivity stirs primal fears in many people, but that an undue sense of its risks can cause real harm. Invisible threats are always the most unnerving, and radiation is not something you can see. Nor can you control it. The traditional secrecy of the biggest commercial user of radiation, the nuclear power industry, hasn’t helped. A justified fear of high and uncontrolled levels of radiation has thus undermined our willingness to see that the risks it poses at low levels are either acceptable or manageable.

Bad Gastein in the Austrian Alps. It’s 10 a.m. on a Wednesday in early March, cold and snowy — but not in the entrance to the main gallery of what was once a gold mine. Toggled out in swimming trunks, flip-flops and a bath robe, I have just squeezed into one of the carriages of a narrow-gauge railway that’s about to carry me 2 km into the heart of the Radhausberg mountain.

Fifteen minutes later we’re there and I’m ready to enjoy what the brochures insist will be a health-enhancing environment. Enjoyment, of course, is a subjective term. The temperature inside the mountain’s dimly lit tunnels is around 40°C, and the humidity is 100 per cent. The

sweat’s already begun to flow. More important, I’m breathing an atmosphere rich in radon.

Hang on... radon? That’s a radioactive gas. Yet here I am, without so much as a film badge dosimeter, never mind the protection of a lead apron, among a group of people who have paid to come to the Gasteiner Heilstollen (“healing galleries”) and willingly, even eagerly, undergo grueling sessions in physical

discomfort because of a much-contested theory that small doses of radiation are not just harmless, but act as a stimulant to good health.

Our view of radiation and its risks and benefits is complicated and mostly — the delights of the Heilstollen notwithstanding — negative. We are all aware of the effects of a nuclear weapon, the Armageddon scenario of a nuclear winter, cancers and birth defects caused by high doses of radiation and the like. Images of mushroom clouds have struck fear into our hearts since the 1940s, but it is what we can’t see in those pictures that scares us the most.

Invisible threats are always the most unnerving, and radiation is not something you can see. Nor can you



control it. Many years ago, a veteran researcher told me how much he wished he could paint radiation blue. If we could see it, he said, we'd be better placed to deal with it and less nervous about it. The traditional secrecy of the biggest commercial user of radiation, the nuclear power industry, hasn't helped. Only belatedly did it realize that doing things out of sight, behind closed doors, is the best way to fuel public suspicion. So it is perhaps understandable why many people say that (medical X-rays and CT scans aside) the only safe radiation is no radiation.

Nevertheless, I disagree. I believe that a justified fear of high and uncontrolled levels of radiation has undermined our willingness to see that the risks it poses at low levels are either acceptable or manageable. Imagine if we treated fire in the same way as all things nuclear: we would have responded to house fires by banning matches.

And I am worried that, as a result of these exaggerated fears, we are failing to make the most of radiation for our greater good.

To appreciate the measure of our hot-button fixation with radioactivity, recall the events of 2011 in Japan. The magnitude 9 earthquake and subsequent tsunami that hit the country on 11 March was by any measure a disaster. 20,000 people died and more than 500 square kilometers of land were flooded. Families lost their homes, their businesses and their livelihoods.

It didn't take long for the media to discover that one of the casualties, in pole position when the tsunami struck, was the Fukushima nuclear power station. From that moment the story ceased to be about a natural event and became, in effect, about a man-made one. It became that chilling scenario: a nuclear disaster.

Of the 20,000 deaths, some were directly due to the earthquake itself, while others were caused by drowning. How many deaths were the result of radiation from the damaged plant? None. In its section on the health consequences of the Fukushima tragedy, the report by the UN's Scientific Committee on the Effects of Atomic Radiation says: "No radiation-related deaths or acute diseases have been observed among the workers and general public exposed to radiation from the accident."

The dose to the public, the report goes on to say, was generally low or very low. "No discernible increased incidence of radiation-

related health effects are expected among exposed members of the public or their descendants."

This is not to play down the impact of the event. Three of the nuclear plant's reactors suffered damage to their cores, and a large amount of radioactive material was released into the environment. Twelve workers are thought to have received doses of iodine-131 that will increase their risk of developing cancer of the thyroid gland. A further 160 workers experienced doses sufficient to increase their risk of other cancers. "However," says the report, "any increased incidence of cancer in this group is expected to be indiscernible because of the difficulty of confirming such a small incidence against the normal statistical fluctuations in cancer incidence."

In short, while a terrifying natural event had killed many thousands of people, the focus of attention in Japan and round the world was on one component of the tragedy that killed no one at the time. Radiation exposure may have shortened the lives of some of those directly involved, but its effects are likely to be so small that we may never know for sure whether they are related to the accident or not.

When it comes to disaster, nuclear trumps natural. Our sense of the relative importance of things is absurdly skewed.

Chernobyl, of course, was much worse. A poorly designed reactor operating under weak safety arrangements in a bureaucratic and secretive society was a recipe for disaster. On 26 April 1986 all the ingredients came together – ironically during an experimental and bungled safety check. One of the reactors overheated, caught fire, exploded and released a large quantity of radioactive material into the atmosphere. 116,000 people were evacuated; another 270,000 found themselves living in a zone described as "highly contaminated."

It sounds bad. For 134 of the workers involved in the initial cleanup, it was very bad. The dose they received was enough to cause acute radiation sickness, and 28 of them soon died. Then, distrust of official information together with rumors of the dire consequences to be expected created a disproportionate fear. One rumor circulating during the period immediately following the accident claimed that 15,000 nuclear victims had been buried in a mass grave. Nor did such rumors die away; another in 2000 held that 300,000



people had by that time died of radiation. The reality, though hardly inconsequential, was less catastrophic. A World Health Organization expert group was set up to examine the aftermath of the disaster and to calculate its future health consequences. On the basis of average radiation exposure for the evacuees, the people who weren't evacuated and the many more thousands of workers later involved in the cleanup, the report concluded that cancer deaths in these three groups will increase by no more than 4 per cent. The report's conclusions have been, and still are, contested — but the weight of orthodox opinion continues to line up behind the expert group's calculations.

"There was certainly a rise in thyroid cancer," says James Smith, Professor of Environmental Science at Portsmouth University and a coordinator of three multinational European Community projects on the environmental consequences of the accident. But he goes on to add a qualification: "The Soviets didn't put in enough measures to stop people eating contaminated food and drinking contaminated milk, and this particularly affected children." The deaths, in other words, were not all inevitable.

included each stage of energy generation from the extraction of any raw materials required to the health consequences of generating and using it.

Coal came out on top while nuclear emerged as the least damaging to health. When you think of coal-fired energy generation, from the hazards of mining to atmospheric pollution, this rank order is hardly surprising. But while the choking murk over many big Asian cities on a still day is clear to see, deaths related to the coal industry don't mobilize either fear or indignation on the same scale as a nuclear incident does. Perhaps it is radiation's invisibility that fuels overheated reporting of relatively minor events — and then the reporting, by its extent as much as by sensationalism, confirms and heightens our fear.

A number of governments responded to the events in Japan in 2011. Most notable was Germany. Although unenthusiastic about nuclear power, it had recently accepted a need to prolong the period for which its existing nuclear plants would operate. Following the events at Fukushima, it changed its mind. Critics of the policy change were left trying to recall the last time Germany had experienced a



really severe earthquake, never mind a tsunami.

Ironically, despite being a nation encompassing some of Europe's most strident opponents of nuclear power, Germans make up a significant proportion of visitors to the radon-rich clinic at Bad Gastein. The particular **Gasteiner Heilstollen tunnel** in which I spent my 30 radon-breathing minutes had room for 20 or so people who had signed on for its protective value or its alleged benefit in alleviating conditions such as rheumatoid arthritis, asthma and sinusitis or skin conditions like psoriasis.

Any death from any cause in any industry is regrettable and, ideally, to be prevented. But is nuclear power inherently more dangerous than other forms of energy? A 2002 review issued by the International Energy Agency compared fatalities per unit of power produced from several energy sources, including coal, biomass, wind and nuclear. The figures

of clinical trials, of surveys testifying to the popularity of the treatment, and of patients who are able to cut down on or even abandon the drug therapies they would otherwise have been using. How much of this evidence would rate as gold standard in quality, I have no idea — but I was struck by the enthusiasm with which some people



seek out the same force of nature that most others think we have to avoid at any cost. One of my fellow transient troglodytes was on her 70th visit.

The managing director of the Gasteiner Heilstollen is Christoph Köstinger, a physicist by education. Some 9,000 patients, he told me, do a full spa therapy of one session per day for 2–4 weeks, and several thousand more have shorter courses. He is well aware of people's conflicting feelings about radiation: "I divide people into three groups," he says. "Those who are really frightened of radiation don't come to us. Then there are people who are not frightened of radiation and say it's all OK. And a lot of people are a little bit frightened, but you can usually explain the balance of risk."

He's also aware of the widespread aversion to nuclear power throughout Germany. "Some patients explain it to themselves by saying that this [radon] is natural radiation," he explains, hastening to add that as a physicist he's aware of the meaninglessness of any distinction between 'natural' and 'unnatural' radiation.

Lying on my bed of discomfort in the Gasteiner galleries, breathing in the radon, just how much radioactivity was I taking on board? Very little. I was inside the mine for slightly over an hour. Köstinger reckons that during a three-week treatment program, patients receive a dose of around 1.8 mSv (millisieverts), or roughly three-quarters of a full year's background radiation – because, of course, we are all exposed to low-level radiation all the time.

First, there is cosmic radiation from the Sun and the rest of the stars in our galaxy and beyond. How much we get depends on the altitude at which we live and on fluctuations in the Earth's magnetic field. And then there's radiation from the Earth itself, including radon. Here, too, geography is a factor: in some places radon can be found leaking into the atmosphere in significantly larger amounts. Naturally radioactive solids such as uranium and thorium in rock and soil also make their contribution. The global average annual radiation dose is 2.4 mSv. To put this in perspective, that's about the same as 120 chest X-rays.

Much of what we know about radiation's effects on human beings comes from far higher doses following nuclear explosions – the bombs dropped in 1945 on Hiroshima and Nagasaki. The Radiation Effects Research Foundation has studied the health of some 100,000

survivors of the two bombings, and the health of their children.

The findings from the survivors themselves came as no great surprise. For cancers other than leukaemia, an excess risk started to appear about ten years after the event. The extent of the risk depended on each individual's distance from the site of the explosion, as well as on age and gender. As an example, anyone about 2.5 km away had a 10 percent greater risk of developing a tumor. In the case of leukemia, the excess number of deaths began to appear just two years after exposure and peaked four to six years later.

What hadn't been expected were the findings from the Hiroshima and Nagasaki survivors' children. The assumption had been that they too would be more likely to develop malignancies of some kind – but so far this has not been the case.

"At this point we have not seen any excess of cancer or non-cancer mortality," says Roy Shore, chief of research at the Radiation Effects Research Foundation. He goes on to point out that a large part of their disease experience will occur over the next 30 years, so he can't entirely rule out a late effect. Nonetheless, the findings so far are a bit of a surprise. "Based on experimental data ranging from fruit flies to mice we would have expected to see some," he adds.

Of the unresolved debates about radiation, the most contentious is the true extent of the harm (or even the benefit, if the Gasteiner Heilstollen evidence persuades you) that it causes at low levels.

There are two schools of thought. The generally accepted view derives from the known relationship between higher levels of radiation exposure and the subsequent likelihood of developing cancer. Plot one against the other, and what emerges is a more-or-less straight line. The uncertainty is over this being extrapolated to very low doses, and whether there is a threshold below which the risk vanishes.

"At really low doses — down in the range of, say, a CT examination — we don't have strong evidence one way or another," says Shore. "It's a matter of interpretation." He himself sees it as prudent to assume there isn't a threshold: the so-called 'linear no-threshold' (LNT) hypothesis.

Professor Gerry Thomas has a chair in molecular pathology at Imperial



College London and takes a close interest in the effects of radiation. As she points out, illnesses caused by radiation are also caused by other things, so at the lower end of the dose range you need a very large group of people to prove it either way. “Most scientific opinion is that there’s no data to say it’s dangerous until you reach about 100 mSv.”

Even so, most radiation regulatory authorities and their advisers back the LNT view. Safety limits are set accordingly low. The upper limit for exposure for a member of the UK public, for example, is 1 mSv per year – less than half the annual average background dose.

Speaking for the Bad Gastein clinic, Köstinger takes a pragmatic view. He balances the risk of low-dose radiation against what he describes as the “scientifically proven effect” of the treatment. “We have a hypothetical risk [from radiation],” he says, “but even in the worst case it is minimal compared to the risks of the drugs our patients are usually able to stop using. If there’s a risk, we can live with it. If scientific knowledge suggests there’s a threshold, that’s also OK.”

The overall conclusion of all this is that radiation is nothing like as damaging as is commonly assumed. Moreover, what often gets lost in the argument is that the difference between a very small risk and a slightly greater very small risk may be of no practical consequence. In fact, policies and decisions that become obsessed with radiation risk minimization may, in the wider scheme of things, turn out to be counterproductive.

Does it matter if large numbers of people have an unwarranted dread of radiation? After all, millions of us have irrational fears about all sorts of things from spiders to flying. We cope. The world still turns.

Two instances serve to illustrate why being unduly fearful of radiation does matter. Both, in their way, are troublesome for individuals and for the community.

The first is our reluctance to exploit nuclear power. From 1970 onward, global electricity production from nuclear power stations experienced a steady rise. In the 1990s, this rise continued, but at a slower pace. From 2000, it flattened out, and then began to slip. Even as enthusiasm for carbon-free energy generation began to increase, the use of carbon-free nuclear power first faltered, then began to decline.

There are many reasons for this, not least the arguments about the cost of building nuclear power stations and of decommissioning them. But public suspicion has possibly — probably — had the key role in policy decisions. We’ve watched as nuclear power stations have begun to reach the end of their working lives. In panic at the prospect of the lights going off, we’ve extended those lives. But some countries have shied away from replacing them, judging that the perceived risk is greater than the potential role of nuclear power to significantly limit man-made climate change. From the evidence, it seems clear to me that the balance lies overwhelmingly in the other direction.

The personal consequences of an excessive fear of radiation are, in their way, even more damaging. Evidence for this can be found in the aftermath of the events at Chernobyl and Fukushima. The WHO Expert Group set up to examine the Chernobyl disaster reported that it had a serious impact on the mental health and wellbeing of the local population who were evacuated.

“There are sad stories from Chernobyl and more recently at Fukushima of people being shunned by the communities they went to because they were thought to be radioactive or in some way contaminated,” says Smith. “One conclusion of the WHO report was that the social and psychological impacts of Chernobyl had been worse than the direct radiation impacts.”

He recalls meeting a man fishing in a contaminated lake within the Chernobyl exclusion zone. “This guy said he wasn’t moving: ‘The Second World War didn’t move me out of my home, so I’m not going to go on account of a bit of radiation.’

“You can’t say for sure, because it’s all about statistics, but he probably made the right decision. He certainly faced an additional risk because he was eating local food, which was contaminated, but the risk he would have taken on if he’d been forced to move to somewhere else and live a different lifestyle would probably have meant he lived less long anyway.”

Although the Fukushima evacuees were less plagued by outlandish rumors than their counterparts at Chernobyl, they too suffered the nagging consequences of an undue fear of radiation and its unpredictable effects on health. A 2012 survey of the evacuees revealed that one in five of them showed signs of mental trauma.



Stress and consequent mental health problems are unavoidable when evacuation and relocation is indisputably necessary. But a zealous application of the precautionary principle, worst-case assumptions about the effects of radiation and wide safety margins have fostered counterproductive risk assessments. Together with unfounded rumor, sometimes boosted by secrecy on the part of officialdom and a reluctance to confront irrational suspicions, radiation has become everyone's worst nightmare.

Rumbling through the train tunnel on the way out of the Gasteiner Heilstollen, I remembered the idea about painting radiation blue. Whimsically, seeking distraction from the humid heat, I wondered what it would be like if we were consciously aware of radiation. Not by painting it, but by some other means.

Imagine if our eyes could see far beyond the visible region of the spectrum and act as a radiation detector, able to signal everything to the brain as a visual sensation – or even as an auditory one. Or if our skin evolved to tingle in the presence of radiation. But radiation is everywhere, and ever-present. If we could sense it, it would be too distracting, all the time.

One man-made alternative is obvious: imagine cheap and universally available wristwatch-sized Geiger counters set to stay silent — crucial, this — below radiation levels with epidemiologically discernible consequences.



Wearers predisposed to being nervous about radiation might be surprised never to hear their detector going off. Certainly not during my trip under the mountain. Not during a whole-body CT scan. Not even during a week's camping holiday beside the cemetery at Chernobyl. But would that be enough to reassure you?

Geoff Watts is a journalist specializing in science and medicine.

Fukushima's 'mutant daisies' trigger radiation fears

Source: <http://www.wnd.com/2015/07/fukushimas-mutant-daisies-trigger-radiation-fears/>



Four years after the powerful earthquake and tsunami that disabled Japan's Fukushima nuclear power plant, photographs of "mutant daisies," taken near the site, are stirring concerns over the long-term effect of radiation.

The images, posted in May by Twitter user @san_kaido of Nasushiobara City, located about 65 miles from the disaster site, show common daisies that appear to have been affected by radiation exposure, oddly fused together like Siamese twins, reports the Weather Channel.



“The right one grew up, split into 2 stems to have 2 flowers connected each other, having 4 stems of flower tied beltlike,” according to Fukushima Diary. “The left one has 4 stems grew up to be tied to each other and it had the ring-shaped flower. The atmospheric dose is 0.5 μSv/h at 1m above the ground.”



三梅堂
@san_kaido

マーガレットの帯化(那須塩原市5/26)②
右は4つの花茎が帯状に繋がったまま成長し、途中で2つに別れて2つの花が繋がって咲いた。左は4つの花茎がそのまま成長して繋がって花が咲き輪のようになった。空間線量0.5μSv地点(地上高1m)
1:49 PM - 27 May 2015

905 393

That radiation dosage is classified as safe for “medium to long-term” habitation, according to Japanese officials, who have permitted 7,000 evacuated residents to return to their homes near the reactors.

Three of Fukushima Dai-ichi’s six reactors experienced meltdowns following damage from the March 2011 earthquake and tsunami. Radioactive water continues to leak into the Pacific Ocean, with trace amounts found in tuna on the U.S. Pacific coast.

The deformed flowers appear to have a natural, but rare, condition in vascular plants called “fasciation” or “cresting” that has been observed in other parts of the world that have not been exposed to large dosages of radiation.

Most land plants’ tips grow outward from the center as one point produces cylindrical

tissue. But where fasciation occurs, the tip grows outwards and becomes elongated from the point of growth, producing a flat, longer looking flower head.



Cresting or fasciation can be caused by hormonal or genetic defects, bacterial or fungal infection or environmental causes that stress the plant. In this case, radiation may be the culprit.



Nuclear Creepout: Iran's Third Path to the Bomb

By Gary C. Gambill

Source: <http://www.meforum.org/5396/iran-creepout>

In assessing whether the Joint Comprehensive Plan of Action (JCPOA) signed by the P5+1

been blocked, both presuppose a decision by Iran to sacrifice its reconciliation with the world in the next ten to fifteen years for the immediate gratification of building a weapon (the purpose of a covert breakout is less to avoid detection before crossing the finish line than to make the process less vulnerable to decisive disruption). Such an abrupt change of heart by the Iranian regime is certainly possible, but more worrisome is the prospect that Iran's nuclear policy after the agreement goes into effect will be much the same as it was before—comply with the letter and spirit of its obligations only to the degree necessary to ward off unacceptably costly consequences. This will likely take the form of what I call nuclear *creepout*—



world powers and Iran last week is an adequate safeguard against the latter's pursuit of a nuclear weapon, Obama administration officials and arms control wonks typically discuss two heavily stylized breakout scenarios.

In an overt breakout, Iran brushes aside nuclear inspectors and begins openly racing to enrich weapons grade uranium (WGU) using its two declared enrichment plants at Natanz and Fordow. The JCPOA ostensibly blocks this path by limiting the number of centrifuges Iran can operate to 5,060 and capping the amount of low-enriched uranium (LEU) it can keep on hand to use as feedstock at 300 kilograms. This supposedly lengthens its *breakout time*—how quickly it can produce sufficient fissile material for one atomic bomb should it make a rush to build one—from two or three months at present to at least a year, giving the international community more time to mobilize a response to the breakout.

In a covert breakout, or *sneakout*, Iran builds parallel infrastructure in secret to produce the fissile material for a bomb. The JCPOA ostensibly blocks this path with an inspections regime designed to detect the diversion of fissile material, the construction of illicit centrifuges, off-the-books uranium mining, and so forth.

Though much ink has been spilled about whether these two "paths" to the bomb have

activities, both open and covert, legal and illicit, designed to negate JCPOA restrictions without triggering costly multilateral reprisals.

It is important to bear in mind that the JCPOA bars signatories from re-imposing any sanctions or their equivalents on Iran, except by way of a United Nations Security Council resolution restoring sanctions. "That means there will be no punishments for anything less than a capital crime," explains Robert Satloff. The language demanded by Iranian negotiators, and accepted by the Obama administration, makes small-scale cheating virtually unpunishable.

Moreover, the specific terms of the JCPOA appear to have been designed to give the Iranians wide latitude to interpret their own obligations. Two, in particular, should raise eyebrows.

The LEU Cap

About 1,000 kilograms of LEU is supposedly needed to produce, through further enrichment, enough weapons grade uranium for a nuclear explosive device (let's assume for sake of argument that that the Obama administration's erroneous math is correct). This is what inspectors call a "significant quantity" (SQ). The JCPOA's requirement that Iran "keep its uranium stockpile under 300 kilograms" would force it to enrich a substantial quantity of natural uranium all the way



up to weapons grade, thereby lengthening the process of producing a SQ by several months. But what exactly happens to LEU produced by Iranian centrifuges in excess of the 300-kilogram limit? The JCPOA appendix says it "will be down blended to natural uranium level or be sold on the international market and delivered to the international buyer." Maintenance of the 300 kilogram limit relies upon Iran continually and punctually reprocessing or transferring material it already possesses.

What happens if Iran's handling of all this is less than perfect? Suppose 100 kilograms or so of LEU in the process of being down-blended or delivered to an "international buyer" of Iran's choosing routinely remains recoverable at any one time because of apparent inefficiencies and bottlenecks. Would the international community be willing to cancel the JCPOA over this infraction? Almost certainly not.

What if this number swelled periodically to 150 or 200 kilograms every so often because of some special complication or another, like a breakout of plant machinery or truck drivers' strike? Probably not. Since an overt breakout attempt would likely commence at one of these peaks in LEU availability (and when smaller amounts of medium enriched uranium have yet to be converted or transferred), we can knock a month or so off its breakout time.

The Centrifuges Cap

The Obama administration's one-year breakout time calculation assumes that Iran uses only the 5,060 IR-1 centrifuges it is allowed to have spinning under the JCPOA—and that it does not bring more into operation for a whole year after kicking out inspectors and beginning a sprint for a nuke. This could have been achieved by dismantling the large majority of its roughly 15,000 excess centrifuges falling outside this quota, but Iran insisted from the beginning that it would never destroy *any* of them and its adversaries eventually caved.

Although U.S negotiators reportedly proposed a variety of disablement mechanisms designed to slow down the process of reconnecting them, all were rejected by the Iranians and the

final agreement makes no mention of any. The JCPOA requires only that excess centrifuges and associated equipment at Natanz be disconnected and put into IAEA-monitored storage *on-site*. At the Fordow facility, buried deep underground, Iran is allowed to keep "no more than 1044 IR-1 centrifuge machines at one wing" installed, but not enriching uranium. There is considerable disagreement among informed analysts about how long it would take the Iranians to get an appreciable number of these excess machines up and running, with estimates ranging from a few to several months. Whatever that length of time is, the Iranians can surely shorten it by training personnel to rapidly reactivate centrifuge cascades, modernizing equipment, acquiring new technology, and other methods not explicitly barred by the JCPOA.

Indeed, the JCPOA appears to have been drafted by diplomats who failed to imagine that the Iranians might seek to bolster their latent nuclear weapons capacity under the new rules of the game with as much guile and gusto as they did under the old. Considering that the Obama administration's one-year projected breakout time for Iran is deeply flawed to begin with, Iranian exploitation of these loopholes could bring it perilously close to the finish line even while remaining officially in compliance with the JCPOA. If the international community has less time to respond to a breakout attempt, an attempt presumably becomes more likely.

But the real danger is that the mullahs will put off a breakout attempt in the next decade or so, while creeping out of their vaguely worded obligations. With so many opportunities to escape the strictures of the JCPOA, the mullahs would be fools not to offer the minimal degree of compliance necessary to keep it in force (while continually stretching the boundaries of how minimal that degree can be). Openly exploiting the JCPOA's loopholes while enjoying its rewards will do more to intimidate Iran's regional rivals than a reckless dash for the end zone or a high-risk covert attempt, while paving the way for eventual grudging international acquiescence to the Islamic Republic's construction of a bomb.

Gary C. Gambill is a research fellow at the Middle East Forum and former editor of Middle East Intelligence Bulletin.



Cyprus sentences Hezbollah man to six years for anti-Israel bomb plot

Source: <http://www.timesofisrael.com/cyprus-sentences-hezbollah-operative-to-six-years-on-bomb-charges/>



June 29 – **Cyprus on Monday sentenced to six years in jail a Lebanese man who pleaded guilty to terror charges linked to 8.2 tons of potential bomb-making material found in his home.**

Judicial authorities said that Hussein Bassam Abdallah, who also has a Canadian passport, was a member of the military wing of the Iranian-backed Shiite movement Hezbollah.

The 26-year-old was sentenced to jail by a criminal court in the southern town of Larnaca after he pleaded guilty to terror charges.

In passing sentence judge Nicolaos Santis took into consideration the accused's remorse for what he did and what he said was his full cooperation with the authorities.

But he stressed that Abdallah "played the role assigned to him within the broader design of things, so that eventually Hezbollah would be able to harm, through terrorist attacks, Israeli interests in Cyprus."

The charges against Abdallah covered the period 2012 until May 27, 2015, during which time the material was stockpiled in Cyprus.

Abdallah was arrested in a Larnaca suburb in May following a surveillance operation.

Authorities seized some 8.5 tons of ammonium nitrate in the basement of his temporary home.

Ammonium nitrate is a fertilizer that when mixed with other substances can be used to make explosives. The prosecution said this was a method used by Hezbollah.

Prosecution lawyer Polina Efthivoulou said Abdallah had admitted to being a member of

Hezbollah's military wing and sent to Cyprus to ensure the ammonium nitrate was safely kept. She said the bomb-making material was intended for terrorist attacks against Israeli interests in Cyprus.

Foreign Minister Ioanis Kasoulides said during a visit to Israel earlier this month that the authorities believe they have thwarted a possible attack on Israeli targets.

The island attracts thousands of tourists from nearby Israel every year. There is also an Israeli embassy in the capital Nicosia.

Defense lawyer Savvas Angelides said his client's role was only to check on the nitrate and to move it to another location — not to carry out attacks.

He also urged the court to show leniency, saying that his client cooperated with authorities and had decided to quit Hezbollah.

Investigative sources have said the amount of ammonium nitrate seized by authorities is the biggest anywhere in the world.

Abdallah also had nearly 10,000 euros in his possession when caught.

Cyprus is not known for its militant activity despite its proximity to the Middle East.

But in 2013, a Cypriot court sentenced a Lebanon-born Swedish man who admitted he was a Hezbollah member, to four years in jail after he was found guilty of targeting Israelis on the island.

A botched bomb attack on the Israeli embassy in 1988 claimed the lives of three people.



IEDs remain insurgents' top gun

Source: <http://www.usatoday.com/story/news/world/2015/07/10/ieds-isis-iraq-syria/29971673/>

July 10 – Islamic State militants are deploying the signature weapon of the Iraq war — the homemade, roadside bomb — in novel ways, including the use of drones to spot targets, a top Pentagon official says.

The tactics used by Islamic State fighters in Iraq and Syria have evolved rapidly with improvised explosive devices (IEDs), Lt. Gen. John Johnson, director of the Joint IED Defeat Organization, told USA

TODAY in an interview. Militants around the world continuously share best-practice tips online, Johnson said.

The IEDs used by the Islamic State, also known as ISIS and ISIL, have been cobbled together with homemade- and military-grade explosives and munitions seized from Iraqi and Syrian security forces.

"They're using everything they can get their hands on," Johnson said. ISIL also has used

could be turned into a new form of IED. "That's a question," he said.

- **Bigger bombs.** Seized military vehicles have been jammed with explosives to produce huge explosions that can penetrate even fortified structures. ISIL's initial assault on Ramadi on May 17 included the use of 30 massive car bombs, prompting Iraqi security forces to flee despite outnumbering the militants.

- **Tunnels.** In Syria, ISIL fighters have been burrowing beneath their targets to avoid detection before setting off IEDs.

At the height of the U.S. war in Iraq in 2007, IEDs caused 70% of American casualties. The rapid, massive introduction of

Mine Resistant Ambush Protected (MRAP) vehicles, bolstered intelligence gathering on bomb networks and improved security brought about by the counterinsurgency strategy helped reduce deaths and injuries caused by IEDs.

Homemade bombs remained the top killer in Afghanistan where U.S. forces shifted their forces in large numbers by 2009. Those two countries remain the global hotspots for IED attacks, according to JIEDDO, followed by Colombia, Syria and Pakistan.

Worldwide, the number of IED attacks has decreased but the number of casualties has increased, indicating a trend toward larger, more lethal weapons.

JIEDDO statistics show **there has been a 42% increase in high-profile attacks, particularly in Iraq, Nigeria, Afghanistan and Yemen,** which has been mired in a civil war.

"This threat isn't going to go away," Johnson said.

JIEDDO isn't either. The military's counter-IED arm, which began as a temporary Army task forces in the early days of the Iraq war and mushroomed into a multi-billion dollar agency,



chlorine as a chemical weapon, he said. Meantime, ISIL fighters have been modifying their tactics to exploit holes in the defenses of friendly forces, Johnson said.

Some of their adaptations, according to Johnson:

- **Drones.** To date, the drones have been used to direct drivers of car bombs to their targets inside Iraqi-held territory, Johnson said. He noted that the unmanned aircraft "can deliver some sort of payload," meaning the drones



has become a permanent Pentagon fixture. Beginning Monday, it will have a new name,

the Joint Improvised-Threat Defeat Agency, or JIDA.

'ISIS Blows Up Baby in Training Class Demo'

Source: <http://www.clarionproject.org/news/isis-blows-baby-training-class-demo>

In one of its cruelest acts to date, Islamic State reportedly blew up a baby to show members how to handle explosives.



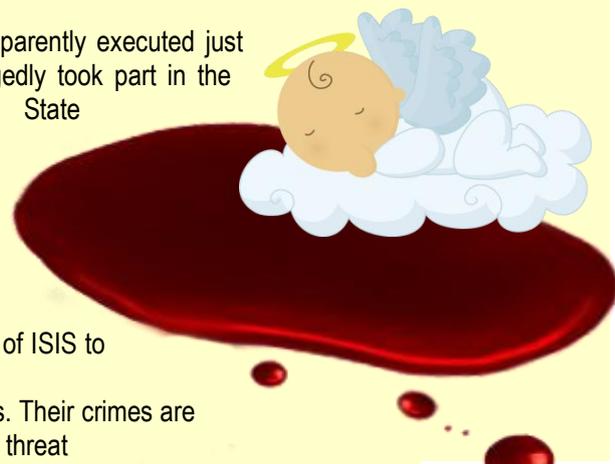
The incredible incident took place in Diyala Province on July 10, according to provincial Security Committee Chairman Sadiq el-Husseini. He detailed the event to the local Arabic-language [A-Sumeriah News](#).

The baby's father was apparently executed just weeks ago, after he allegedly took part in the killing of an Islamic State member.

Sadiq el-Husseini "The organization booby trapped the baby in front of dozens of armed

ISIS men and then detonated it from afar," Sadiq el-Husseini said. The rigging of the baby and its detonation was a training exercise of ISIS to teach its people booby-trapping techniques.

"The organization doesn't care about the most basic human values. Their crimes are incalculable and the blowing up of the baby is the best proof to the threat of ISIS' ideology to the state."



Hi-Tech Explosives Detection Systems

Source: <http://i-hls.com/2015/07/hi-tech-explosives-detection-systems/>



Morpho, through its subsidiary Morpho Detection, announced a contract assigned to its local partner Segtec by Mexico airport operator Grupo Aeroportuario del Sureste (ASUR) for 14 CTX explosives detection systems (EDS).

Under terms of the contract, eight high-speed CTX 9800 DSi™ and six compact CTX 5800 EDS will be deployed to enhance hold baggage screening and operational capabilities at six different airports. SEGTEC will supply maintenance and rapid-response service supported by Morpho Detection to ensure peak performance and

maximum system uptime.

"We are thrilled that ASUR has recognized the CTX family of EDS as having the detection and operational capabilities needed to meet their growing traffic and security demands," said Karen Bomba, president & CEO, Morpho Detection. "Combined with a global service footprint, Morpho Detection's CTX EDS give airports of all sizes the ability to deploy an



automated checked baggage screening program and increase return on investment (ROI) on security infrastructure purchases.”



Capable of screening more than 1,000 bags per hour (BPH), Morpho Detection’s high-speed CTX 9800 enhances operational efficiencies by screening bags faster and with fewer false alarms. Designed to allow small- and mid-sized airports plan for evolving threats and future expansion, CTX 5800 combines industry-leading imaging and data collection in a smaller and lighter solution.

Morpho Detection’s unique Clarity technology, found in both CTX 5800 and CTX 9800, enables both

systems to screen checked luggage at higher speeds while continuing to deliver high-resolution 3-D (HD3-D) images of each bag. Both the computed tomography (CT)-based CTX 5800 and CTX 9800 are certified by the U.S. Transportation Security Administration (TSA) and Civil Aviation Administration of China (CAAC) and approved by the European Civil Aviation Conference (ECAC) as meeting EU Standard 3 requirements.



Morphix Technologies Releases Instructional Video on How-to-Use the TraceX Explosives Detection Training Kit

Source: <http://www.hstoday.us/single-article/morphix-technologies-releases-instructional-video-on-how-to-use-the-tracex-explosives-detection-training-kit/2f20f7e02c0b1086a2e19040e1e57a18.html>



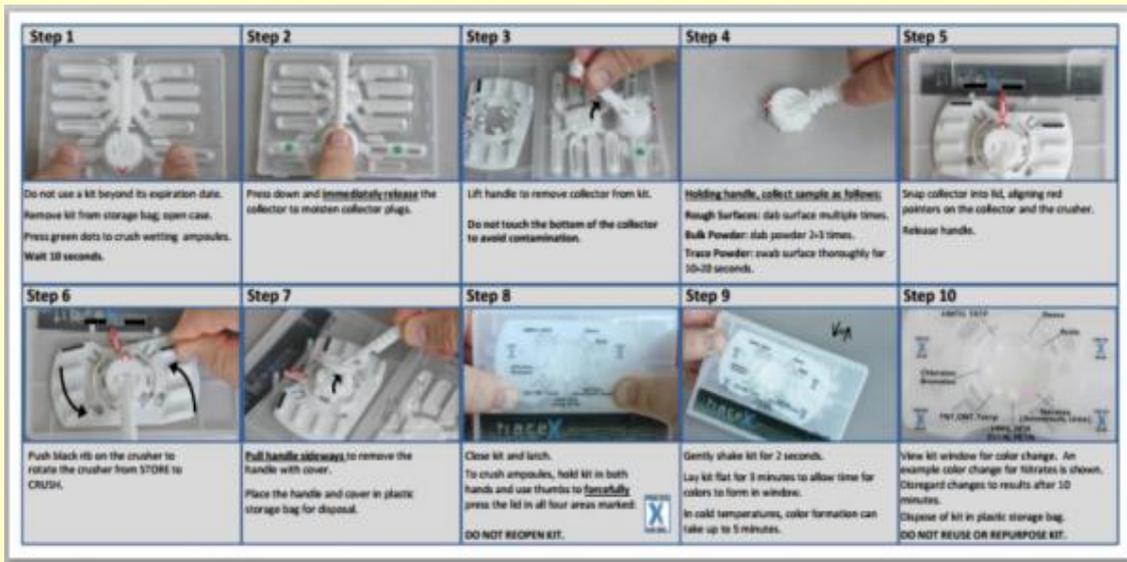
Morphix Technologies has created an instructional video with step-by-step instructions on how-to-use the TraceX Explosives Detection Training Kit. The kit has been newly designed for military, law enforcement and intelligence personnel training facilities and schools in response to the increasing need for homemade explosive detection training. The video



instructs these individuals how to use the training kit and the importance of the product; it can be viewed on YouTube here.

Once trained, military, law enforcement and intelligence personnel will be able to quickly and easily identify bombers, bomb-makers and their bomb-making facilities in a single test using the TraceX Explosives Detection Kit.

“We created this instructional video as part of our commitment to ensure users have the training tools to confidently use the TraceX Explosives Detection Kit. We hope that this training will help you identify bomb-makers who use explosive devices to cause destruction and fear,” said Kimberly Pricenski, Morphix Technologies VP of sales and marketing.



The TraceX Explosives Detection Training Kit makes training simple. Each Training Kit comes with a set of pictorial operating instructions and is provided in a sealed pack containing one TraceX Explosives Detection Kit, a blue plastic film and a foil bag labeled “citric acid powder.”

▶ You can explore the video at: <http://www.morphitec.com/products/tracex/training/>



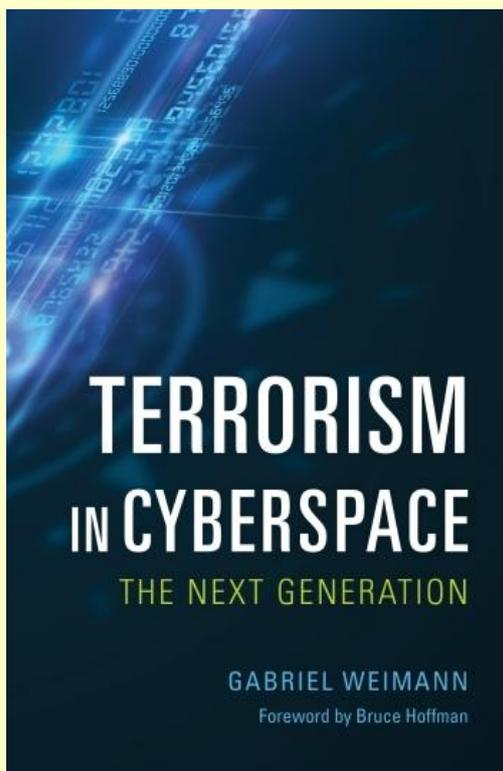
BOOK – Gabriel Weimann: “Terrorism in Cyberspace: The Next Generation”

(New York, NY: Columbia University Press/Washington, DC: Woodrow Wilson Center Press, 2015), 313 pp.

Reviewed by Joshua Sinai

Source: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/429/html>

In the United States, Canada and Western Europe, dozens of al Qaida, al Shabaab- and ISIS-related terrorist-related plots have been thwarted by government counterterrorism agencies through electronic surveillance of terrorist operatives' suspicious activities on the



Internet. While their activities were likely also monitored “on the ground,” the fact that terrorists of all extremist ideological and religious types are so reliant on using their computers and smartphones to access the Internet for their communications, cyberspace has become a necessary focus of operations for counterterrorism agencies.

Tracking the suspicious activities of potential terrorists in cyberspace is so crucial, in fact, that in certain cases where terrorists succeeded in carrying out their attacks, such as Major Nidal Hassan’s murderous rampage at Fort Hood and the Tsarnaev brothers’ bombing of the Boston Marathon, electronic data had existed about their suspicious online activities, but counterterrorism agencies had failed to ‘connect the dots’ to appreciate the

significance of such evidence in their possession prior to these incidents.

Because it is obvious to counterterrorism professionals from intelligence and law enforcement that it is crucial to electronically monitor such suspicious activities (with full legal compliance), it has been somewhat surprising to see the recent controversy in the United States Congress over reauthorization of electronic surveillance operations under the Patriot Act [which was passed in a modified form in early June]. For this reason, among others, we are fortunate to have Gabriel Weimann’s “Terrorism in Cyberspace: The Next Generation,” as an authoritative account of the ways in which terrorists operate in cyberspace. Dr. Weimann (whom I know and, for full disclosure, also wrote the blurb on the book’s back cover), is Professor of Communications at the University of Haifa, Israel, where he leads a research program that tracks terrorist activities on the Internet. He also is the author of the landmark book *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: USIP Press, 2006).

In his new book, Gabriel Weimann addresses the following questions: how are terrorists exploiting the Internet, what new trends in cyberspace can be expected in the future, how can terrorist operations on the Internet be effectively countered, and how can we balance the need for security while protecting civil liberties.

Prof. Weimann explains that terrorist groups—and lone wolves—view the Internet as an ideal arena to exploit for their communications, propaganda, training, fundraising, and for mobilizing support for their violent activities because of its ease of access from anywhere around the world, “lack of regulation, vast potential audiences, fast flow of information,” and, most importantly, the anonymity to post “their extremist beliefs and values” and then “disappear into the dark.” (p. 21). Terrorists and their supporters exploit the Internet’s websites, email,



chatrooms, virtual message boards, mobile phones, Google Earth, YouTube and other online video sharing sites, as well as social networking sites such as Facebook and Twitter. Such exploitation, however, is not being conducted openly, as their tech-savvy operatives often use encryption tools and anonymizing software to make it difficult for counterterrorism agencies to identify “the originator, recipient, or content of terrorist online communications.” (p. 23)

Dr. Weimann identifies three new trends in Internet exploitation: narrowcasting (targeting propaganda and recruitment messaging to narrow audiences that are deemed to be especially susceptible, such as children, women, lone wolves, and diaspora communities), encouraging the proliferation of lone wolf adherents, such as Major Nidal Hassan, and advancing cyberterrorism.

The proliferation of lone wolves is especially worrisome, according to the author, because “they are extremely difficult to detect and to defend against.” (p. 66) Nevertheless, they are not undetectable to counterterrorism agencies because they must still “connect, communicate, and share information, know-how, and guidance — all online — on the ‘dark web.’” (p. 66)

Cyberterrorism is the most threatening of the trends, according to Gabriel Weimann, because they would be able to use their “computer network devices to sabotage critical national infrastructures such as energy, transportation, or government operations.” (p. 150) Dr. Weimann warns that terrorists are keen to develop a cyber-warfare capability, with the possibility of “money, ideology, religion, and blackmail” being used to recruit such “cybersavvy specialists” in the future.

How can terrorist exploitation of cyberspace be countered and defeated? While the Internet and its online platforms, as Dr. Weimann points out, provide terrorists with “anonymity, low barriers to publication, and low costs of publishing and managing content,” (p. 150) at the same time they also provide counterterrorism agencies with the capability to damage and block them. Under what Dr. Weimann terms the “MUD” model (monitoring, using, and disrupting), he recommends covertly tracking their activities in order to gain information about their strategies, motivations, internal debates and associations, while disrupting them with ‘hard’ power cyber-weapons to spread viruses and worms against their websites. These would be accompanied by ‘soft’ power elements that conduct psychological operations to discredit their extremist propaganda and offer constructive alternatives to resorting to terrorism..

In light of the still continuing controversies over the electronic surveillance provisions of the Patriot Act, the book’s final chapter, “Challenging Civil Liberties,” is particularly valuable in discussing the challenges presented by the need to preserve civil liberties when countering online terrorist activities. Dr. Weimann cites the impact of Edward Snowden’s illicit revelations of the U.S. government’s counter-online surveillance measures and proposes a set of guidelines to regulate governmental online surveillance.

“Terrorism in Cyberspace” is a timely and indispensable resource for all those concerned about effectively countering terrorists’ exploitation of the Internet’s and the dark elements that can reside there.

About the Reviewer: *Dr. Joshua Sinai is the Book Reviews Editor of ‘Perspectives on Terrorism’.*

Abu Dhabi’s power system to be used for critical infrastructure cybersecurity study

Source: <https://www.masdar.ac.ae/media-section/news/item/6547-innovative-masdar-institute-and-mit-research-targets-uae-cyber-infrastructure-security-challenges>

June 29 – Masdar Institute of Science and Technology, an Abu Dhabi, UAE-based university focused on advanced energy and sustainable technologies, has recently launched a collaboration with the

Massachusetts Institute of Technology (MIT) to advance cybersecurity research in the UAE.



The objective of the study is to ensure better cybersecurity on critical infrastructure sites in the UAE and globally by assessing potential vulnerabilities to cyberattacks on critical infrastructure. Using Abu Dhabi's power system as a case study, the research will undertake a multilayered methodology to develop a knowledge map of the power system and its shortcomings.

Dr. Fred Moavenzadeh, president, Masdar Institute, said, "Through Masdar Institute's ongoing research efforts, greater emphasis is being placed on the protection of critical infrastructure sites by enhancing cybersecurity. This project will help to develop the Institute into a knowledge center for cybersecurity in the UAE and promote Masdar Institute and its Institute Center for Smart and Sustainable



Systems (iSmart) as a leader in cybersecurity research. The collaboration with MIT will also help to identify competency gaps, generate critical mass between the faculty and develop human capital in the niche area of cybersecurity."

Masdar notes that the collaboration will see Masdar Institute and MIT undertake research involving Abu Dhabi's power system and will focus on using a novel approach to identifying the different sources of cyber gaps in a critical infrastructure system. The research will also investigate the significance of each of these challenges to the integrity of the physical system.

This collaboration is a project of the MIT Technology and Development Program. The principal investigators of the project are Dr. Sameh El Khatib, Assistant Professor in the Masdar Institute Department of Engineering Systems and Management and member of iSmart, and Dr. Nazli Choucri, Professor of Political Science at the MIT School of

Humanities, Arts and Social Sciences, and Principal Investigator and Director of the MIT/Harvard initiative in Explorations in Cyber International Relations (ECIR).

Masdar also notes that a number of research projects have already been undertaken better to secure conventional information systems, but no research had been conducted regarding the protection of critical infrastructure. Dr. Choucri and Dr. El Khatib's work will correct this by addressing the cybersecurity of critical infrastructure. The research will also serve as a guide for policymakers in an age where cybersecurity has become one of the biggest issues for businesses and government.

"Our research aims to contribute to the development of cybersecurity as an emerging field of scientific inquiry. To date, there have

been few robust scientific investigations that provide comprehensive evidence on the sources and consequences of cyber security. The overarching goal of the project is to analyze and define the science behind cyber security in an effort to provide substantial and concrete scientific data related to the weaknesses of critical infrastructure and how to better protect them," said Dr. El Khatib.

The project is due to run for two years. At the end of this two year

period, the collaborating institutions hope that data from the analysis of Abu Dhabi's power system could be compared against data from the projects running concurrently in New York and Singapore to develop a comprehensive knowledge map, capable of being applied to critical infrastructure worldwide. It will also aid with the development of human capital in this area, beginning with the five Masdar Institute students — three of which are UAE nationals — which are working with Dr. El Khatib in this cybersecurity project.

Speaking about her involvement in the project, UAE national student Reem Al Hammadi said, "By undertaking this research in collaboration with MIT, I have had the opportunity to develop knowledge and highly technical skills related to the niche area of cybersecurity and critical infrastructure. The continued development of local talent by Masdar Institute in this area will ensure that the UAE is fully equipped to advance research



related to cybersecurity and critical infrastructure.”

The research collaboration is part of the Masdar Institute and MIT Joint Cooperative Program and in collaboration with the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC³), which is one of three recently launched initiatives by MIT dedicated to lead global research in cybersecurity. The (IC)³ initiative,

which is directed by Dr. Stuart Madnick, Professor of Information Technologies, MIT Sloan School of Management and Professor of Engineering Systems, MIT School of Engineering, has been formed to address the need to improve the cybersecurity of critical infrastructure, with a focus on strategic, operational and managerial issues related to cybersecurity.

So what is the **Duqu2** malware?

Source: <http://i-hls.com/2015/06/so-what-is-the-duqu2-malware/>



Countries with reported Duqu infections. Red represents confirmed infections, orange represents unconfirmed reports.

June 29 – Earlier this year a new malware was detected in Kaspersky company’s labs which spread and affected the company’s systems.

Following this finding, the company launched a thorough investigation by the end of which, company researchers discovered a new species of malware whose capabilities suggest a high level of sophistication and advanced spying abilities.

Following this discovery, the company researchers updated relevant authorities around the world, after which more tainted systems were discovered across the U.S., England, Sweden, India and Hong Kong.

Further tests revealed that attackers used malware to spy after the Iran nuclear talk in hotels around Swiss and also in the 70 years for Auschwitz’s liberation events.

The Duqu2 is actually a new and updated variant of the infamous Duqu, hence its name.

Just to serve as a reminder, the Duqu malware is an advanced spyworm whose capabilities are

gathering data (sensitive files, passwords, users details and more) and deleting files in the infected computer. Duqu had some obvious features, among them the use of Zero-Day hits of the Windows operating system (CVE-2011-3402) and using stolen certificates as disguise to bypass the information security system. In addition, Duqu had the ability to communicate in real-time with its operators for receiving instructions through a command server (C&C). Duqu passed the sensitive information to its operators by creating files beginning with dq~ and sending them by mail or by disguised communication to a data gathering website disguised as an innocent website.

Beyond that, Duqu also used Jpeg files and encrypted folders to store secret data and transmit it. After 36 days of spying, Duqu deleted itself from the computers and systems without a trace.

Analyzing Duqu2 and its method of action reveals the following:



The structure of the malware:

Duqu2 is built of 2 parts, the first being a Backdoor which allows for a two-ways communication between the victim's computer and the malware operators. The second part of the malware is made up of several modules that offer advanced intelligence gathering capabilities such as: mapping the network the victim's computer is connected to, remote activation of means for electronic eavesdropping built in the victim's computer (microphone/camera and such).

Ways of infecting the victims:

The initial method of the malware infection is unknown, but suspicion is that it was done by sophisticated, focused fishing mail. This suspicion is based on the fact that in the computers suspected as initial infection points, all browsing history and mail correspondence has been deleted.

The next stage of attack:

In order to plant the Duqu2 inside the victim's computers, attackers used Zero-Day hits in the Windows Operating System which allows the domain user to simply expand their authorities to Administrator and there was also use in "pass the hash" to go through computer in the internal network and thus reaching the total of network resources.

We should point out that attackers protected the attacking worm so it survives the Microsoft Security Patch by having it presenting an "original" digital certificate by Foxconn and others like it to prove its legality inside the system.

Once Administrator authorizations were granted, the attackers made several things to spread the malware inside the computerized network: they prepared coded installation packs for the malware disguised as legitimate installation pack for Windows MSI and spread them throughout the network. The means for spreading was by using a `msiexec.exe` (an operating system file used to install softwares). In addition, the attackers created a service in the network to run this installation pack as Task Scheduler in the operating system.

Once the pack is running through the network computers, the pack was used as a loader for the rest of Duqu2 modules. From an inspection done, it seems that the installation pack contained about ten different modules allowing the spying capabilities mentioned later on.

It should be mentioned that the attackers were careful enough to use a number of encrypting

algorithms and different file names in order to avoid detection by protections such as AntiVirus. This fact indicates a high level of sophistication and a deep understanding of the malware detection field by the attackers.

The Duqu2 orchestrator is the component for communication with the attackers C&C servers. Communication was done by Https protocol coded under the Self-signed Certificate. The attackers also used SME Network pipes protocols, TCP/IP link in designated protocol and also in Http protocol for passing encoded and encrypted information sealed inside Jpeg/GIF image files, as was done by Duqu.

Beyond the module orchestrator, the installation pack contained more spying modules. The main ones being:

A module for gathering information on the computer and network it is on.

A module for seeking domains, mapping all servers and network shares in the domain.

A taping module designed to steal admin passwords from processes performed on the computer and through them, connect to more computers.

A remote desktop administration module that includes the ability to send and receive data to the desktop, move the mouse marker and photo the user's desktop.

A module for detecting network sniffers working in the computerized platform (wireshark, tcpview, netstat, sumpcap, perfmon and such).

A module allowing extracting information from databases.

Another part of the uniqueness and complexity of Duqu2 is that the attacking worm worked in the infected computer's memory, meaning that it did not leave behind any trace (at the moment of turning the computer on and off, the worm disappears). In order to re-spread it after the computer was turned off and on, attackers infected highly available servers and from there sent the worm to machines with lower availability.

Duqu2 is the next generation of spyware. Its level of sophistication presents technological abilities that suggest that a country or some body with substantial resources was behind it.

A spelling mistake in the information gathering module suggests that the writer of the module does not speak English as a native-tongue, but there's no way of knowing whether or not this mistake was put in on purpose.



In conclusion, we have no information today as to why the Kaspersky company computerized network was infected or who is behind it. So

far, we have been exposed to a variety of theories regarding the attackers' identity, but neither we nor anyone have any valid proof.

Doctors See Big Cybersecurity Risks, Compliance as Key for Hospitals

Source: <http://www.xconomy.com/boston/2015/07/01/doctors-see-big-cybersecurity-risks-compliance-as-key-for-hospitals/>

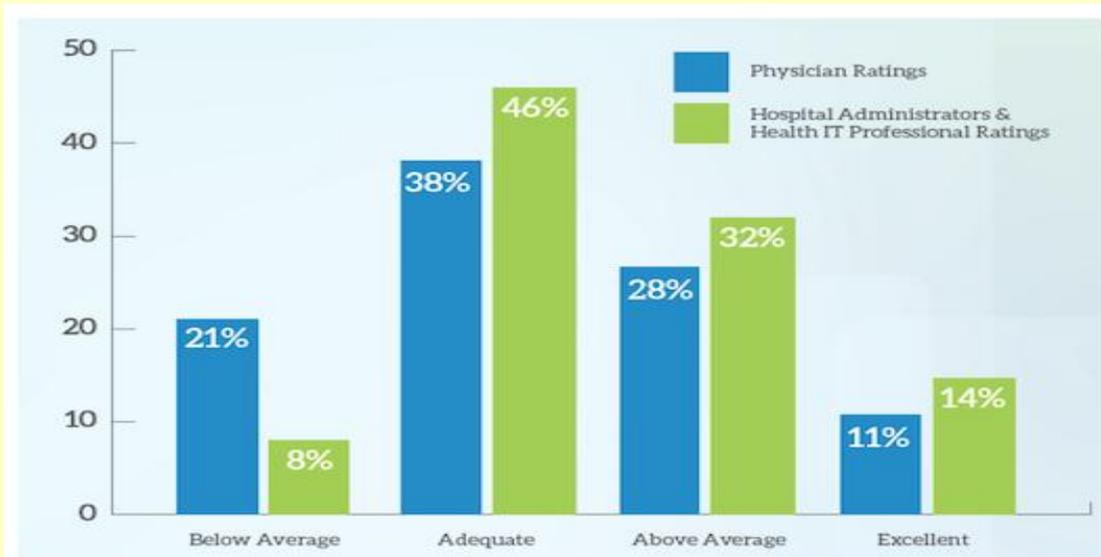
Cybersecurity and healthcare IT are both burgeoning areas of business. Put them together and you



have a volatile mix of emerging technologies, security and privacy risks, and regulatory requirements—but also a lot of opportunity for growth and improvements. It's no surprise that doctors and hospital administrators are concerned with security. The healthcare industry is a top target of cyber attacks (see the Anthem data breach), and it has highly sensitive information about large swaths of the population.

But a new survey from MedData Group in Topsfield, MA, shows that physicians have very different opinions about cyber threats as compared to administrators and health IT professionals. The survey was done in June and polled 272 doctors and healthcare workers around the U.S.

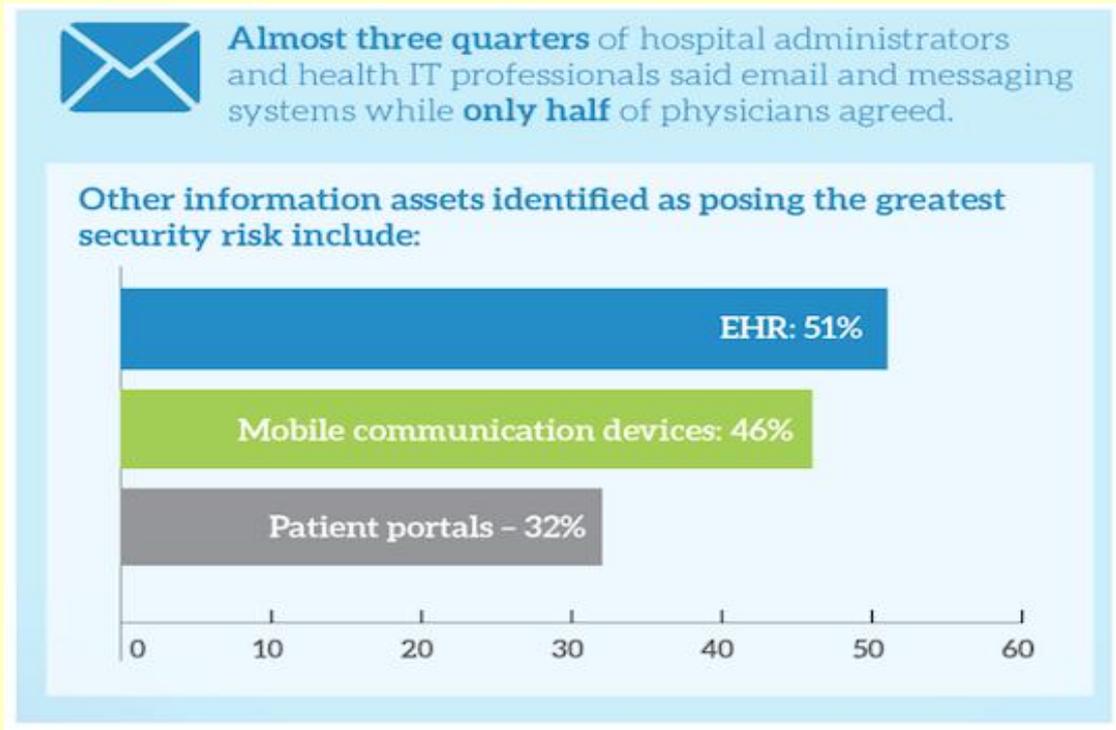
59



A key finding is that doctors gave lower ratings to their organizations' abilities to counter cyber crime than did hospital administrators and IT personnel. The chart below shows 21 percent of doctors rated their clinics' cybersecurity systems as below average, as compared to only 8 percent of administrators and IT workers. (Not surprising, perhaps, but I'm going with the doctors on this one.)

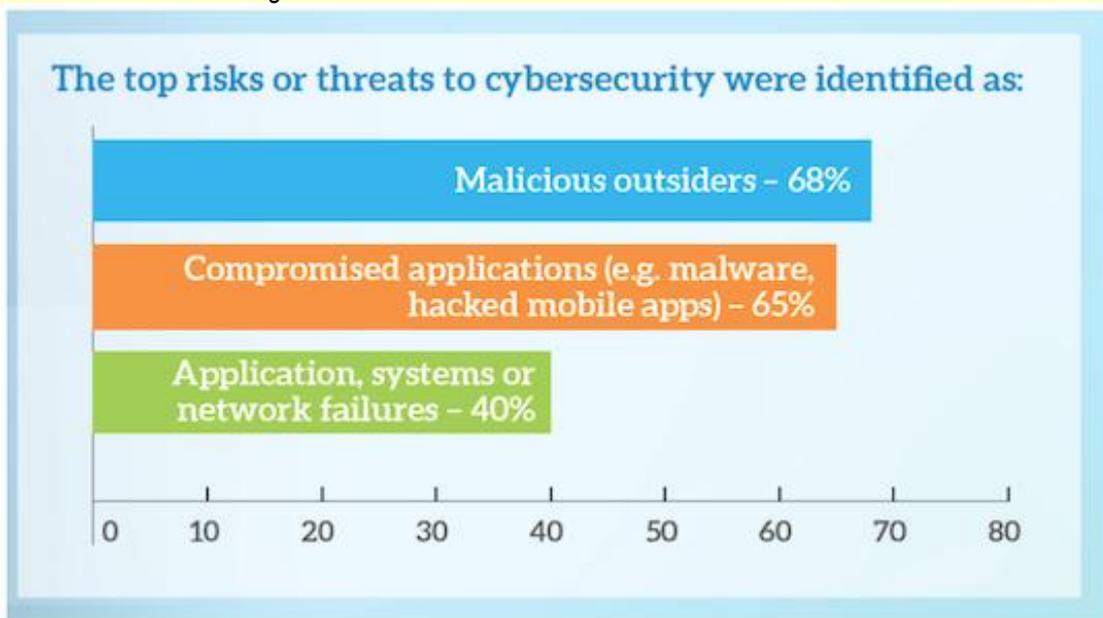


Another difference of opinion is in where the greatest vulnerabilities lie. Administrators tend to cite e-mail and messaging systems as the top weakness, while doctors also list electronic health records, mobile devices, and patient portals:



What everyone seems to agree on is where the threats are coming from. Across all healthcare staff surveyed, the top risks cited are malicious outsiders, malware, and hacked mobile apps, with application or network failures coming in after that:

60



Another point of agreement is on what will drive change. Eighty-three percent of respondents said the top driver for securing sensitive data in healthcare organizations is the need to comply with standards and regulatory requirements.

The healthcare industry has enough to worry about without getting hacked, of course. Sadly, this is the reality in any sector whose companies and organizations have access to



a lot of valuable information. Now is the time to listen to those on the front lines—before the next big attack is discovered.

Studying terrorists' social-media recruiting power in order to negate it

Source: <http://www.homelandsecuritynewswire.com/dr20150703-studying-terrorists-socialmedia-recruiting-power-in-order-to-negate-it>

July 03 – **Last month a United Nations panel asked social-media companies such as Twitter and Facebook to respond to how terrorist groups use their networks to spread propaganda or recruit members with increasing success.** As these terrorist groups,

such as ISIS or al-Qaeda, evolve their social-media skills, Arizona State University will be part of a team monitoring their advancements and trying to determine how their online actions can be negated.

ASU is leading a group project that has been awarded a Minerva grant to study of what types of information go viral online, and what types of actions or responses can halt the spread of viral information.

The Minerva Initiative is a Department of Defense-sponsored, university-based social-science research initiative launched by the secretary of Defense in 2008. It focuses on areas of strategic importance to U.S. national security.

An ASU release reports that this grant will allow the team, which includes people from the U.S. Military Academy and Britain's University of Exeter, to study information cascades — trends marked by people ignoring their own knowledge or information in favor of suggestions from other people's actions — as they relate to the social-media posts of terrorist networks.

"The first phase of the project is we are trying to understand what goes viral. The viral (message) is driven by two things: what type of content and what type of network. The right content and the right types of networks are going to resonate and spread and maybe gain new followers," said Hasan Davulcu, the project's principal investigator, and an associate professor in ASU's Ira A. Fulton School of Engineering and director of ASU's Cognitive Information Processing Systems Lab.

Once they understand the information cascade, Davulcu said they might be able to determine how to counter the viral messages. But, he clarifies, that this study will not include developing content to thwart online terrorism. Rather, the team will be observing what organic information created by social-media users tends to halt terrorists' viral content.

"It's the early detection of what works for them and what works for others opposing them," Davulcu said.

The team believes images and videos might be some of the more persuasive ways to create partisan passion.

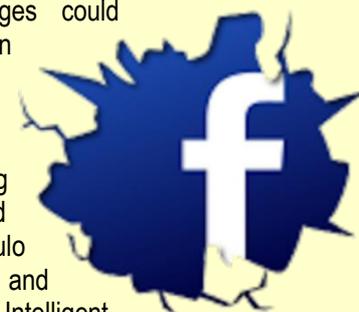
"We are finding pictures to be extremely telling," Davulcu said. "In fact, we are going to collect tons of photos that circulate online and put them into games so we can figure out what do people understand by the picture."

These images could be pictures of enemies or adversaries; a photo of Ghandi to illustrate peace; or something as common as a sports star, suggesting action. Studying the use and relationships of these images could provide a lens into the diffusion of various ideologies.

"It is impossible to monitor all of the conversations, so we have to get better at identifying the ones to which we should be paying attention," said Paulo Shakarian, a team member and director of the Cyber-Scio Intelligent Systems Lab at ASU. "This requires embedding psycho-social models in a logic programming framework that can gather and analyze social networks, specific attributes of individuals and their relationships to others."

Shakarian understands the issue of terrorism from another perspective, as a former member of the U.S. Army who served two years in Iraq.

"The idea is that if we can understand which of the postings and messages of ISIS have the potential to go viral then we can



learn to combat that much better than we do now," he said.

ASU's Minerva grant is situated in its Center for the Study of Religion and Conflict, which incubates new research into the complex role of religion in human affairs.

Mark Woodward, associate professor in ASU's School of Historical, Philosophical and Religious Studies, and Baoxin Li, associate professor of ASU's School of Computing, Informatics and Decision Systems, are also part of the Minerva team.

This is ASU's second Minerva grant. The first was awarded in 2009 to study how to strengthen the voices of the Muslim majority who didn't condone violence.

Davulcu and Woodward were a part of that project, as well. If this second one goes well, there could be more in the future.

"The transdisciplinary environment of ASU has really enabled us to bring together faculty in innovative ways," said Linell Cady, director of the Center for the Study of Religion and Conflict.

"The fact that we have developed two successful Minerva projects is a real testament to the way in which integrating the deep knowledge of the humanities with cutting-edge computer science can produce a whole much greater than the sum of its parts."

5 years of cybercrime: where we've been and where we're going

Source: <http://www.information-age.com/technology/security/123459774/5-years-cybercrime-where-weve-been-and-where-were-going>



Cybercrime is always changing. Despite new developments in cyber security and increases in security budgets, the five years have seen an uptick in major security breaches.

Companies – and even consumers – are creating, storing, and utilising data at unprecedented rates. And it is data that cybercriminals are after, yet many enterprises continue to allocate the bulk of their security technology budgets to network and device security rather than data protection.

62

In fact, research shows that companies allocate just 1% of their total security technology spend to data protection measures. Here's a look at the state of cybercrime over the past five years, and a look ahead at where we're going.

2010: Nearly half of security technology spend allocated to network security

In 2010, companies spent nearly half of their security technology investment (44%) on network security. In that same year, 761 major data breaches were recorded, compromising 3.8 million records.

Physical tampering, spyware, and data-exporting malware were the top three attack methods, yet little spend was dedicated to protecting the very data that serves as the target for so many attacks.

Less than a fifth (19%) of security spend was dedicated to database security, 14% to application security, another 14% to endpoint security/anti-virus, 10% to identity management, and just 1% to data protection.

2011: Stolen credentials emerge as a top mode of attack

In 2011, spyware remained a top mode of attack, joined by brute force and the use of stolen credentials. There were a multitude of notorious cybercriminals who emerged as **serious threats to companies like Sony Pictures, the Massachusetts Institute of Technology (MIT), and others** in 2011.

Yet companies continued to invest most of their security technology spend to network security (39%). In 2011, 855 major data breaches were recorded, compromising 174 million records, a marked increase over 2010 statistics.

Companies saw a slight increase in spend dedicated to database



security in 2011 (21%), while spend on application security and endpoint protection/anti-virus remained stagnant at 14%. Despite the massive increase in attacks through the use of stolen credentials, companies continued to invest just 1% in data protection.

2012: Network security continues to receive the bulk of security technology spend

In 2012, spyware and the use of stolen credentials remained among the top three methods of attack, joined by backdoor

any other method, with data-exporting malware and phishing rounding out the top three modes of attack.

There was a marked increase in both the number of major data breaches recorded and the total number of records compromised occurred in 2013 – with 1,367 major breaches resulting in the **compromise of 822 million records**, including the well-known Target data breach which **compromised as many as 70 million records** alone.

Still, companies dedicated 40% of their total security technology spend on network security, while 21% went to database security, 16% to application security and 12% to endpoint security/anti-virus. Still, just 1% of total security spend was dedicated to data protection, despite the marked increase in stolen records and data theft.

2014: Number of data breaches continues to rise dramatically

In 2014, stolen credentials remained the top mode of attack used by cybercriminals, followed by RAM-scraping malware and



exploitation. In fact, 2012 was the year in which the now widely known **hacking team first gained recognition for its Remote Control System (RCS)**, a sophisticated spyware program marketed and sold exclusively to governments and claimed to be untraceable.

Companies experienced a slight decrease in the number of data breaches from 2011, with 621 major data breaches recorded compromising 44 million records.

Companies increased their total spend on network security in 2012, allocating 43% of their total security technology budgets to network security. Other spend remained largely similar, with a slight decrease in spend dedicated to identity management.

More than a fifth (21%) of total security spend went to database security, 15% to application security, 13% to endpoint security/anti-virus, 8% to identity management, and again just 1% to data protection.

2013: Use of stolen credentials becomes the top mode of attack

In 2013, attackers used stolen credentials to carry out data breaches more frequently than

spyware. **Sony experienced another major breach in 2014**, revealing more than 47,000 Social Security numbers and other valuable sensitive data.

Overall, companies experienced another dramatic rise in the number of major data breaches, with 2,122 major recorded breaches compromising 700 million records.

Even with a marked increase in the number of data breaches and continued data showing that stolen credentials are a frequently used mode of attack, companies failed to shift their security spend accordingly.

In 2014, 38% of security technology spend was dedicated to network security, 18% to endpoint security/anti-virus, 16% to application security, another 16% to database security, and 13% to identity management. Data protection remained the lowest spending category at only 1% of total IT security technology spending.

2015: Cybercrime continues to grow in reach and sophistication

The attacks have grown in sophistication as cybercriminals



use new tools and malicious programs to infiltrate corporations and exfiltrate sensitive data that includes personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) records as well as intellectual property and other confidential documents.

Cybercriminals have grown more creative, using stolen PII from previous large data breaches to commit fraud and identity theft.

For example, in May the IRS reported that cybercriminals used one of the **IRS's online services to obtain tax return information for more than 100,000 households** in the US. The cybercriminals used stolen PII to gain unauthorised access to the tax-agency accounts. Around 15,000 fraudulent refunds were issued as a result.

The large leak of PII from high-profile breaches such as Target and Home Depot places consumers at risk for identity theft and fraud, yet the corporations are the ones responsible for losing consumers' PII.

If more stringent data protection technologies and strategies were put in place, these incidents could have been mitigated and contained to a much smaller scope.

Cybercriminals now run a fully monetised operation and will not relent in their attacks on corporations. However, organisations can prevent these attacks from succeeding if they turn their current cyber security strategy upside down and start focusing on data protection technologies and strategies rather than network security and traditional anti-virus.

Today's technology is advancing at a rapid rate as new ways to leverage cloud applications, mobile devices and complex systems continue to change and evolve. The ways people and organisations use and access data also continue to change, as do cybercriminals' attempts at trying to obtain and exfiltrate data.

The only factor that hasn't changed is that sensitive data is vulnerable and must be secured with data protection technologies and policies that follow corporations' sensitive data while it's in use, in transit and at rest.

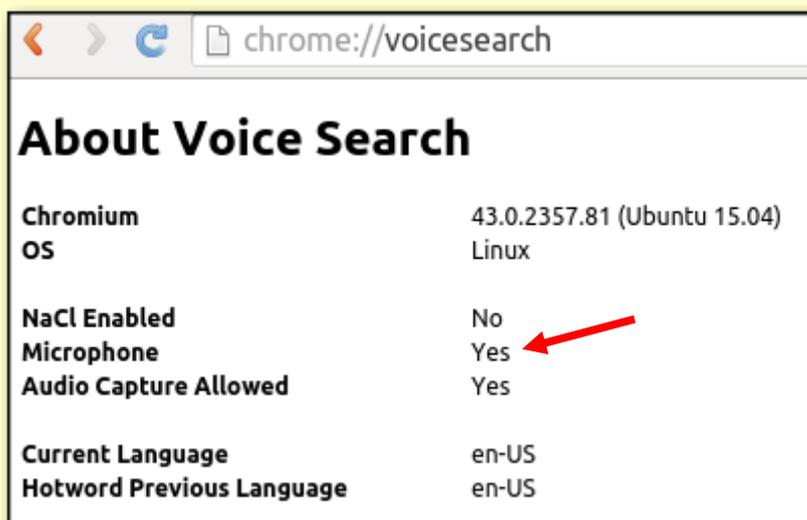
So far, organisations haven't invested in those type of protective technologies and have instead focused on perimeter-based security. As long as this methodology stands, data will continue to be at risk.



Got Chrome? Google Just Silently Downloaded This Onto Your Computer

Source: <http://wearechange.org/got-chrome-google-just-silently-downloaded-this-onto-your-computer/>

On June 17th, Google did not announce (the news broke) that the DARPA affiliated corporation has been silently downloading audio listeners onto every computer that has Chrome.



This effectively means that Google sees your privacy as piddly-squat, which does not necessarily come off as a surprise, when one considers Google's censorship of We Are Change – this very organization as nothing. The website Private Internet Access's Rick Falkvinge reported how he came to understand this new policy:

"It looked like just another bug report. "When I start Chromium, it downloads something." Followed by strange status information that notably included the lines "Microphone: Yes" and "Audio Capture Allowed: Yes".



Without consent, Google's code had downloaded a black box of code that – according to itself – had turned on the microphone and was actively listening to your room.”

Without going into detail, Falkvinge describes the nature of open-sourced/free-software and how it relies on transparency and the innovation of many software programmers before being finished as a final product. The transparency allows the user to know that the open-sourced software truly *does* what it claims to do. Chromium, the open-source version of Google Chrome is supposed to operate the same way. Only Google abused the nature of open-sourced transparency, and by-passed the process that would have prevented this from happening.

Google rationalized that enabling the ability to be eavesdropped via your personal computer was well worth it, because now “Ok, Google” works! Now when you say certain words, Chrome begins searching preliminaries – is it truly worth losing the stability of your privacy though? Obviously, it is Google's servers that respond to what is being said along with your computer. So a computer black-box was installed, hooked onto a private corporation's server and now has the ability to eavesdrop on you and Google had no intention to let anyone know about it!

Eventually Google did respond to the accusation, in which Falkvinge “paraphrased”:

“1) Yes, we're downloading and installing a wiretapping black-box to your computer. But we're not actually activating it. We did take advantage of our position as trusted upstream to stealth-insert code into open-source software that installed this black box onto millions of computers, but we would never abuse the same trust in the same way to insert code that activates the eavesdropping-blackbox we already downloaded and installed onto your computer without your consent or knowledge. You can look at the code as it looks right now to see that the code doesn't do this right now.

2) Yes, Chromium is bypassing the entire source code auditing process by downloading a pre-built black box onto people's computers. But that's not something we care about, really. We're concerned with building Google Chrome, the product from Google. As part of that, we provide the source code for others to package if they like. Anybody who uses our code for their own purpose takes responsibility for it. When this happens in a Debian installation, it is not Google Chrome's behavior, this is Debian Chromium's behavior. It's Debian's responsibility entirely.

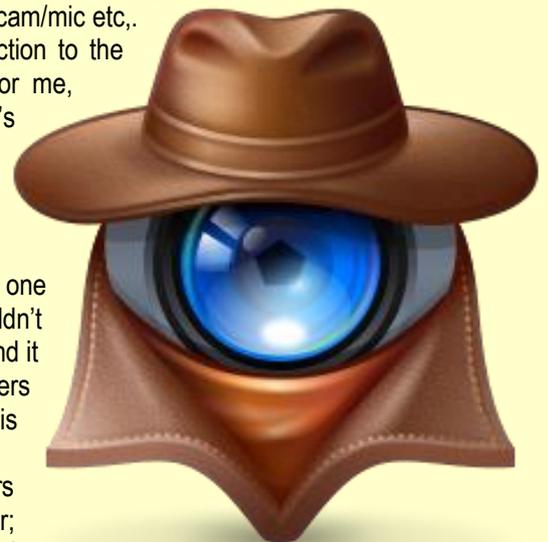
3) Yes, we deliberately hid this listening module from the users, but that's because we consider this behavior to be part of the basic Google Chrome experience. We don't want to show all modules that we install ourselves.”

The writer describes that “software switches” are no longer enough to protect against this type of eavesdropping, software switches are programs that turn off your webcam/mic etc,. Really, the author feels a physical switch that cuts electrical connection to the device is required to prevent this. It is an odd thing to observe for me, because many people were furious when news of the NSA's technological trawler of private information became common knowledge. When Google silently attempts to install even more passage ways for your intimate information to be siphoned, not much is said about it.

In fact many have begun the repetitive nature of apathetic perception, one example being “It only eavesdrops when you say, “OK, Google” (Wouldn't it need to listen to everything to *know* when you say, “OK, Google”?) and it goes on and on. Ultimately, there will always be a large portion of users who simply do not care whether or not a shadowy corporation is listening to them, or a maniacal government for that matter.

Yet in principle, the fact Google did this with the intention of users having no clue that they have had their privacy sliced even deeper; simply demonstrates the corporation's lack of compassion and

boundaries. However you choose to handle this story, deleting Chrome in exchange for more private-oriented software programs, not doing anything or learning more about it; one thing is clear: we also have a *responsibility* to ensure this type of usurpation is not treated with an accepting embrace.



Cyber security to be included in all UK computing degrees

Source: <http://www.cybersecurity-review.com/cyber-security-to-be-included-in-all-uk-computing-degrees>

New government-backed guidelines that embed cyber-security into UK computer science and IT-related degree courses come into force in September with a two-year “grace period” for universities to comply with the new teaching criteria.

The [guidelines](#) and learning outcomes, which support the government's Cyber Security Strategy, were drawn up following consultation with 30 leading British universities and government and industry bodies.

They have been co-published by (ISC)² and the Council of Professors and Heads of Computing (CPHC), with the subject now included in degree accreditation criteria from the British Computer Society (BCS) and the Chartered Institute for IT for computer science degrees. It applies to 100 UK universities which will now teach cyber-security as part of their computing degrees. The aim is to address a critical skills shortage in cyber-security by ensuring more than 20,000 computer science graduates a year study the subject.

The move directly addresses objective four of the Government's National Cyber Security Strategy: “to equip the UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber-security objectives”. Computer science graduates in the UK are currently more likely to be unemployed than graduates of any other discipline, according to data from the Higher Education Statistics Agency.

Adrian Davis, managing director for Europe, the Middle East and Asia at (ISC)², was reported in the Times Higher Education Supplement as saying that the new guidelines would help resolve the UK's “cyber-security talent shortage and a mismatch between the capabilities of computing graduates and the requirements of industry”.

Bill Mitchell, director of education at BCS, adds: “This latest initiative means that

additional guidance on cyber-security elements will be provided to complement the existing information security criteria for computing-related degrees accredited by the BCS. Building cyber-security into UK computing degree courses will go some way to resolving the skills gap situation by helping students to develop the skills that employers need.”

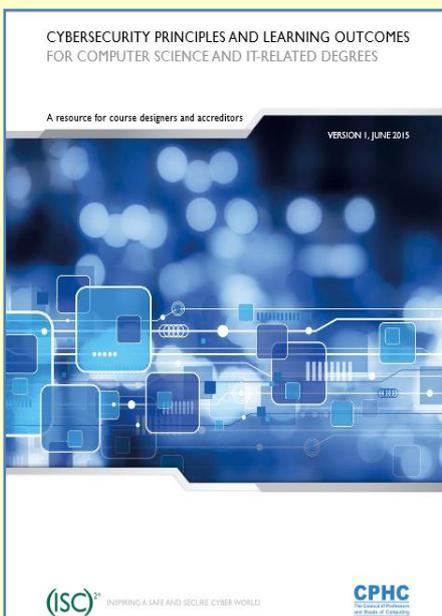
(ISC)²'s Global Information Security Workforce Survey found that 63 percent of UK public and private sector organisations have too few cyber-security workers, with one in five UK respondents admitting they would take over eight days to rectify a security breach.

Davis added: “We are now amongst the first nations in the world to ensure that cyber-security will be embedded throughout every relevant computing degree and, crucially, the most up-to-date skills will be taught as the framework is built and maintained with the input of frontline information and cyber-security professionals.”

Key elements of the courses will now include defensive programming – designing systems from the outset which are secure from vulnerabilities, threats and attacks.

On the content, Hugh Boyes, CEng, FIET, CISSP, cyber security lead at the Institution of Engineering and Technology, said, “The development of these principles and learning outcomes facilitated by (ISC)² is an important step forward in improving the software security and thus the overall cyber-security of systems. It is important that education providers address these principles and outcomes so that our future software engineers are better equipped to address the vulnerabilities that are so often prevalent in deployed software.”

Nick Savage, head of the School of Computing, University of Portsmouth agreed, saying: “The key to the cyber-security guidelines is that content will be integral to computing courses and not just a module added on. This



should be reflected in the knowledge our graduates receive. Application to operating system design will all be taught securely with cyber-security implications at the front of mind. This is an important step change in the approach to cyber-security education in the UK and we all need to be on board."

Meanwhile Dr Tony Venus, head of standards at the Tech Partnership Company, concluded with what appeared to be a widely supported view: "The employers of the Tech Partnership believe that cyber-security awareness should be an integral part of every digital degree".

Study discovers security vulnerabilities in 14 popular VPN services

By Dieter Holger

Source: <http://www.techspot.com/news/61224-study-discovers-security-vulnerabilities-14-popular-vpn-services.html>



This week, researchers from **Sapienza University of Rome** and **Queen Mary University of London** published [a study](#) detailing security vulnerabilities among 14 popular VPN service providers. While normally these services are seen as a secure way to transfer data over a public network or get onto blocked websites, some of them can actually reveal your entire browsing history. This is due to what the researchers describe as "IPv6 traffic leakage" and "DNS hijacking."

Provider	Countries	Servers	Technology	DNS	IPv6-leak	DNS hijacking
Hide My Ass	62	641	OpenVPN, PPTP	OpenDNS	Y	Y
IPVanish	51	135	OpenVPN	Private	Y	Y
Astrill	49	163	OpenVPN, L2TP, PPTP	Private	Y	N
ExpressVPN	45	71	OpenVPN, L2TP, PPTP	Google DNS, Choopa Geo DNS	Y	Y
StrongVPN	19	354	OpenVPN, PPTP	Private	Y	Y
PureVPN	18	131	OpenVPN, L2TP, PPTP	OpenDNS, Google DNS, Others	Y	Y
TorGuard	17	19	OpenVPN	Google DNS	N	Y
AirVPN	15	58	OpenVPN	Private	Y	Y
Private Internet Access	10	18	OpenVPN, L2TP, PPTP	Choopa Geo DNS	N	Y
VyprVPN	8	42	OpenVPN, L2TP, PPTP	Private (VyprDNS)	N	Y
Tunnelbear	8	8	OpenVPN	Google DNS	Y	Y
proXPN	4	20	OpenVPN, PPTP	Google DNS	Y	Y
Mullvad	4	16	OpenVPN	Private	N	Y
Hotspot Shield Elite	3	10	OpenVPN	Google DNS	Y	Y

Out of the 14 VPN services covered by the study, 10 were vulnerable to IPv6 leaks and only one was safe from DNS hijacking. None of the VPN providers were secured against both IPv6 leaks and DNS hijacking.



The issues stem from the VPN providers manipulating the IPv4 routing table but ignoring the IPv6 table.

DE GRUYTER OPEN

Proceedings on Privacy Enhancing Technologies 2015; 2015 (1):77-91

Vasile C. Perta*, Marco V. Barbera, Gareth Tyson, Hamed Haddadi¹, and Alessandro Mei²

A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients

Plus, the paper notes the VPN tunnel protocol PPTP, which is common among the VPN service providers, is particularly vulnerable.

To end the traffic leakage, the researchers suggest the providers ensure their IPv6 table captures all traffic. Additionally, a change should be made to the VPN tunnel protocol so it secures the DNS. Hopefully, the critiqued VPN providers will take notice of the research and swiftly address the security flaws.

'Hackers' give orders to German missile battery

Source: <http://www.thelocal.de/20150707/german-missiles-taken-over-by-hackers>

July 07 – **German-owned Patriot missiles stationed in Turkey were briefly taken over by hackers,** according to media reports on Tuesday.

The attack took place on anti-aircraft 'Patriot' missiles on the Syrian border. The American-made weapons had been stationed there by the Bundeswehr (German army) to protect Nato ally Turkey. According to the civil service magazine, the missile system carried out "unexplained" orders. It was not immediately clear when these orders were carried out and what they were.



The magazine speculates about two weak spots in the missile system which could be exploited by hackers.

One such weakness is the Sensor-Shooter-Interoperability (SSI) which exchanges real time information between the missile launcher and its control system.

The second exposed point is a computer chip which controls the guidance of the weapon.

Attackers might have gained access in two different ways, one that takes over the

operating of the missile system and one that steals data from it.

The patriot missile has been in service in the US army since 1984 and was first used in operation in the first Gulf war in 1991.

In 2012 Turkey asked that its NATO partners support it by stationing Patriot missile systems there, after the civil war in Syria drew closer to its southern border.

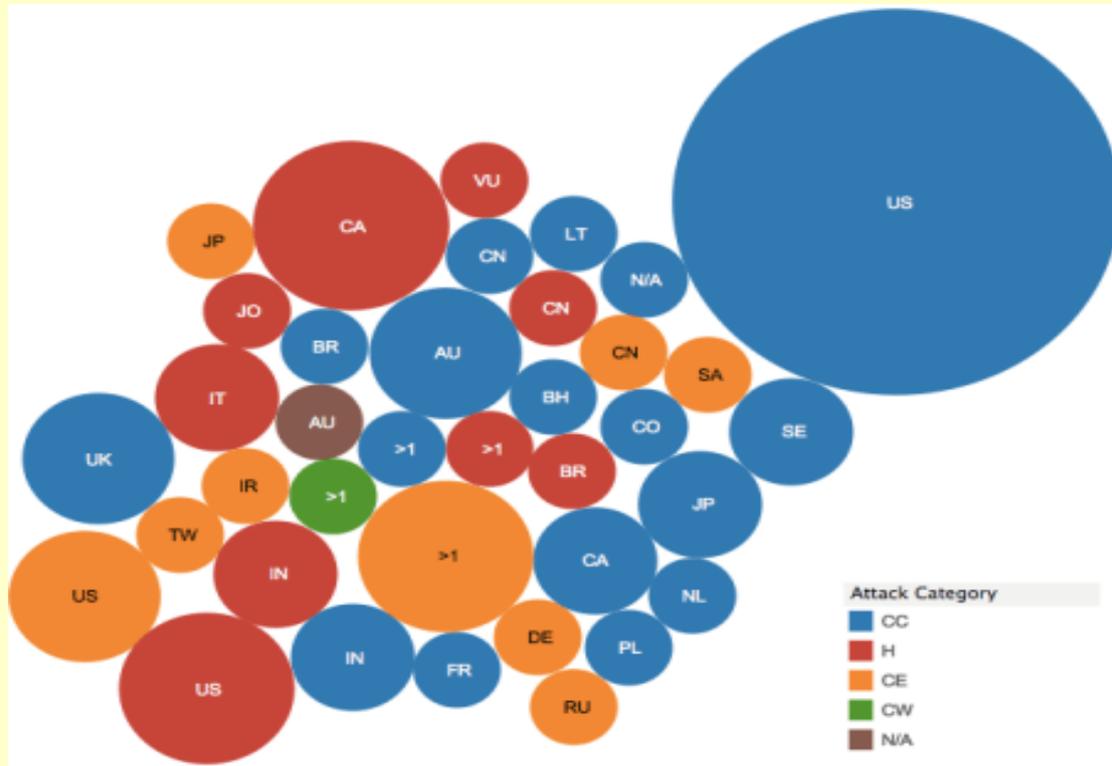
In June 2015 Germany announced that it would replace its Patriot missiles with MEADS (photo right), an air defence system designed in cooperation with the USA and Italy.



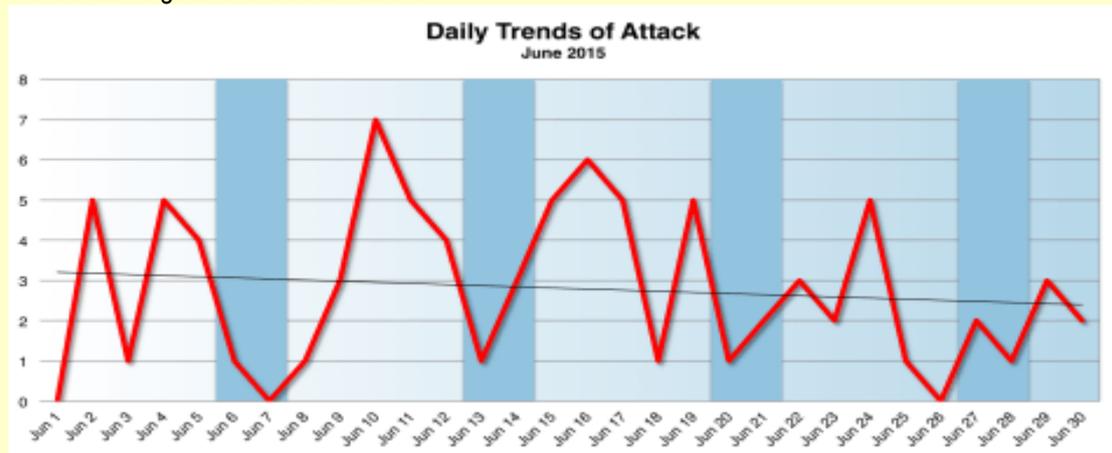
June 2015 Cyber Attacks Statistics

Source: <http://www.hackmageddon.com/2015/07/13/june-2015-cyber-attacks-statistics/>

It's time to aggregate the data collected from the Cyber Attacks Timelines of June ([part I](#) and [part II](#)) into statistics.

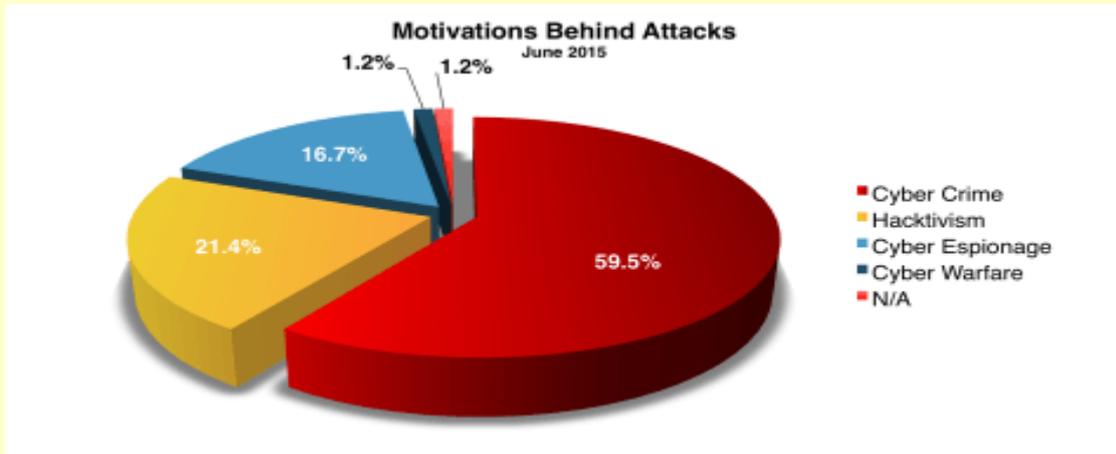


Nothing new under the July sun, for what concerns the **Country Distribution**, which is steadily dominated by the US in all sectors. Canada deserves a special mention for this month though. The country was under the digital fire of the Hacktivists and their OpC51, and this explains the red circle that makes it emerge over the other nations.

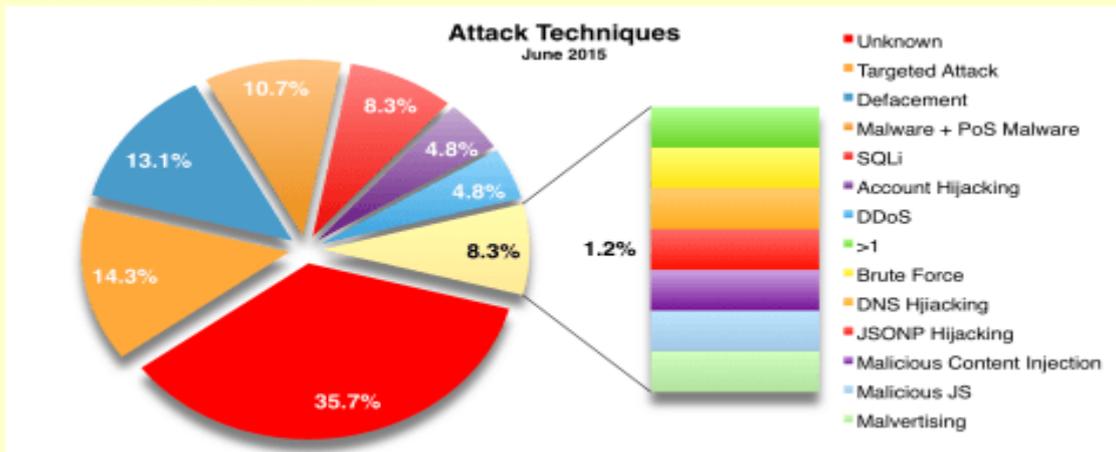


The **Daily Trend of Attacks** chart shows quite an heterogeneous shape throughout the month with a predominant peak during the second week and an apparent break towards the end.

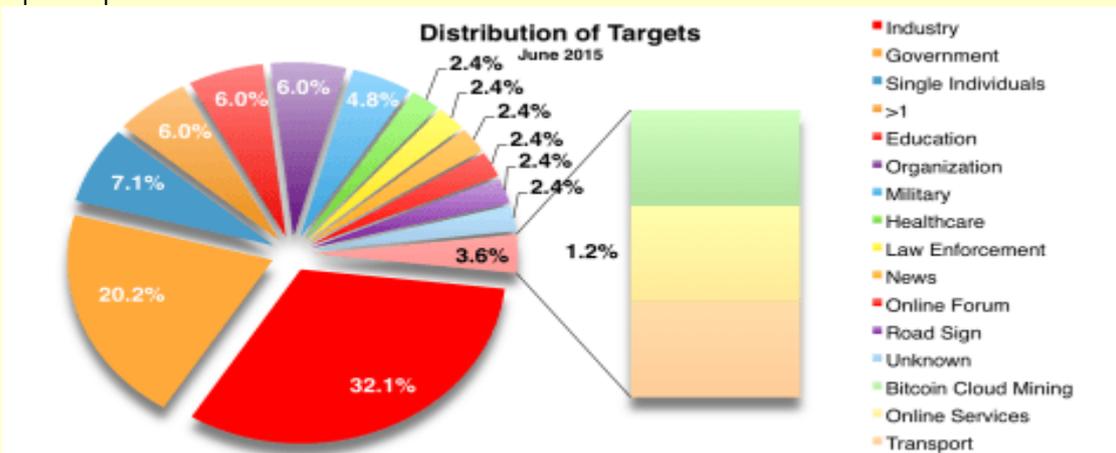




As usual, Cyber Crime ranks on top of the **Motivations Behind Attacks**, but its percentage drops to 59.5% from 68.5% of May. For what concerns hactivism, despite the actions of the Anonymous collective against Canada, the data reports a slight decrease (21.4% vs 22.5% of May). The operations motivated by Cyber Espionage rank at number three and soar to 16.7%, I do not remember to have ever recorded such a similar value.



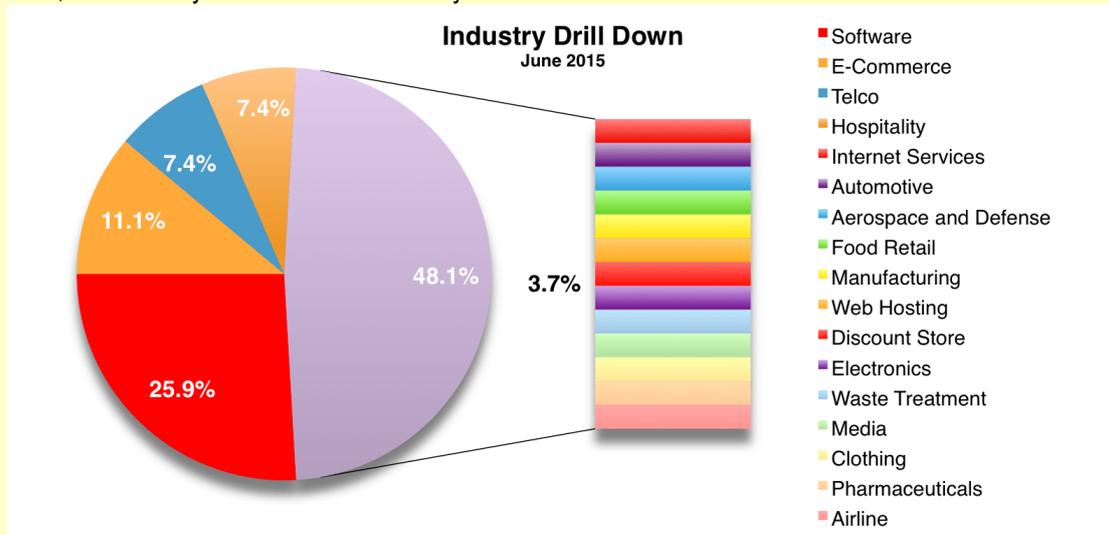
And for the first time, targeted attacks rank on top of the **Attack Techniques** chart (among the known attacks) with a stunning 14.3%. Their momentum continues and June was particularly meaningful (even a security company like Kaspersky fell victim). Defacements are substantially in line with May (13.1%), whereas malware-based attacks jump to an aggregated 10.7%. SQLi drops to 8.3% whereas DDoS reports a poor 4.8%.



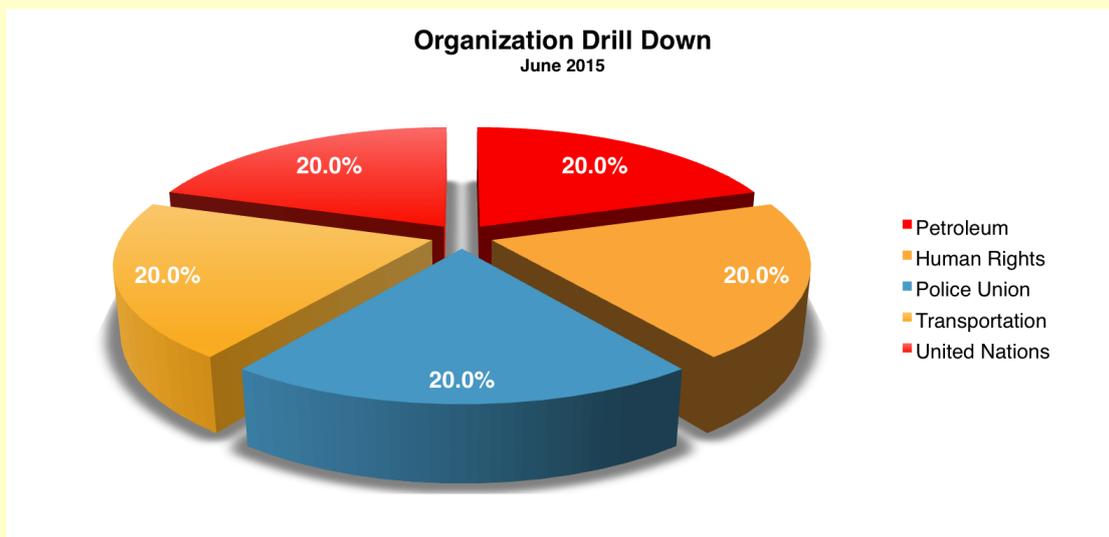
For the tenth month in a row, industry ranks on top of the **Distribution of Targets** chart with 32.1%, reporting an important increase compared to 24.7% of May. Governments rank at number two with 20.2% (exactly the same value of the previous month), while



attacks towards single individuals confirm the third place with 7.1%. Educational targets are stable at 6.0%, substantially in line with 5.6% of May.



The **Industry Drill Down** chart sees software companies on top (25.9%), whereas E-Commerce sites plummet at the second place (11.1%), just ahead of Telcos and Hospitality (7.4% both). Once again, the



Organization Drill Down chart is not particularly meaningful this month.

As usual, the sample must be taken very carefully since it refers only to discovered attacks included in my timelines, aiming to provide an high level overview of the “cyber landscape”.

Cyberjacking may be the new threat to air travel

Source: <http://www.homelandsecuritynewswire.com/dr20150714-cyberjacking-may-be-the-new-threat-to-air-travel>

July 14 – We accept lengthy queues in airport security as a small price to pay for a couple of weeks in the sun. Could the latest threat to air travel, however, be something that cannot be picked up by metal detectors and X-ray machines? Is cyberjacking — hacking into a plane’s computer systems — a possibility? Researchers warn that it is possible. There is no need to cancel that holiday just yet, however.

When Malaysia Airlines flight MH370 vanished en route to Beijing in March 2014, the horror and mystery of the story captivated the public. And as with any mystery, the lack of a definitive answer left a void for speculation and conspiracy theories. Was the aircraft shot



down? Was it hijacked and flown to an unknown location? Was the plane's computer system somehow hacked allowing it to be controlled remotely?



A City release reports that it was this latter theory that most interested David Stupples of City University of London's Department of Electrical and Electronic Engineering. Stupples is an expert in networked electronic systems and, prior to becoming an academic, spent many years developing military surveillance systems for the Royal Signals and Radar Establishment. He also designed secure communications for surveillance satellites and air defense systems for the Hughes Aircraft Corporation.

The MH370 mystery got him thinking: was it possible to "cyberjack" a civilian aircraft? If so, are we at the beginning of a new and terrifying era for commercial air travel?

To answer these questions, it is useful to look at how aircraft have evolved. In the 1970s the U.S government developed the F-117 fighter plane, the first designed around stealth technology and therefore undetectable by radar. Unfortunately, the design made the aircraft aerodynamically unstable: the only way it could be flown was if it had a computer on board.

The computer flies the plane

By the 1990s, Airbus had introduced computers on commercial aircraft and today, with the introduction of the firm's 318, 319, and 320 series, its planes are now almost totally computer controlled. As Stupples says: "The pilot flies the computer and the computer flies the plane."

Today's modern aircraft have numerous systems, including those for flight controls, automatic pilot, navigation, communication, engine management and even passenger entertainment. If these systems can be accessed by anyone with malevolent intentions, the consequences could be disastrous.

In recent years there have been numerous cyberjacking scare stories. In 2008, for example, the United States Federal Aviation Authority (FAA) reported that the computer network in Boeing's 787 Dreamliner passenger compartment was connected to the aircraft's control, navigation and communication systems. This grave security concern was subsequently resolved by Boeing.

In April this year, a security researcher was prevented from boarding a United Airlines flight after tweeting that he could hack the plane's systems. So is it possible to cyberjack a modern civilian aircraft? Stupples says yes — but there is a very large "but."

A tough nut to crack

"Cyberjacking by a passenger is going to be exceedingly difficult," he says. "He can't come through the Wi-Fi system, that's not possible.

He could perhaps interfere with the navigation but the aircraft would warn you. All the systems are totally integrated. How then could he take control of an aircraft? The only way is to get malware on board."

Malware is software designed to cause harm to a computer system, for example to disrupt it or steal sensitive information. Most of us have received suspicious-looking emails asking us to open attached files: these are often malware viruses ready to infect our PCs.

"One way to get malware on board would be for the software developers to put it on when they develop the software," he adds. Of course, this means having a rogue employee working for the software company. "For someone to develop the malware who is outside the aviation industry, that is again a difficult task because the systems are all totally integrated. The other way is to load the malware by accessing the aircraft's on-board electronics bay. This is possible but access controls are very sophisticated."

Stupples and his colleagues recently carried out research into the most likely ways that a system can become infected with malware. They calculated that the biggest threat came from a rogue or coerced employee, backed by serious organized crime or even a state.

So what can companies do to protect themselves? Can a system ever be totally safe? Stupples explains: "We've started working with Airbus and Cranfield University and what we're doing is not looking at how we can protect a system from a



cyberattack — because I think a great many of the controls are already in place and it's debatable how much more secure we can get — but looking at cybersafety, which is something quite different. "If there's malware on the system — and we're talking about any system, whether it's aircraft, trains or nuclear power stations — the system needs to recognize it's behaving in an irrational manner and then revert to a safe state."

Stupples gives the recent example of the Germanwings air tragedy, in which the co-pilot appeared deliberately to crash the plane. "The aircraft started to dive into a controlled but deep descent in an area with no landing facilities," he says. "The system [if a proposed failsafe was in place] would recognize this is an unsafe situation and the aircraft would then take itself to a stable state. We're looking at whether it's possible to take any system affected by malware to a safe state." It's still early days for this research. But in such an increasingly connected world, a security system that detects abnormalities would be highly valued, particularly when the consequences of malware could be catastrophic.

The all-seeing radar

Another threat to the aviation industry comes from drones. Widely available for just a few hundred pounds, remote-controlled aircraft have become a popular gadget. Although relatively small, when willingly or accidentally misused in public spaces they can potentially cause harm.

More ominously, they can be armed with cameras, transmitters or even explosives and

flown into controlled areas unnoticed. They could be used by terrorists for reconnaissance or flown into a descending passenger plane. There is also concern they may interfere with aircraft navigation or train controls.

Due to their size, drones often cannot be seen by conventional scanning radar, so for Stupples' latest research he's working with Cambridge-based company Aveillant to develop a new kind of radar. This collaboration has led to what Aveillant calls "the world's first 3D holographic radar system." What makes this so unique is that it's able to "look" in all directions at once, rather than be on target once every few seconds. As a result it can pick up the tiny drones.

While this advancement may be good news for the likes of Airbus, Stupples says that it could have ramifications for the world's most expensive plane: the multibillion-dollar F-35 Lightning II stealth fighter. Stupples says. "I believe this new radar will be able to see it, which makes you question whether [the F-35 is] the correct route to go down. Not only me but a lot of other people in the radar world take the view that this is not money well spent."

The U.S. and U.K. governments, who have nailed their colors to the mast of the F-35, would probably beg to differ. Regardless, Stupples' research raises an important issue. Undoubtedly, we are living in a world where increasing digitization and interconnectivity are bringing us many advantages. With those benefits, however, come new risks. The research done by Stupples and others makes it easier to understand those risks better and introduce measures that will protect us all.

Hackers take remote control of a Jeep, forcing it into a ditch

Source: <http://www.homelandsecuritynewswire.com/dr20150722-hackers-take-remote-control-of-a-jeep-forcing-it-into-a-ditch>



July 22 – Security experts have called on owners of Fiat Chrysler Automobiles vehicles to update their onboard software to make their vehicles better protected against hackers. The call comes after researchers demonstrated they could hack and take control of a Jeep over the Internet. The researchers disabled the engine and brakes and crashed it into a ditch.

Charlie Miller (left) and Chris Valasek hacking into a Jeep Cherokee from Miller's basement as I drove the SUV on a highway ten miles away. Whitney Curtis for WIRED



Cyber experts say that FCA's Uconnect Internet-enabled software has a vulnerability which allows hackers remotely to take control of the car. Cars' computerized systems have been hacked before, but

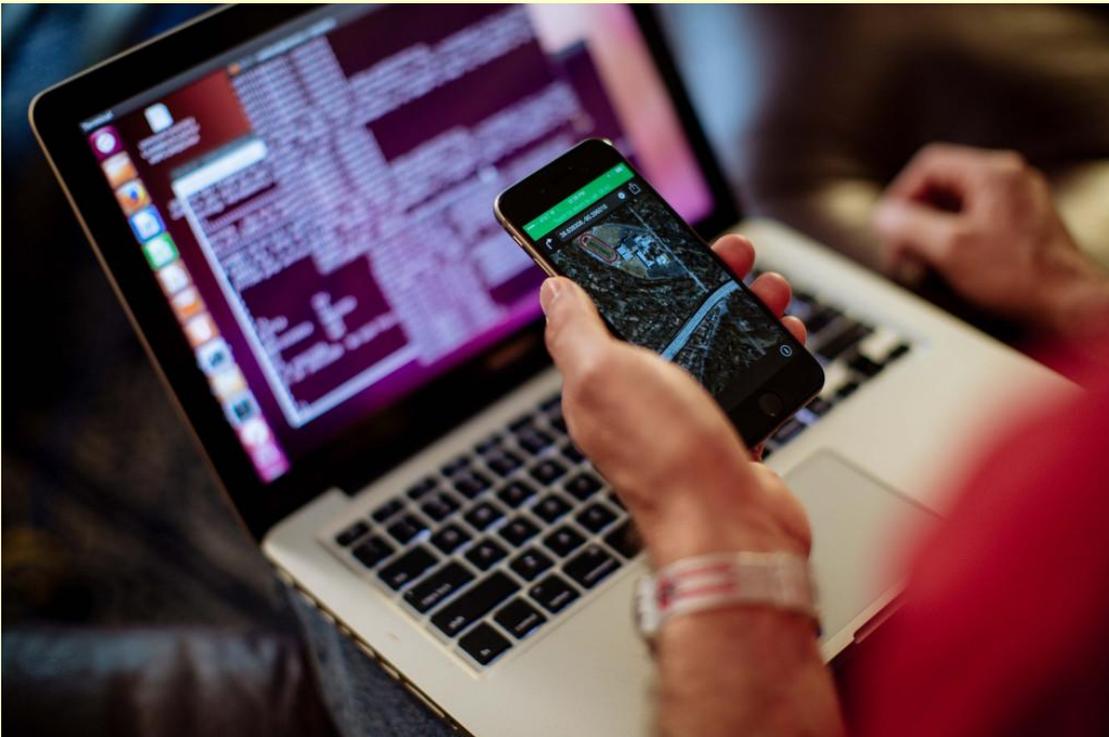


earlier demonstrations of such attacks on involved gaining control of the vehicle's entertainment system. The Uconnect hack took control over the car's driving systems — from the GPS and windscreen wipers to the steering, brakes, and engine control.

The *Guardian* reports that the Uconnect system is installed in hundreds of thousands of cars made by FCA group since late 2013. The system allows car owners remotely to start the car, unlock doors, and flash the headlights.

Andy Greenberg reported in *Wired* that security researchers Charlie Miller and Chris Valasek — who had earlier demonstrated attacks on a Toyota Prius and a Ford Escape — used a laptop and a mobile phone on the Sprint network to take control of a Greenberg's Jeep Cherokee while he was driving it. The two researchers demonstrated how they could take control of the Jeep away from the driver behind the wheel and force it into a ditch. Miller and Valasek informed FCA about the vulnerability, and on 16 July the manufacturer issues a

security patch.



Owners must update their cars manually by visiting FCA Web site to download a program onto a USB flash drive. The drive must then be inserted into the car's USB socket.

Graham Cluley, an independent security expert, added that although the researchers demonstrated the Uconnect vulnerability on a Jeep, "the attacks could be tweaked to work on any Chrysler car with a vulnerable Uconnect head unit."

"You should consider installing a security update that Jeep has issued for cars fitted with a model RA3 or model RA4 radio/navigation system," Cluley writes.



FEMA's New Data Visualization Tool Maps Where Disasters Hit

Source: <http://www.emergencymgmt.com/training/FEMA-New-Data-Visualization-Tool-Maps-Disasters.html>

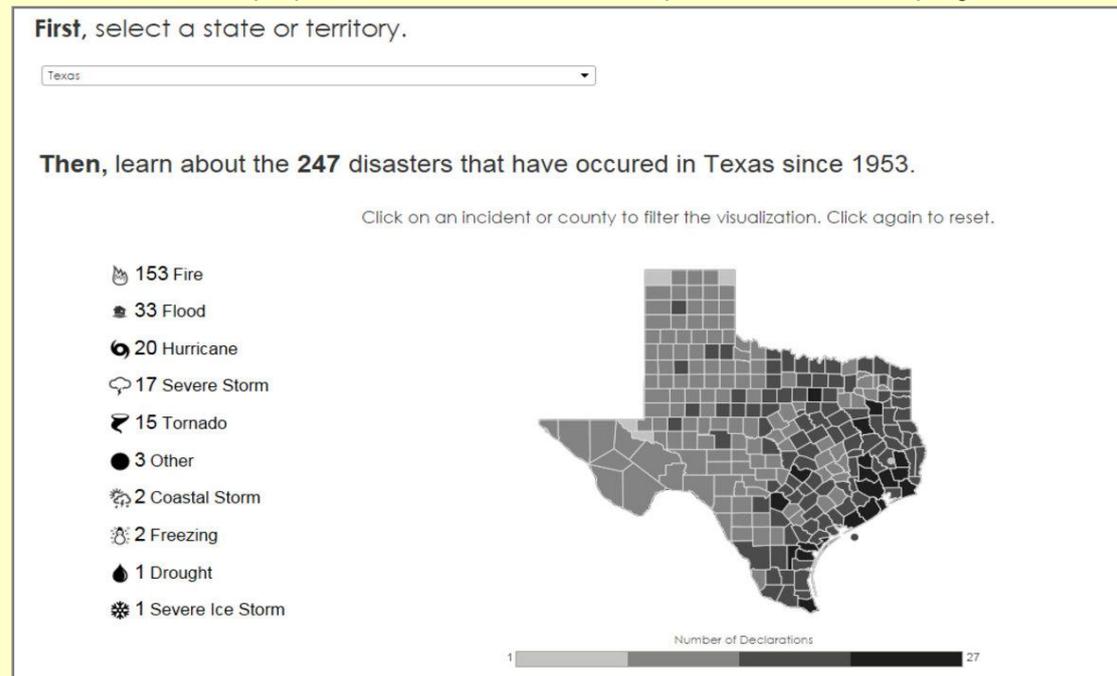
Government is learning what open data means one step at a time. And on June 11, the Federal Emergency Management Agency (FEMA) took a large step forward in its own open data efforts by releasing a new data visualization tool that allows the average person to answer questions about his or her region's history of natural and man-made disasters.

Users can filter through raw data to learn about the number of disaster declarations made — events like fires, storms, snow, typhoons and terrorist attacks — by state, county or tribal nation. The tool has graphs and charts demonstrating financial costs associated with the events, along with links to FEMA resources that encourage disaster preparation. The tool is built on data sets that FEMA had already made available, but to most people, data in an Excel

that that will make it even more accessible to a large number of people — people who may not have an affinity for looking at reams of data in Excel spreadsheets, but have an extra minute to see that data in a way that is easy to understand and convey that information to other people," Lemaitre said, adding that the tool also allows individuals to take action and learn what they can do in response to that data.

"For instance, the importance of preparing for disasters," he said. "I think one of the most striking things of this tool is you'll be hard-pressed to find any county in the United States that has not been hit by some natural or man-made disaster."

From concept to execution, the tool took about one year to create, Lemaitre said. The agency first published the tool in spring in beta form,



75

spreadsheet may as well not exist.

Rafael Lemaitre, director of public affairs for FEMA, explained that this tool's release is a piece of the OpenFEMA initiative, a commitment by the agency to educate the population about disasters through the use of data sets that don't just belong to the agency, but to everyone.

"We're taking an existing investment we've made in open data and building a tool on top of

without all of its features, before the official full release on June 11. But now that the tool is public, the agency hopes that when people see that disasters happen where they live and everywhere else, it will spur them to action.

"We sit on mountains of information here in government," he said, "and our responsibility ... is making sure that that data is accessible to



everybody. It's not our data. It's everybody's data."

FEMA's new open data visualization tool can be found on its website at fema.gov/data-visualization.

Robots on reins to be the "eyes" of firefighters in dark, smoke-filled buildings

Source: <http://www.homelandsecuritynewswire.com/dr20150623-robots-on-reins-to-be-the-eyes-of-firefighters-in-dark-smokefilled-buildings>

June 23 – Firefighters moving through smoke-filled buildings could save vital seconds and find it easier to identify objects and obstacles, thanks to revolutionary reins that enable robots to act like guide dogs.

The small mobile robot — equipped with tactile sensors — would lead the way, with the firefighter following a meter or so behind holding a rein. The robot would help the firefighter move swiftly in "blind" conditions, while vibrations sent back through the rein would provide data about the size, shape and even the stiffness of any object the robot finds.

This potentially life-saving application of robotics has been developed by King's College London and Sheffield Hallam University, with funding from the Engineering and Physical Sciences Research Council (EPSRC).

Project partners have included the charity Guide Dogs, South Yorkshire Fire & Rescue Service, and Thales Ltd. An EPSRC release reports that now proof of concept has been completed, the team plans to build a full working prototype for testing in real-world firefighting conditions.

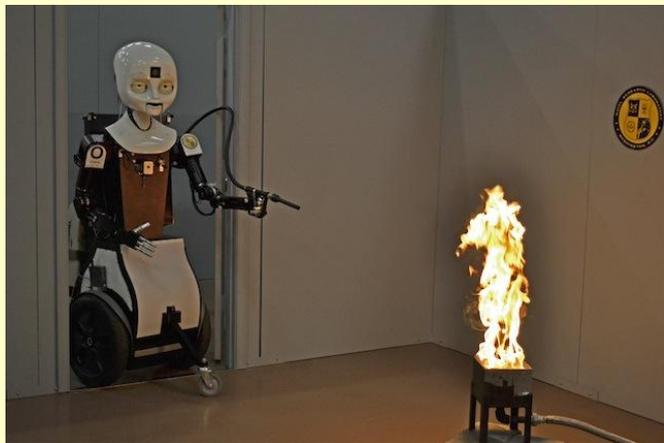
Jacques Penders, from Sheffield Hallam University, explained that the four-year project has seen the team using the tactile robot, as well as a larger Impedance Filter, in a number of scenarios from a university gym to a smoke-filled cave in Germany.

The team has developed a tactile language for using robotics in a number of domestic scenarios and now plans to explore how reins and haptic signals could help older people in their homes.

Currently, even when they have a map of the building, firefighters have to grope their way forward if smoke has badly affected visibility, feeling their way along a wall or following ropes laid by the first firefighter on the scene. But with

only twenty minutes of oxygen per firefighter, there is a real need for any innovation that can help them move more quickly and easily.

With the new system, the firefighter would wear a special sleeve covering their entire arm and incorporating electronic micro-vibrators that turn the signals sent back by the robot into



detailed data that the firefighter would have been trained to interpret.

The robot would also sense any hesitation or resistance from the firefighter and adjust its pace accordingly. In addition, it would be programmed to predict the follower's next actions, based on the way they are moving as well as on their previous actions. In trials, blind-folded volunteers were guided by a robot. By using an algorithm the robot could detect the fire-fighters level of trust.

Dr. Thrishantha Nanayakkara of King's College London says: "We've made important advances in understanding robot-human interactions and applied these to a classic life-or-death emergency scenario where literally every second counts. Robots on reins could add an invaluable extra dimension to firefighting capabilities."

Professor Penders added: "EPSRC support has enabled us to undertake a real breadth of research and given us the scope



to explore a range of approaches for human-robot interaction in no-visibility conditions that we simply couldn't have looked at with other forms of funding. The outcome has been exciting and not only could help our world-class firefighting services become even more effective in future but may also find application in healthcare, for instance."

Senior designer Heath Reed, also of Sheffield Hallam University, added: "With the use of

robots in emergency situations still in its relative infancy it is crucial to develop an understanding of how robotics interact with people and how those communications can be explored."

"This project paves the way for robotics to be developed in a number of exciting sectors and I would expect the next five years to see some real developments based on our own research."

Preparedness - A Balance Between Training & Education

By Bruce Martin

Source:http://www.domesticpreparedness.com/First_Responder/Fire_HAZMAT/Preparedness_-_A_Balance_Between_Training_%26_Education/

"Training for Certainty and Educating for Uncertainty."

Principle of the U.S. Army Command and General Staff College

Agencies within the United States spend a significant amount of resources training and educating their employees to perform specific tasks. Members of a variety of disciplines and organizations spend many hours learning. Yet, in after-action reviews (AARs), the need for training and education – and by extension learning – often is repeated. In AARs of large-scale incidents, the gaps are broad and sometimes difficult to define, for example:

The 9/11 Commission Report released in 2004 labeled one aspect of 9/11 "a failure of imagination."

- A 2006 Hurricane Katrina AAR expressed the desire not to repeat that failure as well as a notion of insufficient training.
- A 2006 *Homeland Security Affairs* article, entitled **"Lessons We Don't Learn,"** reviewed a number of large incidents and found that learning, per se, is not taught in emergency response educational institutions.

Defining the Problem

Although both training and education are critically important, public safety, public health, and emergency management agencies seem to focus more resources on training. Unfortunately, this is a challenge to the evolution and responsiveness of homeland security. Many homeland security operators begin their careers at lower organizational levels where they receive a variety of trainings. As these operators move to higher positions within agencies, they continue to apply training models when educational experience may be appropriate. Depending on the homeland security discipline in which they serve, they may or may not have acquired school-based homeland security education.

Training, by one definition, is the act of teaching a particular skill or type of behavior. Another definition, "to cause (a plant) to grow in a desired shape," is the basis for the word *instruct*, which also could mean *educate* and *teach*. **Education, in turn, is**

defined as providing intellectual, moral, and social instruction to someone else.

Robert H. Essenhigh, professor of mechanical engineering at Ohio State University, explained the difference in a 2010 article as "know how" (training) versus "know why" (education).

Training is created to solve a specific problem set or perform a specific task. The task may be complex, but it is typically definable and clear. Preston Cline of the University of Pennsylvania noted in a 14 March 2014 white paper that many mission-critical teams – for example, special operations as well as urban search and rescue – are created to solve a problem, can be quite complex, and can engage in complex training efforts.

An issue arises when the problem cannot be defined. "Wicked problems," a term coined by Horst Ritter, professor of science of design at University of California-Berkeley, are unstructured, which means that causes and effects are extremely



difficult to identify and model, thus adding complexity and uncertainty and engendering a high degree of conflict. There is little consensus on the problem or the solution. The wicked-problem space comprises multiple, overlapping, interconnected subsets of problems that cut across multiple policy domains and levels of government. Despite all the best intentions and resources, these problems may not be resolved, and efforts to solve them will have consequences for other policy arenas as well.

New Responses to New Problems

Novel circumstances – as seen in some recent homeland security incidents – may be “new” in methodology, scope, or impact. In such cases, there may be a blurred line separating training and education, but education is the foundation to solving new problems. Critical thinking has been a longtime component of education, and simplistically means being able to see more than one side of a problem, or being able to “walk in another’s shoes,” during development of policies and procedures for future incidents. Historically, there is a dichotomy between trades/skills and professions. The training of manual arts took place with a student (apprentice) under the tutelage of a master. The student completed a journey to learn the skills (journeyman), and eventually master them (master of arts). Training results in linear thinking and application of learned concepts and skills.

Some of the trades’ terminology translated into universities; in education, one must at least be a master in order to teach within a discipline. Students typically are educated first in a university setting, then move into the workforce, as opposed to the on-the-job-training approach of trades and operators. Some would argue that universities currently are producing (and industry demanding) trained individuals who can “hit the ground running,” rather than the more idealistic concept of a new team member with education and no experience. Clearly, internships and summer work placements are popular in some university programs. Nonetheless, education has been more about instilling a broad set of facts and knowledge, as well as an understanding of learning and self, in order to develop a student’s nonlinear thinking about problems.

Similarly, teams with complex missions and high-reliability demands are evolving their notion of training to include greater situational awareness and freer use of guidelines versus standard operating procedures to allow for new responses to new problems. Cline recommended to special operations teams that, among other things, access to professional educators and learning research, could give teams an advantage when dealing with emerging problems.

Professional Development – The Union of Education & Training

Homeland security is a relatively young discipline, which has grown considerably since the terrorist attacks of 9/11. A 2014 study in a doctoral dissertation by John Comiskey of St. John Fisher College suggested that the emphasis of homeland security education programs is influenced by the academic discipline in which these programs are housed. In other words, criminal justice programs look through a terrorism lens, fire and emergency management through all-hazards, etc. A brief review of homeland security curricula reveals that many rely on existing training (Federal Emergency Management Agency’s online courses) as components of their coursework.

The U.S. Fire Administration reconciles training and education with its professional development system and models. The ability to do a job is important – whereas training focuses on the road, education focuses on the horizon. Cross-walking of training and educational components lies in the realm of professional standards as presented by curricula, with industry-based hierarchies (ranks) integrated as benchmarks. Admittedly, the U.S. fire service can be considered more as a trade (training) in the process of professionalizing (education) than other homeland security disciplines such as public health. The value of the professional development model is one of presenting a simultaneously cohesive and flexible approach to training and education.

Both training and education are part of preparedness. Both require an understanding of how learning occurs, of what problems are being solved, and of the context of the students and operators. The world of preparedness requires both a pool of operators doing critical work and a pool of open-



minded professionals who will be ready to adapt to solve whatever nature or man next brings.

Bruce Martin retired in 2012 as fire chief for the City of Fremont. He now works as a project manager for the Bay Area Urban Area Security Initiative (UASI) and as an assistant professor of fire technology at the College of San Mateo. He holds a master's degree in security studies from the U.S. Naval Postgraduate School, a bachelor's degree in business from College of Notre Dame, and an associate's in fire science from Indian Valley. He is a Commission on Professional Credentialing (CPC) chief fire officer and was incident commander with others of the East Bay incident management team (Type 3).



Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them

By Amy Donahue and Robert Tuohy

Source: <https://www.hsaj.org/articles/167>

ABSTRACT: Emergency responders intervene before and during disasters to save lives and property. The uncertainty and infrequency of disasters make it hard for responders to validate that their response strategies will be effective, however. As a result, emergency response organizations use processes for identifying and disseminating lessons in hopes that they and others will be able to learn from past experience and improve future responses. But the term “lessons learned” may be a misnomer. Anecdotal evidence suggests mistakes are repeated incident after incident. It appears that while identifying lessons is relatively straightforward, true learning is much harder – lessons tend to be isolated and perishable, rather than generalized and institutionalized. That we see problems persist is a serious concern; as emergency response missions expand to include broader homeland security responsibilities, the ability to capitalize on experience is ever more important. This article reports the results of a qualitative study of both the lessons themselves and the efficacy of the processes by which responders hope to learn them.

79

Adrift - The No-Win Scenario in Responder Training

By Joseph Cahill

Source: http://www.domesticpreparedness.com/First_Responder/EMS/Adrift_-_The_No-Win_Scenario_in_Responder_Training/

In a training scenario, a lose-lose situation may make a lasting impression on students, but does little to improve the decision-making skills of the responders. Regularly faced with making life-or-death decisions, emergency responders should receive training that includes no-win as well as winnable alternatives, thus reflecting real-life scenarios while not deflating student confidence.

“Imperative! This is the Kobayashi Maru, ... nineteen periods out of Altair Six. We have struck a gravitic mine and have lost all power.... Our hull is penetrated and we have sustained many casualties.... Life support systems failing. Can you assist?”

“Star Trek II: The Wrath of Khan,” Jack B. Sowards

This message, which crackled across the radio, marked the start of the Starship Enterprise's training mission to Gamma Hydra. The scenario posed a choice: (a) save about 80 crew members of a disabled freighter and violate a treaty with a hostile



neighboring government; or (b) let the freighter drift to a certain doom, honoring the treaty but violating the commitment to save those in distress. As a plot device, such scenarios define aspects of main characters in a motion picture and set the stage for later conflict, but they also could serve as a valid training tool for first responders.

Choices Leading to Unwinnable Places

Emergency medical technicians and paramedics often face life-or-death decisions, with cardiac arrest being the most severe condition a patient can be in and still receive care from these emergency medical services (EMS). According to 2013 statistics from the American Heart Association, only 9.5 percent of people who experienced out-of-hospital cardiac arrests survived long enough to be discharged from the hospital. EMS programs often teach and test treatment skills for various patient scenarios using simulations, where the simulated patient experiences many conditions, including cardiac arrest.

In order to create an unwinnable scenario, the rules must be stacked against the student, often in an artificial manner. One such scenario is called the “two doors,” which may be used to simulate the EMS response to an active shooter situation. The two-student team would be dispatched to a shooting, and enter a scenario room with an instructor playing the role of a police officer. The sounds of gunfire come from outside, and students have the choice between two doors at either end of the room. Unbeknownst to them, an instructor/shooter with a balaclava – that is, a ski mask that covers portions of the face – awaits behind each door. Since EMS personnel have no effective response to an active-shooter situation, they rely on the police officer for safety and control of the scene. If they call for EMS resources, they simply put more EMS staff in harm’s way without improving the situation. Inherent in this scenario’s design is that the only way to win is to not play.

Instructors may support such scenarios as a way to impress upon students that there are such scenarios that they may encounter in real life. However, what all no-win scenarios need is

a winnable path. After the student arrives at the unwinnable corner, the instructor explains what the student could have done to succeed. In other words, there actually should not be any no-win scenarios, just scenarios that branch off and could lead to unwinnable places. In an EMS scenario, student teams should have the opportunity to spot the threat during scene size-up and to pull back before they become trapped in the room, or alternatively to remove the patient quickly enough that the shooter’s return does not trap them in a room with only two doors, both with dangerous consequences.

Balancing Success & Failure

These decision-making skills should continuously build on previous training and experience. Applying the training received, students should be able to succeed in the scenario, even if each team does not. Observing the success of other teams also can be valuable learning experiences. The stakes are high in EMS and the training should be difficult enough to make students think about what they are doing and understand that there are branches on the decision tree, in most encounters, that may lead to negative consequences.

Training should offer students the tools to make good decisions and understand the necessary procedures intended to keep them safe and make them successful. A no-win branch should only be included in a scenario when three criteria are met: (a) the branch is realistic to conditions in the field; (b) the stakes in a similar real-life scenario are high; and (c) the students’ training would lead them to another path, but they just did not take it. Care must be taken not to paint an outlook that is too positive, but not so negative as to crush the confidence of the students.

Joseph Cahill is the director of medicolegal investigations for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Before that, he was the department’s Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College’s paramedic program and has been a frequent guest lecturer



for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Technology for Disaster Management

By Brandon Greenberg

Source: <http://www.disasternet.co/disastertechnology>

There are many different technologies available for use in disasters. This page highlights the different technologies and categorizes them by type.



The SlideShare below was originally created in response to a number of presentation requests I have had. I will continue to add new technologies as I come across them!

Brandon Greenberg: Research/work btw Policy, Mgmt & Tech 4 Disaster | PhD student @GWEngineering | MPA from @NYUWagner



Operation Twister - Exercising Disaster Behavioral Response

By Craig DeAtley

Source: http://www.domesticpreparedness.com/Training/Exercises/Operation_Twister_-_Exercising_Disaster_Behavioral_Response/

Functional exercises are invaluable for helping participants understand their roles in disasters. This is particularly true for participants who normally are not included in interagency exercises, such as behavioral health personnel. **Triaging following a disaster should not stop at the physical level, but should consider psychological concerns as well.**

Every disaster to one degree or another involves behavioral health issues affecting the public and the response communities. Disaster behavioral health responders typically work in concert with healthcare providers, public health, emergency management, first responders, and volunteer organizations. Although disaster behavioral health is gaining recognition as an integral part of the overall public health and medical preparedness, response, and recovery systems, disaster preparedness exercises often fail to integrate a behavioral health response. Personnel responsible for providing behavioral health assistance and the healthcare facilities both benefit from opportunities to clarify their roles and rehearse their responses to effectively address the full needs of patient populations in disasters.

Recently, a functional exercise was held in the District of Columbia that provided a focused opportunity for the D.C. Department of Behavioral Health to respond to a severe bad-



weather incident and practice its response plan. The plan included the use of **Psychological Simple Triage and Rapid Treatment (PsySTART)** for victim screening and integration with hospitals requesting their assistance in assessing the immediate and long-term behavioral needs of the injured patients and their families. As a result of the exercise, some valuable lessons were learned.

PsySTART™ Disaster Mental Health Triage System

LAST NAME		FIRST NAME		MEDICAL RECORD NUMBER	
AGE	GENDER MALE FEMALE		HOME ZIP CODE		

		INDICATE "YES" ANSWERS BELOW
EXPRESSED THOUGHT OR INTENT TO HARM SELF/OTHERS?	<input type="checkbox"/>	
FELT OR EXPRESSED EXTREME PANIC?	<input type="checkbox"/>	
FELT DIRECT THREAT TO LIFE OF SELF OR FAMILY MEMBER?	<input type="checkbox"/>	
SAW / HEARD DEATH OR SERIOUS INJURY OF OTHER?	<input type="checkbox"/>	
MULTIPLE DEATHS OF FAMILY, FRIENDS OR PEERS?	<input type="checkbox"/>	
DEATH OF IMMEDIATE FAMILY MEMBER?	<input type="checkbox"/>	
DEATH OF FRIEND OR PEER?	<input type="checkbox"/>	
DEATH OF PET?	<input type="checkbox"/>	
SIGNIFICANT DISASTER RELATED ILLNESS OR PHYSICAL INJURY OF SELF OR FAMILY MEMBER?	<input type="checkbox"/>	
TRAPPED OR DELAYED EVACUATION?	<input type="checkbox"/>	
HOME NOT LIVABLE DUE TO DISASTER?	<input type="checkbox"/>	
FAMILY MEMBER CURRENTLY MISSING OR UNACCOUNTED FOR?	<input type="checkbox"/>	
CHILD CURRENTLY SEPARATED FROM ALL CARETAKERS?	<input type="checkbox"/>	
FAMILY MEMBERS SEPARATED AND UNAWARE OF THEIR LOCATION/STATUS DURING DISASTER?	<input type="checkbox"/>	
PRIOR HISTORY OF MENTAL HEALTH CARE?	<input type="checkbox"/>	
CONFIRMED EXPOSURE/CONTAMINATION TO AGENT?	<input type="checkbox"/>	
DE-CONTAMINATED?	<input type="checkbox"/>	
RECEIVED MEDICAL TREATMENT FOR EXPOSURE/CONTAMINATION?	<input type="checkbox"/>	
HEALTH CONCERNS TIED TO EXPOSURE?	<input type="checkbox"/>	
NO TRIAGE FACTORS IDENTIFIED?	<input type="checkbox"/>	

©2007-2014 K.W. Schmitz





Original - Patient Chart

Funded through 1HHS HFP grant #01 U0REPS00370
For use with the PsySTART Incident Management System

hitting the District of Columbia with torrential rain, damaging winds, and eventually a tornado. Numerous incidents occurred, which caused mass casualties involving adults and pediatric patients. Some patients had critical trauma including burns; whereas others were severely emotionally traumatized from the resulting dangers, utility outages, and general disruption to their normal lifestyles.

Several hospitals requested assistance from the D.C. Department of Behavioral Health to manage the immediate and possible long-term behavioral health problems of their patients. The department deployed three members of the Behavioral Health Emergency Response Team to work with the Psychiatry Department staff at a large trauma center hospital that received nearly 100 moulaged victims. The request was made by phone as well as on the coalition's intranet-based system for information sharing.

The team arrived at the hospital within an hour after the request was received. Once at the hospital, they reported per instructions to the Hospital Command Center, where they were briefed and redirected to the Emergency Department to support the work of the staff from the hospital's Psychiatry Department. Together, the two teams triaged 29 of the victims with the PsySTART tool. The nonintrusive format took less than 10 minutes to administer and manually record the triage

Operation Twister

The three-hour exercise, named "Operation Twister," was sponsored by the D.C. Emergency Healthcare Coalition. Dr. Kevin O'Brien, director of Disaster Behavioral Health Services for the D.C. Department of Behavioral Health, was part of the exercise planning team. The scenario involved severe bad weather

scores.

PsySTART

PsySTART is a strategy for rapid mental health triage during a large-scale incident. This evidence-based concept was originally created by Dr. Merritt



Schreiber at the Center for Disaster Medical Services at the University of California Irvine School of Medicine, and is used in numerous communities in the United States including hospitals and the D.C. Department of Behavioral Health. The U.S. Department of Health and Human Services' Hospital Preparedness Program grant money was used in 2012 to provide initial training in the District of Columbia to hospitals, fire, and emergency medical services, and D.C. Department of Behavioral Health staff members.

Periodic refreshers and new training have been conducted annually since then. The triage tool can be used for assessing both adult and pediatric patients. Patient answers can be written on the questionnaire or entered into a computer database for analysis. The questionnaire's primary purpose is providing situational awareness of at-risk individuals, and it uses a "floating triage algorithm" that prioritizes those who need to be seen first from those who can be referred for assessment after the initial surge is over.

Exercise Lessons Learned

The exercise was an excellent overall learning experience according to O'Brien, who served as an exercise controller/evaluator. "It gave our department a chance to rigorously exercise our emergency response plan in coordination with other members of the healthcare community. We don't get a chance to do that very often." The value of having a redundant approach for making a request for assistance was reinforced because, for some of the facilities, their phone lines were not functioning and use of the coalition's intranet-based Healthcare Information System (HIS) was the only way they could make the request for help.

The exercise provided the D.C. Department of Behavioral Health a chance to rehearse

deploying their personnel to a hospital, while taking into account the bad weather and potentially dangerous road conditions. O'Brien pointed out in his hot wash remarks that, "Having our staff actually integrate into a hospital operation during a crisis was new for us, and proved invaluable so we could learn how to support and not interfere."

The exercise also brought to light the importance of having multiple personnel – whether in the Department of Behavioral Health or at a hospital – being familiar with and adept at using the PsySTART tool itself. Although both responders and the hospital had trained personnel using PsySTART, just-in-time refresher training was needed for some of the users to quickly become comfortable using it.

Interestingly, the analysis of the answers these "make believe" disaster victims gave indicated that all of the patients evaluated would require follow-up care – something that otherwise might not have been recognized so quickly. Knowing these results allowed both the hospital and O'Brien's colleagues to better devise long-term discharge plans for these patients. Plans also were discussed but not implemented for administering the questionnaire to hospital staff and using the results to determine staffs support needs. However, exercise time limitations precluded such plans from actually being implemented.

Operation Twister was an exercise that had the usual focus on emergency medical services and hospital performance of patient triage and treatment. However, this exercise also provided a much-needed opportunity for key members of the city's healthcare system to evaluate their ability to address the behavioral health concerns rather than simply the physical needs of victims and responders to severe weather or any other emergency.

Craig DeAtley, PA-C, is director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region's largest hospital; he also is the emergency manager for the National Rehabilitation Hospital, administrator for the District of Columbia Emergency Health Care Coalition, and co-executive director of the Center for HICS (Hospital Incident Command System) Education and Training. He previously served, for 28 years, as an associate professor of emergency medicine at The George Washington University, and now works as an emergency department physician assistant for Best Practices, a large physician group that staffs emergency departments in Northern Virginia. In addition, he has been both a volunteer paramedic with the Fairfax County (Va.) Fire and Rescue Department and a member of the department's Urban Search and Rescue Team. He also has served,



since 1991, as the assistant medical director for the Fairfax County Police Department.

When the phones went dead: 7/7 showed how disasters call for tomorrow's tech

By Nigel Linge

Source: <http://www.homelandsecuritynewswire.com/dr20150709-when-the-phones-went-dead-7-7-showed-how-disasters-call-for-tomorrow-s-tech>

July 09 – **One aspect of the London bombings of 7 July 2005 that many who were there remember is that their phones went dead.** Mobile phone coverage in parts of central London was almost unavailable. This was not due to damage; the emergency services had shut down public access to the networks.

At times of crisis communications are essential. The emergency services need to coordinate their response while the general public wants to contact loved ones and find out what's happening. The problem is that there simply isn't enough capacity for everyone to use the networks simultaneously, particularly in densely populated areas like central London. Networks of all types are designed to cope with typical traffic demands, and so in exceptional circumstances they become massively

can be set to operate within defined geographic areas.

SIM, the key to the network

All mobile phones contain a Subscriber Identity Module, universally known as a SIM card, which stores network-specific information that authenticates and identifies subscribers on their network. Each SIM is also assigned to a privilege access class, which is a code number between 0-14. For general users this will be in the range 0-9, while emergency services responders are assigned classes 12-14.

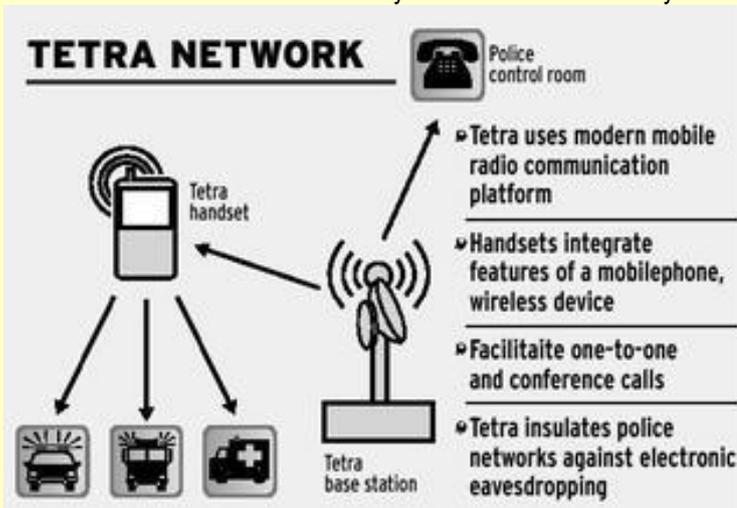
When connected to a mobile network via a nearby base station, the details in the SIM card are transmitted over the network. During an emergency when MTPAS has been invoked, the privilege access class is checked and the network will drop attempts to connect from non-emergency class SIMs.

So while the network is certainly still up and running, it will seem unobtainable until the phone moves further from the MTPAS-controlled area where a connection can be re-established. Emergency 999 calls are unaffected. This way the mobile network cells in the area are free for use by the emergency services.

Packing TETRA

On 7 July 2005, police requested O2 to invoke MTPAS (or rather its predecessor, Access Overload Control or ACCOLC) within one square kilometer of the Aldgate Tube Station for a period of four hours. Unfortunately this was only partially successful because not all emergency service personnel at the time had MTPAS-equipped mobiles, which meant their calls were blocked too. Following an inquiry after the event, that problem has been addressed.

In addition to using a mobile network, since 2005 the



overloaded. Operators need to prioritize access. At such times, the emergency services invoke the government's Mobile Telecommunication Privileged Access Scheme (MTPAS) procedure. This is where the police "Gold" commander — the senior officer managing a disaster or emergency event — can notify mobile network operators that they should start prioritizing calls and messaging from the emergency services over others. This



emergency services have had their own dedicated digital communications network called TETRA (TErrestrial TRunked RAdio). But TETRA has not been without its problems — and now the government is planning to replace it on the grounds of cost and its limited capability for transmitting data.

Today’s emergency services want to make better use of video and exploit the potential of real-time mapping applications — both of which demand a network with a greater data-handling capacity.

The future is 4G (until 5G comes along)

The natural place to find this capacity is the 4G mobile network that is now being rolled out around the world. But this will require new services to be designed and built for emergency services use. For example, the

walkie-talkie style push-to-talk feature offered by TETRA for police officers, firefighters or paramedics who don’t want to be scrolling through menus and contact lists — they need to be able to quickly just push and talk to colleagues.

The demand for this sort of feature has been sufficient that the next release of the international 4G network standards now incorporate this feature as part of an effort to support mission-critical and public safety use.

Of course, moving all emergency services’ communications to the mobile network won’t mean they start monopolizing the network over the general user. Emergency service use will need to be partitioned and managed separately from that of the general public — and for those emergency situations, MTPAS will still be available to fall back on.

Nigel Linge is Professor, Computer Networking and Telecommunications at [University of Salford](http://www.universityofsalford.ac.uk).

Superheroes in Waiting: Emergent First Responders

By Wayne P. Bergeron

Source:http://www.domesticpreparedness.com/Government/DoD/Superheroes_in_Waiting%3a_Emergent_First_Responders/

Although they may not want to be called “heroes,” military members and veterans can fill a critical gap in emergency and disaster response. Their unique qualities of training, discipline, leadership, and teamwork make them the perfect emergent responder either as a member of an organized team, or simply by being in the right place at the right time.

It is not a normal everyday occurrence for U.S. Army Captain Steve Voglezon to rescue people from a burning car and pull multiple people to safety. Even more unlikely, is that he would be wearing a Captain America T-shirt while doing it. However, that is the nature of the military or veteran emergent first responder, someone who is in the right place at the right time with both the will and the courage to act. Simply on his way to the mall, the soldier from Fort Bragg, North Carolina, found himself in May 2015 thrust into the role of first responder as he pulled two people to safety from a vehicle collision with one of the vehicles fully engulfed in flames. When asked about the courage and bravery of his actions, the young captain simply said, “I really didn’t have time to think or be

scared, just time to react – I saw people who needed help and I guess the Army programming just kicked in.” Luckily, for the two victims, it did.

A list of the qualities for the perfect emergent first responder likely would include the following:

- Able to operate in complex, confusing, and quickly changing situations;
- Able to endure hardship;
- Thrives in austere environments;
- Mission focused and able to operate with minimum guidance;
- Comfortable with leadership;
- Confident;
- Physically fit;
- Able to inspire loyalty;
- A team player; and
- Passionate about volunteerism and serving others.

It is no surprise that these qualities also are some of the perfect descriptions for the modern generation of military members and veterans. These qualities and a number of other factors make the military



member or veteran the perfect emergent first responder in times of crisis. Many military veterans become formal first responders, with a tendency to gravitate toward professions within the law enforcement, fire, emergency medical services, and emergency management communities when they leave the service. However, many others return to their communities to open small businesses, or to become managers, foremen, bankers, electricians, etc. Some return to the university to complete their education, and many others settle into the community and start families, join faith communities, coach youth sports, and do all the activities that young adults are expected to do.

However, for many veterans, they sometimes feel that something is missing – a sense of duty or a sense of service. It might just be a fleeting thought at times, but it is present. That might very well be the end of the story, but local emergency managers or newly designated crisis incident commanders should take stock and consider the talents and capabilities of military members and veterans. These valuable resources could serve either as part of a designated reserve manpower pool or simply as an emergent first responder during times of an emergency. In any case, it is a wise choice in terms of the latter and a great strategic investment in terms of the former.

The Unique Qualities of Military Personnel and Veterans

There are key areas of emphasis for emergency management and response that make military personnel and veterans a perfect fit for most emergency management and responder organizations. Three basic categories are: (a) training and discipline; (b) leadership and teamwork; and (c) tested and proven experience.

Training and discipline: From the first day of initial entry training (boot camp), all branches of the military instill a unique sense of self-discipline in each member. This then contributes to an overall sense of teamwork and group identity that allows a bunch of strangers to become a functioning, organizational unit with a group identity and shared sense of purpose in a very short period of time. Military members and veterans never forget that experience and are able to repeat it even many years after leaving the service. The military also teaches practical skills such as

physical agility, problem solving, survival skills, navigation, first aid, etc. All of these teachings and many more are the recipe of skills that most first responder organizations need as well. Veterans also value structure and the chain of command, so they intuitively understand the Incident Command System (ICS).

Leadership and teamwork: It is no secret that the military operates as a unit or a team at all levels. Even the smallest special operations unit or the fighter pilot has a team of talented and dedicated individuals that they rely on to help them perform their tasks and, in so doing, they all contribute to the overall mission. In addition to teamwork, one of the greatest strengths of the U.S. military is the ability of all of its members – from the most junior private, seaman, or airman to the most senior general or admiral – to step into a leadership role when necessary and appropriate. For an emergency manager or incident commander, this skill can be critical in knowing that a particular individual is up to the task of leadership at a critical point in a crisis.

Tested and proven experience: One of the biggest unknowns within the emergency response community is exactly how a person – particularly one who is not a formal responder – will respond when faced with his or her first real crisis situation. Regardless of the amount of training or number of exercises, the “real thing” always seems to add an increased level of anxiety and stress. For the most part, military members and veterans in the current generation have served at least one deployment or combat tour with many having served three or more in a normal tour, service, or career. That kind of experience proves invaluable in an emerging crisis situation.

Leveraging Military Members & Veterans

There is no single best method to leverage military members and veterans within the emergency management community, but there are options. One option is to create an emergency response organization fully staffed by veterans, which is exactly what the organization known as Team Rubicon did in the wake of the 7.0 magnitude earthquake that hit the island nation of Haiti in 2010. Two Marines (there are no “former” Marines) together with six other veterans gathered funds and medical supplies from friends



and family and flew into the Dominican Republic, where they rented a truck, loaded their gear, headed west to Haiti, and began helping the response efforts. They have not looked back since and have created a dynamic organization of self-deploying veterans, which continues to deploy both domestically and internationally when disaster strikes – most recently in Texas helping with flood relief.

However, not every community can have a Team Rubicon, or even be members of the organization because of day jobs, families, responsibilities, and an inability to pick up and deploy for a few weeks or more at a time. There are several ways that military members and veterans can help their communities, and

that local organizations can capitalize on the skills and abilities of these community members.

The first and perhaps most productive way is to become a member of a local Community Emergency Response Team (CERT). Veterans would be instantly familiar and comfortable with the squad-like paramilitary structure of the organization. If a community does not have a CERT, it is relatively easy to start one. Other options to leverage veterans include recruiting them for: volunteer fire departments, rescue squads, search and rescue teams, and similar response teams. *The bottom line:* The possibilities are endless after tapping into this great reservoir of talent (capes are optional)!

Wayne P. Bergeron, lieutenant colonel, retired from the United States Army in May 2011 after a 23-year career within the Military Police Corps and Special Operations Forces. He currently serves as an instructor teaching both criminal justice and security and emergency management at the University of North Alabama in Florence, Alabama. His education includes undergraduate degrees in criminal justice and political science, a master's degree in international relations from Troy University, and he is currently a doctoral candidate in emergency management at Jacksonville State University.

Response Management: Back to Basics

By Stephen Grainer

Source:http://www.domesticpreparedness.com/Industry/Standards/Response_Management%3a_Back_to_Basics/

When a seemingly unrealistic incident occurs, emergency managers must be equipped with the base knowledge necessary to respond to the previously unknown scenario. Acronyms are a good way to remember what to do when stress levels are high and time is short. By getting back to the basics, managers are better equipped to respond and to protect their communities.

Emergency managers and responders across the United States confront a wide array of hazards and emergency situations daily. Whether responding to and managing floods, droughts, tornadoes, hurricanes, terrorist attacks, or any other natural or human-caused threat, effective operations begin with preparedness.

A Worst-Case Scenario

Preparedness efforts typically focus on the principle of planning for the worst, and hoping for the best. As such, planning, training, exercising, and evaluating preparedness frequently begin with the premise of identifying the worst situations imaginable and developing response protocols accordingly. Although this may enable the emergency responder community to broadly take an all-hazards approach to planning and preparedness, it also may create a lengthy menu of procedural guidelines that can overwhelm emergency or incident managers. During times of high stress and urgent need, the emergency or incident

manager may become so stressed that identifying the starting point for establishing management functions is the first challenge.

As is often said, managing major incidents is a good news-bad news situation. The relatively infrequent incidence of catastrophic emergencies is the good news. Major incidents with potentially horrific consequences and threat to life are relatively rare. Correspondingly, that same rarity also is a primary cause for concern for emergency managers and incident commanders. The opportunities to apply acquired knowledge, skills, or abilities



associated with major incident management for most personnel are very limited. In order to offset the limited experience in actual major incident response management, many preparedness efforts involve conducting exercises with scenarios that are close to unimaginable and incomprehensible – perhaps even unrealistic.

Additionally, in the efforts to support the “all-hazards” concept associated with the National Incident Management System (NIMS), preparedness efforts – specifically exercises – sometimes incorporate an array of different threats and hazards concurrently. This can lead to a descending cycle of efforts to develop and conduct more complex and detailed scenarios for each successive exercise. If this progression continues, emergency preparedness and planning efforts result in more detailed and complex plans and protocols.

The net effect can be that both emergency managers and incident commanders may

the magnitude or uniqueness of a threatening situation.

The **“P” in P-O-S-T represents “priorities.”**

One unchanging element in every incident is the fact that there are three common core priorities. From an “all-hazards” perspective, the priorities are constants and may be the only elements that do not change regardless of threats, hazards, vulnerabilities, or risks. These priorities can be listed by another acronym – L-I-P, which stands for: (a) Life safety; (b) Incident stabilization; and (c) Property conservation (or Preservation). The order in which they are listed also represents the relative order in which these priorities should be addressed when defining the parameters of any emergency. It is from these three core priorities that all further decisions and actions can be programmed.

Priorities also may be stated using different or more detailed (subordinate), verbiage. For example, an incident commander states that the “*first* priority is to reopen the highway.” Although this is a legitimate statement, it may be driven by the recognition that opening the highway is critical to implementing life-saving operations (priority number 1). Alternately, if there are no immediate life-safety threats, reopening the highway would facilitate stabilizing the incident situation sooner (core priority number 2). Or finally, reopening the highway may limit continuing damage to property. In any case, the original statement to “reopen the highway” captures the intent of one of the three core priorities or perhaps all three.

The **“O” in P-O-S-T represents “objectives.”**

Once the situational demands of the incident can be defined within any or all of the core priorities, incident managers can identify operational objectives to confront the threat(s) and conform to these priorities. Objectives are broad statements of intent or desired outcomes relative to the priorities and actions anticipated. The **“S” in P-O-S-T represents “strategy”** (or strategies). Based on the objectives established, incident managers typically then assess several alternative strategies for action to meet the objectives and select the one or two strategies deemed best under the circumstances. There may be cases in which two (or more) compatible strategies may be adopted. The important decision relative to adopting strategies is to remember that if multiple

K.I.S.S.
Keep it Short and Simple

become overloaded with situational details that can cause “decisional paralysis” or information overload. Sometimes characterized as “brain drain,” such overload causes a person to become unable to think through an orderly sequence of decisions in a timely manner. If this occurs, it may be best to remember another old adage, “Keep it simple, son” (or KISS).

From Priorities to Preservation

One fundamental – or back-to-basics – tenet of the Incident Command System (ICS) is to employ an orderly methodology by which emergency managers and incident commanders organize and focus response efforts to address threats and hazards of any type or magnitude, indeed all hazards. This principle is captured with the acronym **P-O-S-T** and has been presented in various ICS training programs for many years. Often the “P” is overlooked or minimized because it is a consistently recurring step, but it can help begin the initial thought process regardless of



strategies are considered, they must not be counterproductive and cannot “neutralize” each other.

Finally, the **“T” in P-O-S-T represents “tactics” or “tasks.”** These are the functional actions undertaken to disrupt, deter, or redirect the event(s) to achieve a more favorable outcome. As with strategies, several alternative tactical options often are assessed. Selection of tactics most commonly are dependent on the immediacy (or urgency) of the threat; readily available resources; time necessary to acquire resources not on hand; and functional constraints to perform the actions under consideration.

Putting P-O-S-T into Action

One example of using the P-O-S-T process might be as follows:

A tornado touches down suddenly in a suburban locality wreaking havoc on an area of residential occupancies 200 yards wide by half a mile long. Fortunately, National Weather Service warnings provide sufficient time for most residents to take protective measures; however, structural damage is extensive.

All three *priorities* come into play. Life safety for citizens and responders are the preeminent priority. With that, incident stabilization (priority 2) and property conservation (priority 3) also steer initial decision-making.

The objectives may be stated as follows:

1. Identify and provide emergency medical care for any injured citizens in the impacted area within ___ hours. (Priority 1)
2. Ensure all emergency response personnel conduct operations in the safest and most expedient manner possible using appropriate personal protective clothing and equipment. (Priority 1)
3. Map and cordon/secure the impact area from unauthorized incursion within ___ hours. (Priority 2)
4. Survey for any externally visible structural damage, especially for residential occupancies, within ___ hours. (Priority 3)

Strategies may include:

1. Organize search teams of trained/qualified response personnel and conduct surveys and searches for any victims. Remove any readily extricable victims, provide triage and treatment, remove to safety, and report any

- victims needing technical rescue assistance and/or life support.
2. Establish technical rescue crews prepared, equipped, and capable of conducting technical rescue activities.
3. Establish emergency medical services (EMS) operations in a safe location to provide care for victims or any injured personnel.
4. Establish traffic control points at all roads providing access to the affected area and prohibit entry for all by authorized personnel.
5. Contact local power and other utilities and cut off all services within the impacted area pending determination of safety for restoration on a case-by-case basis.
6. Obtain local tax maps or other records to support assessment operations.

Tactics may include:

1. Conduct aerial (preferably rotary wing) overflight of the impacted area (conditions permitting), noting visible victims and report same to command. If possible provide live-stream video to command or other downlink location.
2. Establish 10 three- to five-person teams of fire/EMS personnel who, wearing appropriate personal protective equipment and having appropriate hand tools, conduct house-to-house “walk-around” surveys on a street-by-street basis to locate any victims. Assess victims for injuries, provide preliminary treatment, and direct them to the EMS care location or notify supervisory personnel of need for more extensive victim care and/or removal assistance.
3. Establish two- or three-person EMS teams to provide care for victims within the impact zone and to remove any victims as needed.
4. Request utility companies to interrupt utility services to the area at main control points for the area.
5. Establish squads of heavy equipment to conduct debris removal operations to facilitate access to any debris-blocked streets.
6. Establish a branch in the operations section to record all reports of damage to structures and coordinate structural triage activities.

The development and implementation of the objectives, strategies, and tactical operations should follow an orderly



progression initiated based on core priorities.

Confidence, Effectiveness, Efficiency & Safety

Emergency managers and incident commanders should develop an intuitive sense of awareness to fall back to the P-O-S-T process in order to organize their thoughts based on core priorities, regardless of the nature or scope of the incident. (It also may help to have a “cue card” simply stating P-O-S-T located with other emergency response field guides or first responder job aids.) Using these three core priorities to formulate objectives as statements of intent, emergency managers

then can assess strategies – or means to achieve the objectives.

Once viable strategies have been identified, the tactics or actions to accomplish the strategies can be formulated. Based on an orderly progression, as captured in the acronym P-O-S-T, emergency managers would be more confident that any scenario confronted, no matter how complex, unique, or potentially overwhelming, could be resolved with a greater degree of effectiveness, efficiency, and, above all, SAFETY. Often, the most basic of processes can be the best solution to the biggest challenges.

Stephen Grainer is the chief of IMS programs for the Virginia Department of Fire Programs (VDFP). He has served in Virginia fire and emergency services and emergency management coordination programs since 1972 – in assignments ranging from firefighter to chief officer. He also has been a curriculum developer, content evaluator, and instructor, and currently is developing and managing the VDFP programs needed to enable emergency responders and others to meet the National Incident Management System compliance requirements established by the federal government. From 2010 to 2012, he served as president of the All-Hazards Incident Management Teams Association.



Improving flood risk management in Europe

Source: <http://www.homelandsecuritynewswire.com/dr20150625-improving-flood-risk-management-in-europe>

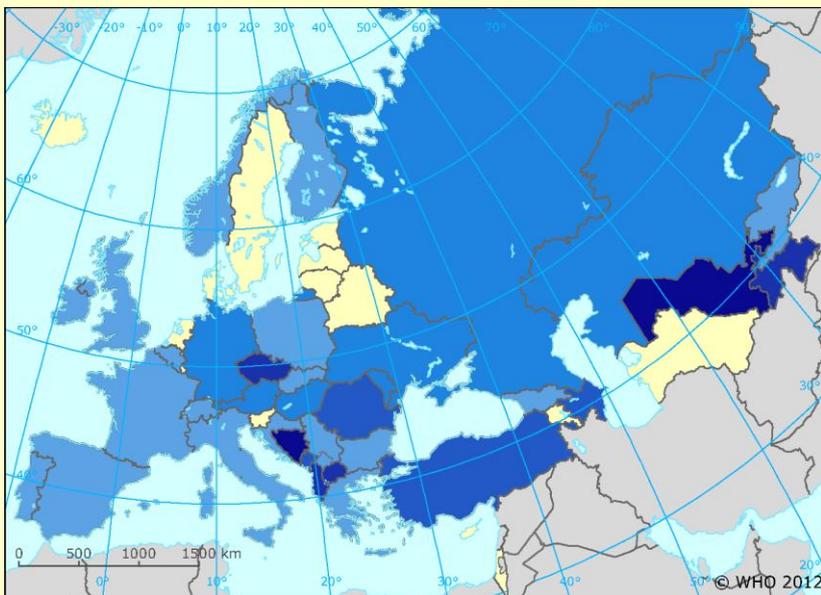
June 25 – **From 2000 to 2013, floods resulted in €5.5 billion in annual losses in Europe, and this figure is set to increase fivefold by 2050,** according to a study published last year in *Nature*. European governments have been hard at work trying to ensure sustained protection from floods by developing dykes, dams, or floodgates, but are such defense strategies alone sufficient?

“We should also focus on prevention, mitigation, flood preparation and recovery,” explains Prof. Peter Driessen of Utrecht University in the presentation video of [STAR-FLOOD](#). The project, which kicked off in October 2012 with €5.4 million in EU funding, aims to analyze, explain, evaluate, and design policies to better deal with flood risks from rivers in urban agglomerations across Europe. CORDIS reports that STAR-FLOOD has now reached the end of its core Work Package 3, which saw researchers studying flood risk

One issue that emerged was that, while the countries studied by STAR-FLOOD all seem to have been making efforts to diversify, link



together, and align Flood Risk Management Strategies, this has proved to be challenging.



91

governance in the Netherlands, Belgium, France, the United Kingdom, Poland, and Sweden based on three case study areas in each country. A thorough analysis has been performed and, although the respective reports will not be finalized until the end of September 2015, some interesting facts have already emerged from making comparisons between the countries, a process which will be at the heart of Work Package 4.

“In many cases, change towards more diversified Flood Risk Management was found to be caused by the actions of change agents throwing their weight behind new developments or by shock events (for example, floods),” the team explains on the project Web site. On the other hand, they also point to national flood policies and regulations in the United Kingdom which “were found to have a



certain degree of in-built flexibility leading to gradual changes in flood risk governance.”

In all countries, government actions for dealing with flood risks were found to be complemented by specific local actions performed by local authority actors but also by business, civil society actors and sometimes residents themselves. For the STAR-FLOOD team, this raises the fundamental question of how such initiatives can best be facilitated, and this is an issue which they will delve into over the next months.

Finally, the project notes differences in the implementation of the Floods Directive. “While all STAR-FLOOD countries are EU Member States in the process of implementing the EU Floods Directive (Directive 2007/60/EC), the relative influence attributed to the Floods Directive differs considerably between the STAR-FLOOD countries. In Poland, for

instance, there is some evidence that the Floods Directive implementation legitimized innovative policies and legislations. In the Netherlands, on the other hand, although some policymakers welcome the flood hazard and flood risk maps, in general the Floods Directive implementation is viewed as a bureaucratic exercise: it is more seen as a formalization of ‘business as usual’ than as an opportunity to improve flood risk governance,’ the team explains.

CORDIS notes that the country analysis follows the completion of the project’s Work Package 2 in November 2013, in which researchers had developed an assessment framework to perform the country and case study analyses. The project is set to end on 31 March 2016 with the release of design principles for appropriate and resilient Flood Risk Governance Arrangements (FRGAs).



Climate change risk assessment: “The inconvenient may become intolerable”

Source: <http://www.homelandsecuritynewswire.com/dr20150714-climate-change-risk-assessment-the-inconvenient-may-become-intolerable>

July 14 – An international group of scientists, energy policy analysts, and experts in risk from finance and the military on Monday (13 July 2015) released a new independent assessment of the risks of climate change, designed to support political leaders in their decisions on how much priority to give to the issue.

Their report argues that the risks of climate change should be assessed in the same way as risks to national security or public health. That means focusing on understanding what is the worst that could happen, and how likely it is to occur.

A University of Cambridge release reports that the report identifies thresholds beyond which “the inconvenient may become intolerable.” These include limits of human tolerance for heat stress, and limits of crops’ tolerance for high temperatures, which if exceeded could lead to large-scale fatalities and crop failure; as well as potential limits to coastal cities’ ability to successfully adapt to rising sea levels. It suggests that these thresholds could become increasingly likely to be crossed over time: an extreme event that may be very unlikely at one point in time could be highly likely at some later point. This will especially be the case if global emissions of greenhouse gases continue to rise, as the report suggests they will in the absence of stronger political commitment and faster technological development.

The report suggests that the largest risks of climate change may be those that are magnified by the interactions of people, markets, and governments. It finds that migration from some regions of the world could become “more a necessity than a choice” and that the risks of state failure could rise significantly, affecting many countries simultaneously.

The report recommends that climate change risk assessments should be updated regularly and communicated to political leaders at the highest level.

Speaking at the report’s launch at the London Stock Exchange, Foreign Office Minister Baroness Anelay said, “When we think about keeping our country safe, we always consider the worst case scenarios. That is what guides our policies on nuclear non-proliferation, counter-terrorism, and conflict prevention. We have to think about climate change the same way. Unlike those more familiar risks, the risks of climate change will increase continually over time — until we have entirely eliminated their cause. To manage these risks successfully, it is essential that we take a long-term view, and that we act in the present, with urgency.”



Fiona Morrison, president of the Institute and Faculty of Actuaries, a co-sponsor of the report, commented: “As the report shows, adapting to, and mitigating the risk of, climate change is of vital importance for governments. One of the most important goals of climate change policy should be to recognize the possibility of very bad outcomes and a full risk assessment of all possibilities is the best way to achieve this. As actuaries, we see good decisions as being based on exploring difficult scenarios and using this information to mitigate risk. This report will be a very useful tool in assessing the important risk factors that need to be considered and the existential implications, in the coming years, of an increase in global temperature.”

In total, the report includes contributions from over forty scientists, as well as from experts in security, finance, and economics, from eleven different countries.

Climate change risk assessment: Policy brief

The international group of experts which yesterday released the report *Climate Change: A Risk Assessment* (University of Cambridge, July 2015), summarized their recommendations in a policy brief. “An honest assessment of risk is no reason for fatalism. Just as small changes in climate can have very large effects, the same can be true for changes in government policy, technological capability, and financial regulation,” the experts write. “Leadership can make this virtuous circle turn faster, more fully mobilizing our ingenuity, resources, and commitment. In this way, the goal of preserving a safe climate for the future need not be beyond our reach.”

The international group of experts which yesterday released the report *Climate Change: A Risk Assessment* (University of Cambridge, July 2015), summarized their recommendations in a policy brief.

Here is the brief:

The most important political decision to be made about climate change is how much effort to expend on countering it. That decision should be informed by a full assessment of the risks. At the minimum, we have to think about three things:

1. *What we are doing to the climate* is emitting greenhouse gases that trap heat and warm it up. Whether those emissions go up or down in future will depend mainly on the policy choices we make, and the technological progress that expands our options. Our best guess at the moment, based on current policies and trends, is that emissions will keep going up for another few decades, and then either level off, or come down slowly. This is for two reasons: governments are not making maximum use of the technologies to reduce emissions that we already have; and technology is not yet progressing fast enough to give governments the policy options they will need in the future. In the worst case, emissions could keep on rising throughout the century.

2. *How the climate may change, and what that could do to us*, are both highly uncertain. The important thing to understand is that uncertainty is not our friend. There is much more scope to be unlucky than there is to be lucky. For any pathway of emissions through time, there are wide ranges of possible increases in global temperature and sea level. On a high emissions pathway where the most likely temperature increase is estimated to be 5°C by 2100, anything from 3°C to 7°C may be possible. However, while on this pathway the chances of staying below 3°C will become vanishingly small over time, the chances of exceeding 7°C will increase, and this extreme outcome could become more likely than not within the following century. Similarly, there is very little chance that the global sea level rise will slow down from its current rate, and every chance that it will accelerate — the only question is by how much. While an increase of somewhere between 40cm and 1m looks likely this century, the delayed response of huge ice-sheets to warming means we may already be committed to more than 10m over the longer term — we just do not know whether that will take centuries or millennia. What may appear to be small changes in climate could have very large effects, especially if important thresholds are passed. Crops have limited tolerance for high temperatures, and as the climate warms, these limits are likely to be exceeded increasingly often. This is one reason why a temperature increase of 4°C or more could pose very large risks to global food security. People have limited tolerance for combinations of high temperature and humidity. Although people do die of heat stress in the current climate, their upper limits of tolerance are rarely if ever exceeded by climatic conditions alone.



Somewhere between 5°C and 7°C of temperature increase, it starts to become likely that hot places will experience conditions that are fatal even for people lying down in the shade. Population growth alone is likely to double the number of people living below a threshold of extreme water shortage by mid-century. Climate change is likely to cause even more extreme water scarcity in some regions, while increasing the risks of flooding in others. Coastal cities probably have thresholds in terms of the rate and extent of sea level rise that they are able to deal with, but we have very little idea where those thresholds are.

3. *What, in the context of a changing climate, we might do to each other* is deeply uncertain. But we can start from the understanding that the climate hardly changed at all in the first ten thousand years of human civilization, and that even the 0.8°C of climate change we have seen so far is now causing us significant problems. It seems likely that high degrees of climate change would pose enormous risks to national and international security. Extreme water stress, and competition for productive land, could both become sources of conflict. Migration from some regions may become more a necessity than a choice, and could take place on a historically unprecedented scale. The capacity of the international community for humanitarian assistance, already at full stretch, could easily be overwhelmed. The risks of state failure could rise significantly, affecting many countries simultaneously, and even threatening those that are currently considered developed and stable.

Clearly, there are great risks not only of economic losses, but also of human losses. How to value those losses is as much a question of ethics as one of economics.

Recommendations for continuing risk assessment

Our climate change risk assessment is far from perfect, but we hope it will provoke thinking about how such assessments are done, who they are done by, and who they are done for. We recommend that:

1. *The risks of climate change should be assessed in the same way as risks to national security or public health.* When we think about keeping our countries safe, we always consider the worst case scenarios. Climate change gets worse over time, so that means we have to take a long view. We can start by identifying what we want to avoid, and then asking how the likelihood of encountering it will change over time. In all three areas discussed above, our risk assessment would be strengthened if we were to use a consistent set of indicators — so we could track how expert opinion changes over time.

2. *The risk assessment should involve a wide range of experts.* Policy analysts and energy experts should be asked where they think global emissions are most likely to be going. Political leaders should have a role in defining what it is we want to avoid; scientists can then assess its likelihood. Military strategists should be asked what security risks they would expect to arise from a high climate change world, and how manageable those might be.

3. *The risk assessment should report to the highest level of government;* not only, for example, to the environment minister or to those who are responsible for planning. The most important decision — about the level of priority to give to this problem — is one that only the head of government can take. The risk assessment should be repeated regularly and consistently, so that the direction of any changes in assessment can be clearly seen.

Risk reduction: elements of a proportionate response

An honest assessment of risk is no reason for fatalism. Just as small changes in climate can have very large effects, the same can be true for changes in government policy, technological capability, and financial regulation. Policy measures can bring down emissions directly, by regulating for cleaner energy, used more efficiently. At the same time, the right incentives can direct more investment toward clean energy technologies, accelerating innovation so that new policies become possible in future. Leadership can make this virtuous circle turn faster, more fully mobilizing our ingenuity, resources, and commitment. In this way, the goal of preserving a safe climate for the future need not be beyond our reach.

— *Read more in David King et al., [Climate Change: A Risk Assessment](#) (Center for Science and Policy, University of Cambridge, July 2015)*



Climate change a security risk second only to terrorism: Aussie defense report

Source: <http://www.homelandsecuritynewswire.com/dr20150715-climate-change-a-security-risk-second-only-to-terrorism-aussie-defense-report>

July 15 – The Australian government’s energy White Paper made headlines for its reluctance to mention the term “climate change” — but a forthcoming defense White Paper does not share these reservations.

A report on community consultations conducted by the authors of the defense White Paper highlights the consequences of climate change, extreme weather events, and environmental pressures as a significant security risk for Australia – second only to the risks posed by terrorism.

“Many people suggested [climate change] would lead to an increased need for humanitarian and disaster relief activities, including by armed forces,” the report released on Wednesday said. “Some people also noted that climate change and resource stresses, such as food and water shortages, could drive unregulated cross-border movements of people.”

The community consultations also unearthed “considerable interest in evolving the ADF [Australian Defense Force] to reduce its greenhouse gas emissions and manage its environmental impact.”

“That interest was not confined to environmental groups, and such efforts were viewed as being not only good management of resources, but also likely to improve the ADF’s operational flexibility and survivability.”

Read more in [The Longest Conflict: Australia’s Climate Security Challenge](#) (Center for Policy Development, June 2015).

Can your city survive the apocalypse?

Source: <http://edition.cnn.com/2015/07/21/tech/disaster-architecture/>

July 21 – The destruction of New Orleans by Hurricane Katrina was heralded as a wake-up call for the U.S., a catastrophe that illustrated the scale of the threat from natural disasters, and the inadequacy of preparations.

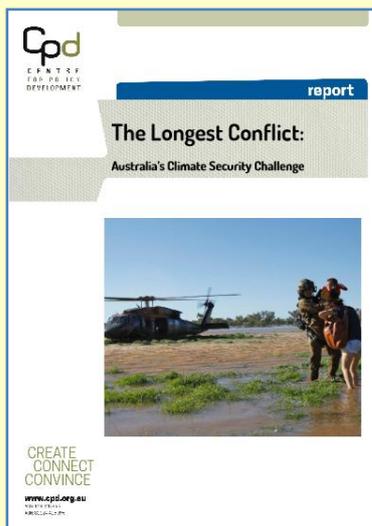
The *Guardian* quotes the Australian Strategic Policy Institute’s executive director, Peter Jennings, who oversaw the consultation process, to say that recognizing the impact of climate change did not actually require anyone to “take a position on the causes of climate change.” It was a simple strategic calculation, and one the defense White Paper needed to grapple with.

“I think our thinking here is simply to say that defense needs to make sure it’s able to manage, as it were, strategic consequences of climate change,” Jennings told the *Guardian*.

“Even if we don’t need to take a position on the

causes of climate change we do need to understand how defense forces might be called upon to respond to effects which are the products of climate change. That’s something that needs to be addressed in the white paper context.”

Jennings said defense force personnel were often required to help respond to extreme climate events in Australia such as floods, bushfires and cyclones. “Again, the question is, if we’re seeing these extreme weather events — put to one side the cause of these things — we do need to have adequate defense plans in place to respond to them.”



devastated and deeply vulnerable. Hamstrung by its position -- much of New Orleans sits below sea level -- ancient infrastructure and widespread poverty, the next disaster could be the city's last.

Hurricane Sandy underlined the urgency by ruthlessly exposing New York's structural weaknesses, paralyzing power, water and transport networks as the lights went off across Manhattan. California also suffered as historic droughts settled in, and the 2014 wave of winter storms terrorized the North, emphasizing that extreme conditions were here to stay and could strike anywhere.

This bought the U.S. into line with the global situation. The U.N.'s [global risk report](#) anticipates a record \$314 billion of damage through natural disasters each year, exacerbated by the effects of climate change such as rising sea levels and more common 'freak' weather conditions. The report also highlights a widespread lack of preparedness and "continuous mispricing of risk."

Responding to disaster

Of course, there are few easy answers to how to withstand a hurricane or ferocious drought. Eye-catching novelties such as Vincent Callebaut's prefab [coral reef design](#) in Haiti, or Dan Nelson's [tsunami-proof house](#) offer originality but are difficult to scale.



A more grounded and systematic approach to resilience is beginning to emerge. Boston narrowly escaped a battering from Sandy but remains threatened by rising sea levels, and the city recently sought designs for a new age with its ground-breaking competition '[Living with Water](#).'

Creative solutions flooded in from floating parks, to charge basins that provide hydrokinetic energy, and protection through elevating the most important parts of buildings, such as power hubs.

[Rebuild By Design](#), launched in the wake of Sandy to discover and implement resilience measures, has initiated wide-ranging projects worth almost a billion dollars across the Northeast. These include the 'Meadowlands' led by MIT that would cultivate natural buffers as flood defenses in New Jersey, while the grandest scale project would protect Manhattan with a re-designed waterfront including water-based social spaces, waterproofed buildings and additional bridges.

A bespoke solution is needed for each environment, says Amy Chester, project manager of Rebuild By Design.

"There is no one size fits all approach - every region is completely different. New York won't get a tsunami. For us hurricanes are a big threat, and we are looking at the immediate threat."

Chester believes that institution-led development must be combined with building resilience at an individual and community level.

"The first thing is shoring up property to withstand whatever comes at it. Communities are able to bounce back quicker if the water and electricity systems still reach them."

"We need a wider paradigm shift but we won't get there unless people are ready to make small choices, such as making home improvements a bit greener and reducing waste. We trade off working in public schools and improving infrastructure long term. We need public opinion and with incremental changes a tipping point arrives."

Rebuild by Design looked to the Netherlands for inspiration, which has always faced the threat of water damage and has been at the forefront of developing solutions.

'Out there' solutions

Dutch architect Koen Olthuis has pioneered an approach of building on the water itself, creating floating structures on a foundation of foam and concrete, using 'scarless' techniques that don't damage the environment. His designs are in development from a hotel off Norway (photo p.90) to a community in the Maldives, and the concept of building islands has become popular around the world.

"The only limit is finance," says Olthuis.

"Building on water is much easier than people think, it just needs a mind-set change -- people have to see water as a threat but use it as an asset."



The concept has gone from 'freak architecture' to a practical necessity, he believes.



"Governments are starting to see the possibilities -- it could bring safety and also create new spaces. Hong Kong, New York and London have no space left to build."

Amphibious solutions also offer greater flexibility, allowing for the possibility of temporary and mobile buildings. One striking suggestion is that Olympic stadiums could be transferred between host nations rather than each country bearing their enormous costs.

fittingly it is Japanese architect [Shigeru Ban](#) that has led the field of innovative disaster relief, winning the 2014 Pritzker Prize for his structures across the world, such as the paper-based cabins used in the Philippines.

Ban stresses the importance of using local resources and local labor:



"Each time it's totally different...that's why I have to go there to find a specific solution. I'm using local materials, the traditional materials. It's too expensive to hire contractors, so I propose construction methods that can be done by the victims themselves."

Ban has broken the mould by valuing aesthetics and dignity in his emergency homes, painstakingly matching color schemes and facilitating privacy. Many of his temporary designs have remained in perpetuity and serve as models for adapting architecture to a dangerous environment.

"There are no boundaries between temporary and permanent," says Ban.

The US has much to learn from regions suffering the worst of extreme conditions in its efforts to formulate an effective, coherent response, says Rachel Minnery, Director of Built Environment Policy at the American Institute of Architects.

"For seismic risk, Japan is a beautiful example, as safety from natural disaster is a priority for them. When advertising new apartment, seismic safety is as important as the granite countertop. It's not that we don't do that now, but new construction is only a small part of the built environment."

Japanese buildings are now commonly base-isolated, so that the foundations can absorb a shock without toppling the structure, a technique that will be increased demand with new reports indicating a catastrophic earthquake threat to the West Coast. Minnery wants architects to work across disciplines with the construction industry, labor force, planners and policy makers to ensure that



"People with money can own places that are higher and drier, and people with less money are more threatened. By having this technology on a larger scale we can improve the safety of threatened places. The natural location to do that is places like the Maldives, where you can have a positive effect on the slums and change the DNA. In this way, you can use architecture to create a more fair society."

The Dutchman favors a joined-up solution that combines resilient structure with urban planning that best protects the vulnerable points, along with sustainable practices that can forestall future danger, and effective disaster responses.

Learning from the front line

Few nations have been so devastated as Japan in the wake of the 2011 tsunami, and



resilience has the funding and priority it requires.

There has been movement. The President's Climate Action Plan will mandate that states include climate hazards in their disaster mitigation plans, and Minnery is confident that

the innovative resilience concepts will be adopted once they are proven, whether this means flood-proofing, seismic retrofits or building on water.

The agonizing concern is that such measures may arrive too late.



A Proven Method for Public-Private Virtual Collaboration

By Christina Fabac & Chas Eby

Source:http://www.domesticpreparedness.com/Industry/Private_Sector/A_Proven_Method_for_Public-Private_Virtual_Collaboration/

During a disaster, private sector companies may not have access to valuable public sector resources and information. Some government agencies, though, are building online portals that provide businesses with situational awareness, such as real-time weather forecasts, road closures, and emergency alerts, as well as a chat room to increase public-private collaboration and private sector resilience.

The ability of businesses to prepare for, maintain operations during, and recover from disasters and emergencies is vital to the safety and well being of the public. Private sector preparedness also is fundamentally aligned with the mission of many emergency management agencies: to help ensure community members have access to resources and services during incidents and to collaborate and build preparedness with stakeholder groups, including those outside government. Emergency management agencies can accomplish this in many ways. The Maryland Emergency Management Agency (MEMA) focuses on providing training, hosting regular meetings, issuing alerts, and building relationships with the private sector. Many of the aforementioned activities contribute to the goal of including businesses in emergency management and are similar to tactics used to engage government agencies outside the homeland security and emergency management discipline.

Still, risk managers and continuity experts in the private sector may not have much time to commit to traditional, scheduled meetings and conference calls, especially during crises that distress their companies. For this reason, MEMA has developed an asynchronous platform using commercially available technology to create a virtual business operations center (VBOC). Members of MEMA's Private Sector Integration Program (PSIP), who are private sector employees with responsibility for their business' emergency preparedness, can access the VBOC at any time during a disaster for situational awareness, incident-specific documents, and

access to government officials staffing the state emergency operations center (SEOC).

Engaging & Integrating Businesses

MEMA started PSIP to engage and collaborate with companies operating in Maryland. The mission of PSIP is to increase communication between government and business sectors during normal operations, and leverage these established partnerships to increase information exchange during emergencies and disasters. PSIP is a continuous effort and the program includes ongoing engagement with members and specific operations during emergency activations. During such activations, PSIP uses three components to integrate businesses into state emergency operations: (1) the Business Operations Center (BOC), which includes the VBOC; (2) Operational and Situational Preparedness for Responding to an Emergency (OSPREY) Business, a geographic information system tool that maps business locations and their operating status; and (3) the BOC representative program, which allows vetted PSIP members to assist in the staffing of the BOC desk in the SEOC.

The BOC is responsible for providing businesses, nongovernmental organizations, and trade associations with situational awareness and for coordinating government agencies to help solve issues affecting these stakeholders during emergencies. The goal is to provide PSIP members with information appropriate to the private sector in order to assist them in making decisions regarding business operations and continuity. The BOC is a physical location within Maryland's SEOC. One of the key factors contributing to the success of PSIP – and likely an important characteristic for any emergency management program that incorporates the private sector – is that the majority of situational awareness products, information, and interaction are accessed asynchronously. PSIP members can log into the VBOC at any time, as opposed to establishing



set times to distribute information or convene conference calls.

Emergency management, homeland security, and related agencies that would like to establish an effective private sector preparedness program may want to consider developing an online or virtual method for collaborating with and providing information to businesses during disaster or emergency operations. MEMA has accomplished this by establishing the VBOC and operationalizing this system during emergency operations center activations for threats or hazards that could potentially impact businesses throughout the state.

Components of a Virtual Business Operations Center

The MEMA VBOC is hosted on the Homeland Security Information Network Adobe Connect platform and is a trusted method for sharing sensitive but unclassified information with PSIP members. The purpose of activating the VBOC is to give businesses the ability to pull real-time information during an emergency so they can make informed decisions related to business operations and continuity. Much of the information provided, such as situation reports, live traffic cameras, and real-time radar, are sources typically used by government response agencies, and that may not be easily accessible to private companies. All members of PSIP have access to the interactive, online VBOC as soon as it is activated by MEMA.

MEMA's collaborative virtual operations center for the private sector includes a variety of information, components, and screens that are useful to businesses, including the following:

- *File-sharing database.* A database that can store important documents issued by government is useful because it allows businesses to enter the VBOC and download the files at their convenience. Such documents have included situational reports, weather forecasts, and press releases. In addition to files from the SEOC, private sector members are able to post information to the database.
- *Chat room.* A chat feature is important to an asynchronous operation because it allows businesses to post questions, concerns, or feedback at any time without necessitating that the user wait for a response. Posts and answers are saved in the chat room so that other users entering the VBOC later may

see previous posts, questions, and answers.

- *Live traffic maps, highway cameras, and collision reports.* One advantage to the Maryland VBOC, which uses multiple data sources and screens, is that it becomes a single site with pertinent information for businesses' decision making. Though traffic congestion maps may be readily accessible, these maps, in conjunction with live-streaming traffic cameras and collision reports, provide an easy way for businesses to identify transportation issues that could impact their business operations.
- *Weather radar.* Direct access to National Weather Service or other trusted weather agency forecasts and live radars provide important information to the private sector from the same source that government agencies use to make operational and emergency response decisions.
- *Emergency operations center webcam.* The Maryland SEOC uses a live-streaming webcam of the activated emergency operations center, which is made available to businesses through the VBOC. Though this may have less direct benefit than other information streams in the VBOC, it also may augment engagement. Some businesses yearn to be part of the emergency management process and this partnership is advantageous to both government agencies and private sector partners.

Regular collaboration between government agencies involved in incident response and private sector businesses is an essential component of whole-community emergency management. However, this partnership cannot be effectively established by traditional methods. Private sector employees may not be able to shift work schedules and obligations around meetings, conference calls, and even emails. A solution to these issues is to develop an online virtual business operations center that can be accessed intermittently and includes all of the information that businesses need to make informed decisions during emergencies. MEMA's PSIP and the Maryland VBOC enhance the important partnership between government and the private sector, which is critical to the successful resolution of emergencies and disasters.



Christina Fabac joined the Maryland Emergency Management Agency (MEMA) as a National Capital Region planner and the private sector liaison. As the private sector liaison, she manages the Private Sector Integration Program, which communicates and collaborates with private sector partners and coordinates the Maryland business operations center. Prior to joining MEMA, she worked in the private sector practicing law in Prince George’s County, Maryland. She received a Juris Doctor from University of Baltimore School of Law.

Chas Eby was appointed as external outreach branch manager at the Maryland Emergency Management Agency (MEMA), where he develops strategy and oversees programs that include disaster recovery operations, public information and outreach, and individual, community, and private sector preparedness initiatives. Prior to joining MEMA, he was chief planner for emergency preparedness at the Maryland Department of Health & Mental Hygiene (DHMH), where he led health systems recovery, mass fatality management, bioterrorism, and private sector preparedness planning. He received a Master of Arts degree in security studies from the Naval Postgraduate School. He previously graduated from Boston College.

*Significant contributions to this article were made by **Brendan McCluskey**, the director of preparedness at the Maryland Emergency Management Agency (MEMA). His portfolio includes the Adaptive Planning, Active Learning and Exercising, and External Outreach Branches and the Mitigation Unit at MEMA. Prior to joining the agency, he was the executive director of the Office of Emergency Management and Occupational Health and Safety at the University of Medicine & Dentistry of New Jersey. He received a Juris Doctor degree from the Rutgers University School of Law.*

ISO business impact analysis technical specification approved

Source: <http://www.continuitycentral.com/index.php/news/business-continuity-news/370-iso-business-impact-analysis-technical-specification-approved>

July 16 – **ISO/PRF TS 22317**, the new technical specification for business impact analysis, has reached stage 60.00 in the ISO standards development process.

This means that the technical specification, officially titled ‘Societal security -- Business continuity management systems -- Guidelines for business impact analysis (BIA)’, has had its final draft (FDIS) approved by a formal vote.

The 27 page document will now be prepared for publication.

ISO/PRF TS 22317 is being developed by the ISO Technical Committee 292 (Security and Resilience).

