September 2014

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

www.cbrne-terrorism-newsletter.com

Fukushima Child Thyroid Issue

By Leslie Corrice

Source: http://www.hiroshimasyndrome.com/fukushima-child-thyroid-issue.html

*(The following are the facts with **Fukushima Prefecture**'s **child thyroid anomalies**. It is a synopsis of reports posted in Fukushima Updates and Fukushima Commentary on this website between March, 2011 and January, 2014. The summation shows the frequency of **thyroid cancers** had nothing to do with the nuclear accident.)*

On October 8, 2011, Fukushima University doctors began checking the thyroids of children in Fukushima Prefecture. The examinations, on a scale that medical officials called unprecedented, came amid concern that the cancer rate among Fukushima Prefecture's children could surge due to the Fukushima nuclear accident. Dr. Shinichi Suzuki of the university's medical school predicted it would take several years to carry out preliminary examinations because of the large number of those 18 and under, and the voluntary nature of the study. Suzuki said it would take several years for any irregularities in the children's thyroids to manifest as cancer. He pointed to the fact that an increase was seen four-to-six years after the 1986 Chernobyl meltdown in Ukraine, but not before. In the international news media, a few critics contended that a longer period of latency should be considered before drawing firm conclusions because of a controversy concerning the biological effects of low level radiation exposure.

For more than a year, the prefectural government offered free thyroid medical exams to the parents of 360,000 children in Fukushima Prefecture. Of the more than 38,000 children tested through March of 2012, 13,646 were found to have thyroid lumps or cysts by the prefectural medical staff. However, the existence of these thyroid anomalies could not be compared to other Japanese children who lived far away from Fukushima because no such data existed. Thus, researchers could not determine if the large number of positive tests was due to the Fukushima accident. Medical researchers planned to conduct similar extensive thyroid examinations on roughly 4,500 children aged 18 or younger, far away from Fukushima Prefecture, in order to make a statistical comparison. Benign thyroid anomalies are not uncommon in children. But, the Japanese government had no epidemiological data-base to make a valid appraisal of the impact of a nuclear accident on child thyroids.

Immediately after these numbers were made public, the antinuclear voices of doom said the data from Fukushima Prefecture was the onset of a cancer epidemic in Japan. Long-standing nuclear

energy critic Helen Caldicott, a licensed Australian pediatrician living in the United States, maintained that all positively-detected children should be immediately biopsied because 13,766 of 38,114 children tested, or 36.1%, having either nodules or cysts was alarmingly high. She further insisted that this was an early appearance of thyroid abnormalities, strongly indicating that the children received a very high dose of radiation, and not the very low exposures publicized by the Japanese officials. She also asserted that it is not normal for children to have these nodules and/or cysts. However, Japanese medical experts lacking Caldicott's extreme antinuclear agenda, scoffed at her statements. Doctors Suzuki and Shunichi Yamashita of Fukushima University posted a formal

letter on the Web which concluded, “We have defined what needs the second-stage examination as nodules over 5.1 mm and cysts (non-solid but colloidal or liquid collection only) over 20.1 mm. Thus, in addition to those with no abnormal findings, those with nodules smaller than 5 mm or cysts smaller than 20 mm have been decided not to be the subjects of further testing such as biopsies, or treatments.” [1.] Thus, less than 0.6% of the Fukushima children who tested positive for these anomalies were medically worthy of further study and/or biopsy. The overlying tone of caution in the Fukushima researcher’s letter was due to their lack of national data which could be used to draw a confident conclusion.

On August 20, 2013, the Fukushima researchers announced discovery of 18 papillary child thyroid cancers. This was out of the 210,000 children which had been tested across the prefecture, up to that point in time. In addition to the 18 confirmed cases, another 25 were suspected of possibly developing the cancer. The national incidence of thyroid cancers across all age groups was said to be “one in hundreds of thousands”, but the data was sparse and lacking a high degree of confidence. For example in 2006, 46 cases of thyroid cancer were officially confirmed in Japan across all age groups, but there was no data on papillary child thyroid cancers in the statistical cohort. Fukushima’s medical team said they could not determine whether or not the 18 cancers were caused by Fukushima radioactive releases. Though unlikely, they could not say it was absolutely impossible. [2.] However, the medical team again stressed that examinations of this sensitivity and detail had never been run on a population of Japanese children this large before, so there was no relevant data in Japan with which to compare the results.

On November 14, 2013, Fukushima’s unprecedented child thyroid survey had found a few more cancers. Of the 226,000 children that had been screened, 26 child thyroids were found to be cancerous and another 32 are felt to be possible thyroid cancer cases. All 26 of the confirmed children underwent successful cancerous material removal surgery and were doing well. The Prefecture’s experts pointed out that papillary thyroid cancer develops at a very slow pace and not enough time has passed to link the newly discovered cancers to the Fukushima accident. Fukushima’s screening program had never occurred before in Japan, thus there is no way to assess whether or not the number of cases is typical. [3.] In addition, there was scientific evidence that papillary thyroid cancers are more common than data might suggest. [4.] In fact, the referenced report states, "Studies published as early as 1947 demonstrated it [the commonality of papillary child thyroid cancer], and more recently, a report has shown that nearly every thyroid gland might be found to have a cancer if examined closely enough." Thus, scientific evidence on the specific thyroid cancer found in the Fukushima cohort added further intensity to the desire for a more substantial data base using prefectures far from Fukushima.

Many Japanese Medical experts said these frequencies were probably not unusual for Japan when the extreme sensitivity of the survey and type of cancer was considered. They pointed to similar screenings which were run in three far-distant Prefectures in 2012 and early 2013, the numbers of which were publically posted. Results showed that the Fukushima child thyroid cancer frequencies were relatively consistent with the other three Prefectures. In fact, the other three Prefectures had child thyroid anomaly rates slightly higher than with Fukushima. [5.] The three tested prefectures, far from Fukushima, were Nagasaki, Aomori and Yamanashi. While the percentage of Fukushima children with detectible nodules/cysts was 41.2%, the combined percentage found in the other three prefectures was 56.6%! Further, while 0.6% of the Fukushima children with the anomalies were considered worthy of further testing, the other three prefectures had a rate of over 1%. The total number of children tested in the far-from-Fukushima prefectures was 4,300, thus the data was considered scientifically and statistically valid. One over-riding conclusion was drawn out of this study: It seemed the child thyroid anomalies first detected in Fukushima Prefecture had been occurring quite normally across the entire country, but had gone largely unnoticed before the national screenings of 2102-13. But, the bottom line was that the Fukushima data was in no way indicative anything unusual.

However, that's not what many radiation-averse people in Japan wanted to hear. Millions of Japanese wanted to believe the bad news and rumors concerning the child thyroid situation in

Fukushima, and disbelieved any posted evidence to the contrary. Many concluded either that all of Japan was so heavily contaminated by the Fukushima nuclear accident that children outside Fukushima have even higher incidents of thyroid abnormalities, or that the Fukushima researchers were doctoring the statistics. Thus, even the most conclusive evidence concerning child thyroid issues with respect to Fukushima, and all of Japan, was rejected by a numerically-significant fraction of Japan's population because it contradicted their pre-existing mind-set.

Finally, it was reported on December 23, 2013, that there were 59 cases of child thyroid cancers either confirmed or suspected. A few medical critics remained convinced it was possible that the number of child thyroid cancers in Fukushima Prefecture may have been due to nuke accident exposure, clinging ruthlessly to a comparison with national registry data. One dissenter, Okayama University professor Toshihide Tsuda, purported that the frequency of child thyroid problems in Fukushima Prefecture is "several tens of times" higher than before the accident. He said national statistics between 1975 and 2008 showed a variance of between 5 to 11 cases per million people. Tsuda concluded that 59 cases out of ~240,000 Fukushima children is so much higher than national registry data, that the possibility of Fukushima radiation as a cause cannot be dismissed. However, most medical experts said that Tsuda's conclusion was non-scientific because it was based on national statistics covering all age groups and should not have been compared to the 18-and-under cohort alone. Tetsuya Ohira of Fukushima Medical School said it is not scientifically appropriate to compare the Fukushima child numbers with the national cancer registry. Another Fukushima Medical University professor Suzuki said there is no actual link between the low nuclear accident radiation exposures and the confirmed/suspected child thyroid cancer cases in Fukushima. The expert opinions were presented at a December 21, 2013, meeting held by Tokyo's Environment Ministry and the Fukushima government. [6]

By the end of December, 2013, the consensus of Fukushima medical experts were agreed that the apparently-elevated child thyroid cancer rate in the prefecture was probably not due to the accident. Generally, they said it was too soon to judge that Fukushima radiation was the culprit and the new national data seemed to confirm their opinion. They continued to stress it was unlikely that the cancers are due to the nuke accident because of the fact that Chernobyl thyroid anomalies did not happen until 4-6 years after the accident, and it had been less than three years since the atmospheric release of radioactive Iodine from Fukushima. Plus, the amount of radioactive Iodine expunged into the environment from F. Daiichi was many times less than with Chernobyl. Further, severe food consumption restrictions were imposed in Japan that were not the case in the Ukraine. Thus, the worst-case child exposures from Fukushima were many, many times less than what occurred with Chernobyl. Dr. Choi Kin of Hong Kong Medical Association added that no one can scientifically prove the increase in cancer incidence was from Fukushima, and that other natural causes were most likely the root-cause of the issue. [7]

Update, May 20, 2014 - The number of children diagnosed with cancerous growths in their thyroids increased to fifty. More than 290,000 children have been screened, to date, and another 70,000 are going to be tested by the end of 2014. [8] Since it is unlikely that any of the

detected cancers are due to the Fukushima accident (see above), it is likely that the detailed screening program has been a benefit to the families of the affected children. Without this groundbreaking program, it is likely that none of the cancers would have been found.

▶ **References are available at source's website.**

Leslie Corrice has a Bachelors degree in Nuclear Technology and Environmental Sciences and a Masters degree in Philosophy. Corrice is member of the American Nuclear Society and Scientists for Accurate Radiation Information.

Feasibility of a Low-Yield Gun-Type Terrorist Fission Bomb

By B. Cameron Reed

Source: http://fas.org/pir-pubs/feasibility-low-yield-gun-type-terrorist-fission-bomb/

Edward Friedman and Roger Lewis's essay "A Scenario for Jihadist Nuclear Revenge," published in the Spring 2014 edition of the *Public Interest Report,* is a sobering reminder of both the possibility of a terrorist nuclear attack based on stolen highly-enriched uranium and the depressing level of public ignorance of such threats.[1] Articles exploring the issue of terrorists or rogue sub-national actors acquiring and using a nuclear weapon or perpetrating some other type of nuclear-themed attack have a long history and have addressed a number of scenarios, including a full-scale program to produce a weapon from scratch,[2] use of stolen reactor-grade plutonium,[3] an attack with a radiological dispersal device,[4] and the vulnerability of research reactors.[5]Equally vigorous are discussions of countermeasures such as detecting warheads[5] and searching for neutron activity due to fissile materials hidden inside cargo containers.[6] An excellent summary analysis of the prospects for a terrorist-built nuclear weapon was prepared almost three decades ago by Carson Mark, Theodore Taylor, Eugene Eyster, William Maraman and Jacob Wechsler,[7] who laid out a daunting list of materials, equipment, expertise and material-processing operations that would be required to fabricate what the authors describe as a "crude" nuclear weapon – a gun or implosion-type device similar to *Little Boy* or *Fat Man*. The authors estimated that such a weapon might weigh on the order of a ton or more and have a yield of some 10 kilotons. Perpetrators would face a serious menu of radiological and toxicological hazards involved in processing fissile materials. For example, both uranium (U) and plutonium (Pu) are chemically toxic; also, U can ignite spontaneously in air and Pu tends to accumulate in bones and kidneys. Of course, longer-term health effects might be of little concern to a group of suicidal terrorists.[8]

While the difficulties of such a project might provide reassurance that such an effort has a low probability of being brought to fruition, we might ask if nuclear-armed terrorists along the lines envisioned by Friedman and Lewis would be willing to settle for a relatively low-yield device to achieve their ends. A bomb with a yield of 10 percent of that of *Little Boy* would still create a devastating blast, leave behind a radiological mess, and generate no small amount of social and economic upheaval. Such a yield would be small change to professional weapons engineers, but the distinction between one kiloton and 15 kilotons might largely be lost on political figures and the public in the aftermath of such an event. Timothy McVeigh's 1995 Oklahoma City truck bomb used about 2.5 tons of explosive; a one-kiloton detonation would represent some 400 such explosions and make a very powerful statement.

Motivated by Friedman and Lewis's scenario, I consider the feasibility of an extremely crude gun-type U-235 device configured to be transported in a pickup truck or similar light vehicle. My concern is not with the difficulties perpetrators might face in acquiring fissile material and clandestinely preparing their device, but rather with the results they might achieve if they can do so. The results reported here are based on the basic physics of fission weapons as laid out in a series of pedagogical papers that I have published elsewhere.[9] The essential configuration and expected yield of the device proposed is described in the following section; technical details of the physics computations are gathered in the Appendix.

A Crude Gun-Type Fission Bomb

The bare critical mass of pure U-235 is about 46 kg; this can be significantly lowered by provision of a surrounding tamper. I frame the design of a putative terrorist bomb by

assuming that perpetrators have available 40 kg of pure U-235 to be packaged into a device with a length on the order of 2-3 meters and a total estimated weight of 450 kg (1000 pounds), of which 200 kg is budgeted for tamper material. The 40-kg core is subcritical, and the uranium need not be divided up into target and projectile pieces as in the Friedman-Lewis scenario, although the design suggested here could easily be modified to accommodate such an arrangement.

As sketched below, I assume that the uranium is formed into a cylindrical slug of diameter and length L_{core}. The core and a plug of tamper material are to be propelled down an artillery tube into a cylindrical tamper case such that the core will be located in the middle of the case once assembly is complete; the assembled core-plus-tamper is assumed to be of diameter and length L_{tamp}. The choice of tamper material is a crucial consideration; it can seriously affect the predicted yield. In the case of *Little Boy*, readily-available tungsten-carbide (WC) was employed. Beryllium oxide (BeO) has more desirable neutron-reflective properties, but is expensive and its dust is carcinogenic; more importantly, an effort to acquire hundreds of kilograms of it is likely to bring unwanted attention. I report results for both WC and BeO tampers.

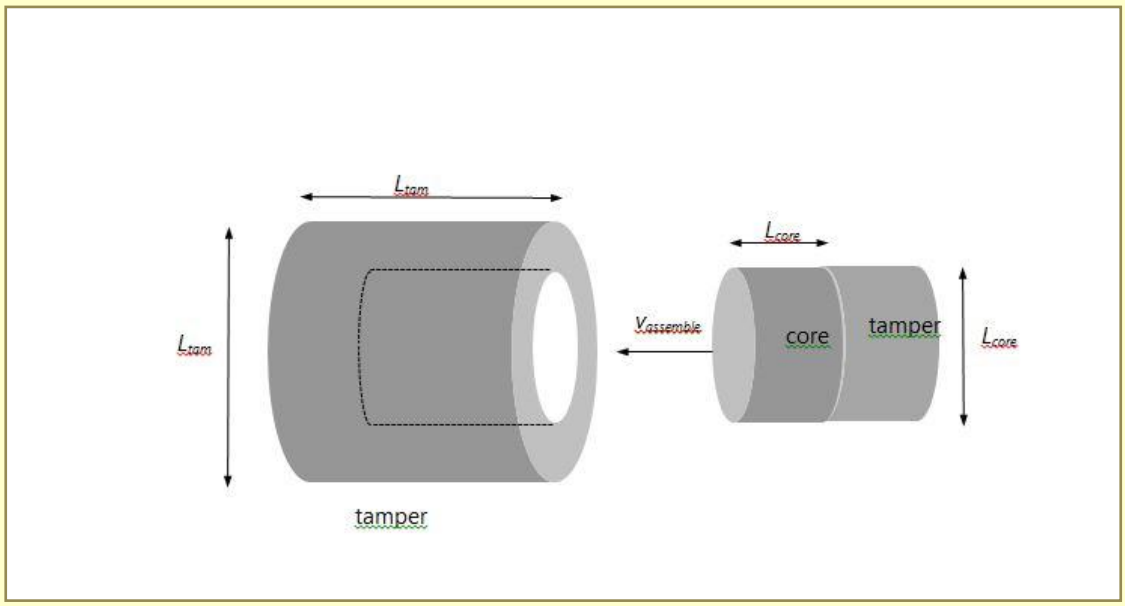


Figure 1: Sketch of a cylindrical tamper case and core/tamper-plug projectile assembly. A 40-kg U-235 core of normal density will have Lcore = 14 cm.

Adopted parameters and calculated results are gathered in Table 1. Technical details are described in the Appendix; the last line of the table gives estimated yields in kilotons. To estimate these yields I used a FORTRAN version of an algorithm which I developed to simulate the detonation of a spherical core-plus-tamper assembly (see the numerical simulation paper cited in footnote 10). A spherical assembly will no doubt give somewhat different results in detail from the cylindrical geometry envisioned here, but as the program returns an estimated yield for a simulation of *Little Boy* in good accord with the estimated actual yield of that device, we can have some confidence that the results given here should be sensible.

For both configurations in Table 1, the sum of the core, tamper, and artillery-tube masses is about 315 kg (700 lb). With allowance for a breech to close off the rear end of the tube, neutron initiators, detonator electronics, propelling chemical explosives and an enclosing case (which need not be robust if the weapon is not to be lifted), it appears entirely feasible to assemble the entire device with a total weight on the order of 1,000 pounds. Beryllium oxide is clearly preferable as the tamper material, but even with a tungsten-carbide tamper the yield is about 10 percent of that of *Little Boy*. In open terrain a 2-kiloton ground-burst creates a 5-psi overpressure out to a radius of about one-third of a mile; such an overpressure is quite sufficient to destroy wood-frame houses.

In summary, the sort of vehicle-deliverable makeshift gun-type fission weapon envisioned by Friedman and Lewis appears to be a very plausible prospect; yields on the order of a few kilotons are not out of reach. In view of the fact that all of the calculations in this paper are based on open information, there are sure to be nuances in the physics and

particularly the engineering involved that would make realization of such a device more complex than is implied here. But this exercise nevertheless serves as a cautionary tale to emphasize the need for all nuclear powers to rigorously secure and guard their stockpiles of fissile material.

Technical Appendix

Refer to Table 1 and the figure above. A 40-kg U-235 core of normal density (18.71 gr cm^{-3}) will have L_{core} = 13.96 cm. The first three lines of Table 1 give adopted atomic weights, densities, and elastic-scattering cross sections for each tamper material. The next two lines give the tamper size and plug mass, and the sixth line the total length of the core-plus-plug bullet.

To estimate the yield of the proposed device I assumed for sake of simplicity that the core is spherical (radius ~ 8 cm) and surrounded by a snugly-fitting 200-kg tamper. Each fission was assumed to liberate 180 MeV of energy and secondary neutrons of average kinetic energy 2 MeV. The number of initiator neutrons was assumed to be 100, radiation pressure was assumed to dominate over gas pressure in the exploding core, and the average number of neutrons per fission was taken to be n = 2.637.

Lines 7 and 8 in Table 1 refer to two important considerations in bomb design: the speed with which the core seats into the tamper and the propellant pressure required to achieve this speed. The core material will inevitably contain some U-238, which, because of its high spontaneous fission rate (~ 7 per kg per second), means that there will be some probability for premature initiation of the chain reaction while the core and tamper are being assembled. (There is no danger of pre-detonation before seating as 40 kg is less than the "bare" critical mass of U-235. The danger during seating arises from the fact that the tamper lowers the critical mass.) The key to minimizing this probability lies in maximizing the assembly speed. If our 40-kg core contains 10 percent by mass U-238, the pre-detonation probability can be kept to under 10 percent if the time during which the core is in a supercritical state during assembly is held to no more than four milliseconds (see the pre-detonation paper cited in footnote 10). The seventh line of Table 1 shows corresponding assembly speeds based on this time constraint and the core-plug lengths in the preceding line. These speed demands are very gentle in comparison to the assembly speed employed in *Little Boy*, which was about 300 m s^{-1}.

To achieve the assembly speed I assume that (as in *Little Boy*), the core-plus-plug is propelled along a tube by detonation of a conventional explosive adjacent to the rear end of the tamper plug in the tail of the weapon. To estimate the maximum pressure required, I assumed that the propulsion is provided by the adiabatic expansion (in which no heat is gained or lost) of the detonated explosive. Adiabatic expansion of gas to propel a projectile confined to a tube has been extensively studied; an expression appearing in Rohrbach et. al.[10] can be used to estimate the initial pressure required given the cross-sectional area of the tube, the mass of the projectile, the length of the tube, a value for the adiabatic exponent _gand the assembly speed to be achieved. This pressure also depends on the initial volume of the detonated explosive; for this I adopted a value of 0.004 m^3, about the volume of the core-plug assemblies. The eighth line of Table 1 shows the estimated necessary initial pressures (neglecting any friction between the projectile and the tube) for a travel length of 1.5 meters for g = 1.4; this value of g is characteristic of a diatomic gas. These pressures are very modest, and would set no undue demands on the tube material. Stainless steel, for example, has an ultimate strength of ~ 500 MPa (~75,000 psi); such a tube of inner diameter 7 cm, thickness 1 cm, and length 2 meters would have a mass of about 75 kg. This would bring the sum of the core, tamper, and tube masses to ~ 315 kg (700 lb).

A final technical consideration is the so-called fizzle yield that this makeshift weapon might achieve, that is, its yield if the chain reaction should begin at the moment when the core achieves first criticality. As described by von Hippel and Lyman in Mark (footnote 3), the fizzle yield as a fraction of the nominal design yield can be estimated from the expression $Y_{fizzle}/Y_{nominal} \sim (2t\ F/a\ t_O)^{3/2}$, where t is the average time that a neutron will travel before causing a fission, F is the natural logarithm of the number of fissions that have occurred when the nuclear chain reaction proper can be considered to have begun, a is a parameter in the exponential growth rate of the reaction set by the masses and sizes of the core and tamper, and t_O is the time required to complete the core assembly. As described by Mark, $t \sim 10^{-8}$ sec and $F \sim 45$. For the design posited here, a~ 0.32 for the WC tamper and ~ 0.47 for the BeO tamper; see Reed (2009) in footnote 10 or Sect. 2.3 of the last reference in footnote 10 regarding the computation of a. Taking t_O = 0.004 sec gives $Y_{fizzle}/Y_{nominal} \sim 1.9 \times 10^{-5}$ for the WC tamper and 1.0×10^{-5} for the BeO tamper. With nominal yields of 1.4 and 4.9 kt, the estimated fizzle yields are only ~ 27 and 50 kilograms equivalent. While the

perpetrators of such a device might be willing risk such a low yield in view of the low pre-detonation probability involved, they would be well-advised to increase the assembly speed as much as possible.

Parameter	Unit	WC	BeO
Atomic Weight	gr mol^{-1}	195.84	25.01
Density	gr cm^{-3}	14.8	3.01
Elastic-scattering cross-section[a]	bn	6.587	5.573
Tamper size L_{tamp}	cm	27.11	44.37
Tamper plug mass	kg	14.90	7.01
Core + plug length	cm	20.5	29.2
Assembly speed	m s^{-1}	51	73
Firing pressure	psi	2030	3330
Yield	kt	1.4	4.9

Table 1: Adopted and calculated parameters for a simple gun-type fission weapon, assuming a 40-kg core of U-235.

*Fission-spectrum averaged elastic-scattering cross-sections adopted from Korea Atomic Energy Research Institute Table of Nuclides, http://atom.kaeri.re.kr

Cameron Reed *is the Charles A. Dana Professor of Physics at Alma College, where he teaches courses ranging from first-year algebra-based mechanics to senior-level quantum mechanics. He received his Ph.D. in Physics from the University of Waterloo (Canada). His research has included both optical photometry of intrinsically bright stars in our Milky Way galaxy, and the history of the Manhattan Project. His book The History and Science of the Manhattan Project was recently published by Springer.*

Ontario delaying federal push to get anti-radiation pills to those who live near nuclear plants

By Ashley Csanady (News editor, Canada.com.)
Source: http://o.canada.com/health/ontario-delaying-federal-push-to-get-anti-radiation-pills-to-those-who-live-near-nuclear-plans

Almost nobody within 10 km of Ontario's nuclear plants has anti-radiation pills because bureaucrats are bickering over who will hand out the drugs.

The Canadian Nuclear Safety Commission has recommended the mandatory distribution of potassium iodide (KI) pills to all residents within a 10-km radius of nuclear facilities. The pills, if taken immediately before or after a nuclear disaster, can help alleviate the effects of radiation poisoning.

But Ontario bureaucrats are delaying the process.

"This is a critical piece of our responsibilities of the public and I would hate to see it lost because of jurisdictional issues," said Dr. Sandy McEwan, a member of the Nuclear Safety Commission and past president of the Canadian Association of Nuclear Medicine. The circles in the map show the areas where pills should be distributed.

Two letters obtained by Canada.com show the province supports the pre-distribution of radiation-blocking potassium iodine (KI) pills, but is quibbling over who will do it.

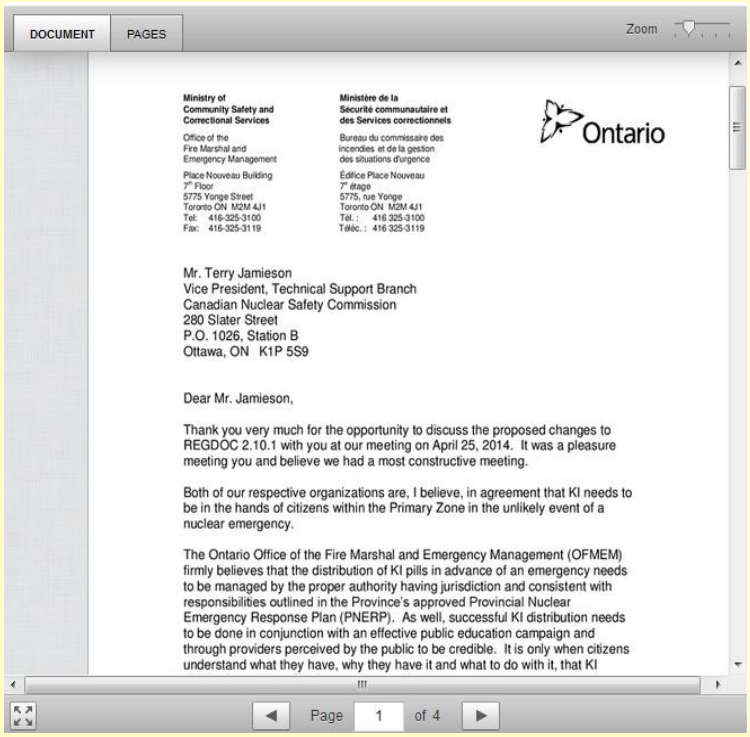
The province wants the chief medical officer of health to take charge while the federal regulator wants nuclear facilities to send out the pills.

Meanwhile, nobody is actually sending out pills to the people who may need them.

Commission President Michael Binder slammed Ontario officials

at a hearing in Ottawa Thursday, saying they're unnecessarily delaying a necessary public safety measure. He called out the health ministry for failing to send anyone to the hearing and told provincial officials the commission expects the pills to be sent out by December 2015 or it will step in.

"Our preferred outcome is that the Ontario government would be the lead in this… but we will not accept a forever paralysis by analysis," Binder said.


DOCUMENT PAGES Zoom

Ministry of Community Safety and Correctional Services
Ministère de la Sécurité communautaire et des Services correctionnels
Ontario

Office of the Fire Marshal and Emergency Management
Bureau du commissaire des incendies et de la gestion des situations d'urgence

Place Nouveau Building, 7th Floor, 5775 Yonge Street, Toronto ON M2M 4J1, Tel: 416-325-3100, Fax: 416-325-3119
Édifice Place Nouveau, 7e étage, 5775, rue Yonge, Toronto ON M2M 4J1, Tél.: 416 325-3100, Téléc.: 416 325-3119

Mr. Terry Jamieson
Vice President, Technical Support Branch
Canadian Nuclear Safety Commission
280 Slater Street
P.O. 1026, Station B
Ottawa, ON K1P 5S9

Dear Mr. Jamieson,

Thank you very much for the opportunity to discuss the proposed changes to REGDOC 2.10.1 with you at our meeting on April 25, 2014. It was a pleasure meeting you and believe we had a most constructive meeting.

Both of our respective organizations are, I believe, in agreement that KI needs to be in the hands of citizens within the Primary Zone in the unlikely event of a nuclear emergency.

The Ontario Office of the Fire Marshal and Emergency Management (OFMEM) firmly believes that the distribution of KI pills in advance of an emergency needs to be managed by the proper authority having jurisdiction and consistent with responsibilities outlined in the Province's approved Provincial Nuclear Emergency Response Plan (PNERP). As well, successful KI distribution needs to be done in conjunction with an effective public education campaign and through providers perceived by the public to be credible. It is only when citizens understand what they have, why they have it and what to do with it, that KI

Page 1 of 4

Health Minister Eric Hoskins said in a statement that Ontario shares the federal government's goal of ensuring all Ontarians have access to potassium iodine pills. He said The Office of the Fire Marshal and Emergency Management leads nuclear planning but didn't address the allegations of delays.

"We are working closely with both municipalities and nuclear facilities on plans for the distribution of Potassium Iodide (KI) pills," he said.

Paired with the pill distribution, though, is the need for a public education campaign to teach people what they should do with the pills once they get them. That information is also sorely lacking in the areas around nuclear facilities.

"A number of participants knew about these [KI pills], but none had these pills on hand at home for their household, and few knew that they were made available for free at certain pharmacies," the report states.

"It is obvious that there is a similar lack of awareness and lack of uptake of KI by households in advance of a potential accident

and therefore pre-distribution is the only reasonable approach," the Canadian Environmental Law Association states in a submission to the commission.
Ontario is the only province in which the KI pills aren't distributed within a designated range around its generating stations in Kincardine, Pickering and Ajax. Canada's only other two nuclear power plants, in Quebec and New Brunswick, both distribute the pills every five years within an eight- and 20-km radius respectively. In countries around the world it's standard practice.
Both CELA and Greenpeace Canada want the pills distributed beyond 10 km, especially to vulnerable populations like pregnant women and children.
KI pills block radioactive iodine from invading the thyroid, the most sensitive part of the body to radiation. The pills do not protect against other effects of radiation and can have severe side effects, so they should not be taken except in an emergency.
Ontario Power Generation has 700,000 KI pills stashed in the event of an emergency. And Bruce Power 20,000 pills stored for employees and residents. Both corporations have also raised concerns about who would be responsible for distributing KI pills in the event of an emergency.

▶ **Read the two letters in full at source's URL.**

Worldwide deployments of nuclear weapons, 2014

By Hans M. Kristensen and Robert S. Norris
Source: http://bos.sagepub.com/content/early/2014/08/26/0096340214547619.full

As of mid-2014, we estimate that there are approximately 16,300 nuclear weapons located at some 97 sites in 14 countries. Roughly 10,000 of these weapons are in military arsenals; the remaining weapons are retired and awaiting dismantlement. Approximately 4,000 are operationally available, and some 1,800 are on high alert and ready for use on short notice (see Table 1).

Russia	8,000*
United States	7,300**
France	300
China	250
Britian	225
Israel	80
Pakistan	100–120
India	90–110
North Korea	<10
TOTAL	**~16,300**

*Approximately 4,300 of the Russian warheads are operational or in military custody. The remaining 3,700 warheads are thought to be excess warheads awaiting dismantlement.

**Approximately 4,760 of the U.S. warheads are in the military stockpile (about 1,980 deployed); 2,540 retired warheads are awaiting dismantlement.

Table 1. Estimated global nuclear weapons inventories, 2014

By far the largest concentrations of nuclear weapons reside in Russia and the United States, which possess 93 percent of the total global inventory (Kristensen and Norris, 2013a). In addition to the seven other countries with nuclear weapon stockpiles (Britain, France, China, Israel, India, Pakistan, and North Korea), five non-nuclear NATO allies (Belgium, Germany, Italy, the Netherlands, and Turkey) host about 180 US nuclear bombs at six air bases. (For a

listing of all the sites worldwide, see Table 2; it includes sites where there is reason to believe that nuclear weapons are deployed or stored.)[1]

	Saint-Dizier AB	Champagne-Ardenne	TNAs, ASMPAs, ALCMs	For Rafale K3 fighter-bombers. Might also store weapons for Rafale MK3 on Charles de Gaulle aircraft carrier based in Toulon NB.
	Saint-Jean, south of Ile Longue	Bretagne	TN75, (TNO from 2015)	Warhead storage site for M45 and M51 SLBMs at nearby SSBN base.
SUBTOTAL	6			
Germany	Büchel AB	Rheinland-Pfalz	B61-3/4	US bombs for delivery by German PA-200 Tornados of the 33rd Tactical Air Force Squadron. Weapons in custody of US 702nd MUNSS.
SUBTOTAL	1			
India	Chandighar Plant	Punjab	Various	Possible warhead production.
	Jodhpur facility	Rajasthan	Prithvi/Agni SSMs	Potential storage for Prithvi and Agni SSMs and warheads.
	Unknown Air Force storage facility[6]	Unknown	Bombs	For potential use by Jaguar IS at Gorakhpur and Lohegaon ABs and Mirage 2000H at Ambala and Gwalior ABs.
	Unknown Army storage facility[6]	Unknown	Prithvi/Agni SSMs	For use by 222nd and 333rd Missile Groups (Prithvi) and 334th and 335th Missile Groups (Agni).
	Unknown Navy facility[7]	Unknown	Dhanush SSMs	For Dhanush ship-launched SSMs.
SUBTOTAL	5			
Israel	Dimona site	?	Various	Negev Nuclear Research Center. Plutonium, tritium, and warhead production.
	Sdot Micha missile base	?	Jericho II SSMs	25–50 mobile MRBMs in caves. Warheads potentially on base or at Tirosh depot.
	Soreq Nuclear Research Center	?	Various	Possible warhead design, fabrication, and maintenance.
	Nevatim AB	?	Bombs	For potential use by F-16A/B fighter-bombers. Bombs potentially at base or remote depot.
	Tel Nof AB	?	Bombs	For potential use by F-16Is and F-15I fighter-bombers. Bombs possibly on base or remote depot.
SUBTOTAL	5			
Italy	Aviano AB	Friuli-Venezia Giulia	B61-3/4	For delivery by US F-16s of the 31st Fighter Wing.
	Ghedi Torre AB	Lombardia	B61-3/4	US bombs for delivery by Italian PA-200 Tornados of the 6th Fighter Wing. Weapons in custody of US 704th MUNSS.
SUBTOTAL	2			
Netherlands	Volkel AB	Noord-Brabant	B61-3/4	US bombs for delivery by Dutch F-16s of the 1st Fighter Wing. Weapons in custody of US 703rd MUNSS.
SUBTOTAL	1			
Pakistan	Khuzdar Depot	Balochistan	Various	Potential underground weapons storage.
	Masroor Depot (Karachi)	Sindh	Various	Potential storage of bombs for Mirage Vs at Masroor AB and warheads for SSMs.
	National Defense Complex (Fatehjang)	Punjab	SSMs	SSM launcher assembly and potential warhead storage.
	Sargodha Depot	Punjab	Various	Possible storage site of bombs for F-16s at nearby Sargodha AB and warheads for SSMs.[8]

(continued)

United States

The United States today stores nuclear weapons at 18 sites, including 12 sites in 11 states in the United States and another six sites in five European countries.[2] At the end of the Cold War, the United States maintained thousands of nuclear weapons outside of its borders on land and on the high seas.[3]

Since our previous estimate in 2009, the United States has further consolidated its nuclear weapons into fewer sites. Most significant is the apparent termination of nuclear weapons storage at Nellis Air Force Base in Nevada, which only a decade ago contained one of the world's largest concentrations of nuclear weapons. Similarly, nuclear weapons have been removed from Barksdale Air Force Base, one of three remaining heavy bomber bases,[4] and from all tactical fighter-bomber bases in the continental United States. All Air Force nuclear warheads are now stored at five locations: three intercontinental ballistic missile (ICBM) bases (F. E. Warren, Malmstrom, Minot), two bomber bases (Minot, Whiteman), and one central storage facility, Kirtland Underground Munitions Storage Complex (KUMSC).

The last naval non-strategic nuclear weapon system—the Tomahawk land-attack cruise missile (TLAM/N)—was eliminated in 2012. The weapons were stored at the Strategic Weapons Facilities at Bangor in Washington and at Kings Bay in Georgia, the only two remaining naval nuclear weapons storage sites.

The United States is the only nuclear-armed state that deploys nuclear weapons in other countries. Approximately 180 non-strategic nuclear bombs are stored in underground vaults beneath 87 aircraft shelters at six bases in five European countries (Belgium, Germany, Italy, the Netherlands, and Turkey) for delivery by US and NATO fighter-bombers.

Russia

There is considerable uncertainty about the number of Russian nuclear weapons storage sites, for several reasons. First, the Russian government provides almost no information about its nuclear warhead storage program. Second, Western governments say very little about what they know.[5] Moreover, estimates vary on what constitutes a "storage site;" some count each fenced storage bunker as a site, even though there may be several individually fenced bunkers within a larger storage complex.

We count each storage complex as one site or storage location and estimate that Russia today stores nuclear weapons permanently at 40 domestic locations. This is a slight reduction from our 2009 estimate, but a significant reduction from the 100 sites in the late-1990s, 250 sites in the mid-1990s, and 500 sites in 1991.[6]

Although the Russian government provides almost no public information about its nuclear weapons storage program, it has occasionally made declarations. For example, at the 2010 Non-Proliferation Treaty Review Conference, Russia declared that "the total number of nuclear weapons storage facilities has been reduced fourfold" since 1991 (Russian Federation, 2010a: 8). At the same event, the Russian delegation distributed a publication stating that "[a]ll Russian non-strategic nuclear weapons are concentrated in centralized storage bases exclusively ob [sic] the national territory" (Russian Federation, 2010b: 14). Moreover, twice a year under the terms of New START, the Kremlin hands over a detailed list of its strategic force deployments to the US government. Unfortunately, the list is secret.[7]

There is also uncertainty about the status of many nuclear weapon systems, including what constitutes "non-strategic" weapons. For example, medium-range Tu-22M3 Backfire bombers are sometimes described by Russians as more than tactical, but they are not considered strategic in arms control agreements signed by Russia. Consequently, this notebook considers the Tu-22M3 and all other weapons not covered by New START to be non-strategic and to be covered by the Russian declarations that all non-strategic nuclear warheads have been placed in central storage.

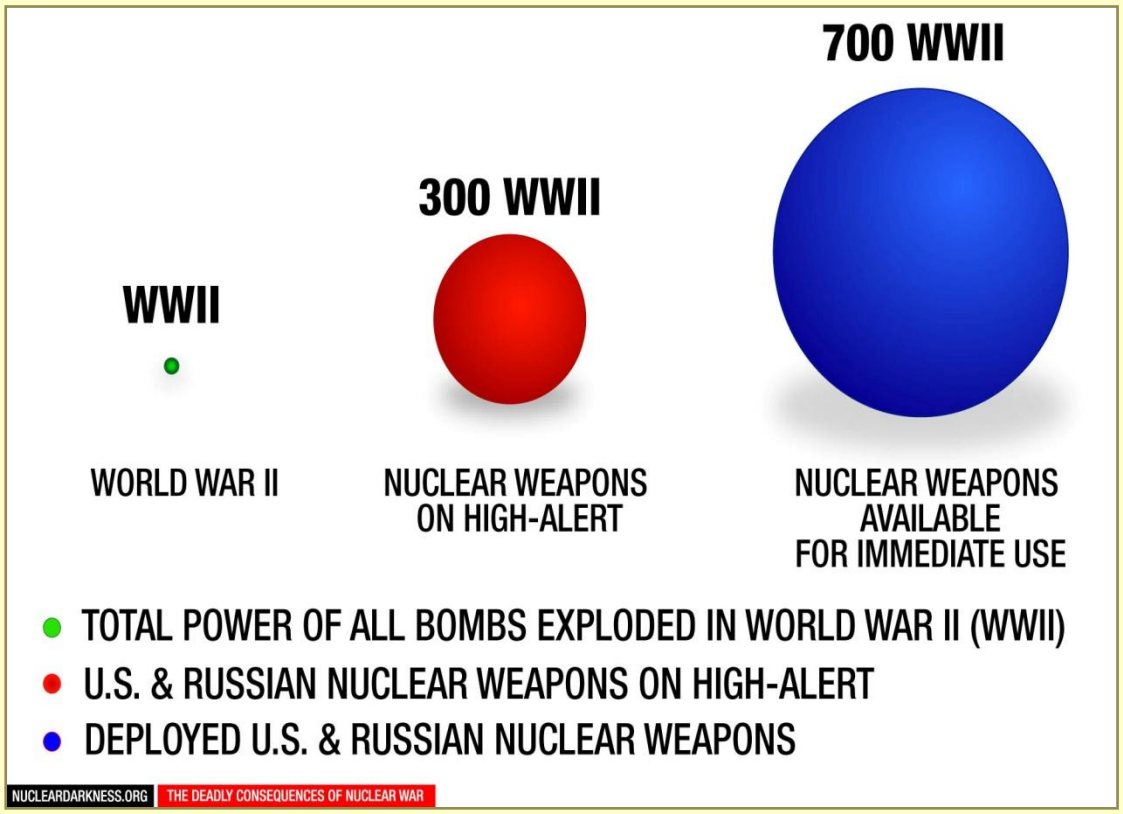
Russian permanent nuclear weapon storage locations fall into three main categories: operational warheads at Strategic Rocket Force, navy and air force bases; non-strategic and reserve/retired warheads at national-level storage sites; and warheads at assembly/disassembly factories.[8]

The storage locations for operational warheads include 11 ICBM fields and garrisons, two nuclear submarine bases, and two heavy bomber bases.[9] The national-level storage sites include 12 separate storage sites, although the status of a few of these is unclear. The warhead production complexes also have warhead storage facilities.

Britain and France

London and Paris have reduced the size of their arsenals and limited where their weapons are deployed. Britain only has one type of nuclear weapon, the Trident II submarine-launched ballistic missile (SLBM). The missiles and associated warheads are located at

two facilities in Scotland, although warheads are also serviced at two factories southwest of London.[10] France has retained two types of nuclear weapons: SLBMs at a submarine base in Bretagne and air-to-surface missiles for land- and carrier-based aircraft. France also has a warhead production and maintenance complex at Valduc. We estimate the French warheads to be at six locations.[11]



China

Researching Chinese nuclear weapons storage is difficult given the almost complete official secrecy that surrounds China's nuclear forces. Moreover, as is the case with other nuclear-armed states, Western governments say very little about what they know.[12]

Even so, important new information has become available from other sources since our previous estimate was made in 2009. This includes more satellite images on Google Earth that allow the public to monitor developments of Chinese forces. Moreover, a number of publications by Mark Stokes at the Project 2049 Institute have made invaluable new information and analysis available to the public.

One of Stokes's reports describes China's central underground nuclear weapons storage site near Baoji in the western part of Shaanxi province in central China (Stokes, 2010). China's use of underground facilities to conceal and protect military equipment and provide leadership and civil defense shelters has been reported for many years but gained new attention in 2011 due to a Georgetown University study (Karber, 2011).

We cautiously estimate that China may have nuclear warheads at 12 facilities. Nearly all of China's 250 nuclear warheads are concentrated in the central nuclear weapons storage site, known as 22 Base. The Second Artillery missiles intended to deliver these warheads are dispersed across China at approximately 25 brigade bases organized under six Base Headquarters. Each of these Base Headquarters probably has a small number of nuclear warheads in regional storage sites.

The navy has two bases with nuclear-capable missile submarines, each of which might have an adjacent warhead storage facility. The Air Force has a couple of intermediate-range bomber bases that might have a secondary nuclear mission. China has also started deploying ground-launched cruise missiles that US Air Force intelligence characterizes as nuclear-capable.[13]

China has a small number of warhead design, production, and maintenance facilities, presumably with a small number of warheads present.

Pakistan

Islamabad is quantitatively and qualitatively increasing its arsenal and deploying weapons at more sites, yet the locations are difficult to pinpoint. For example, no reliable public information exists on where Pakistan produces or stores its nuclear weapons. Thus, we have used commercial satellite images, expert studies, and local news reports and articles to make the assumption that nuclear weapons are likely to be at, or near, wherever nuclear-capable weapon systems are deployed. Based on this work, we cautiously estimate that Pakistan stores nuclear weapons at seven locations.

Pakistan has a rapidly expanding nuclear arsenal of 100 to 120 warheads and an increasing portfolio of delivery systems.[14] Pakistan's nuclear weapons are not believed to be fully operational under normal circumstances. We have found no credible information that identifies permanent nuclear weapons storage locations, but there are a few clues.

Former Secretary of State Hillary Clinton told Congress in 2009 that Pakistan's nuclear weapons "are widely dispersed in the country." She said the weapons "are not at a central location" but that Pakistan has "adopted a policy of dispersing their nuclear weapons and facilities" (Clinton, 2009). Senior US officials subsequently said that most of the Pakistani nuclear arsenal was south of Islamabad.[15] One of our suspected sites is the Masroor depot near Karachi.

Former President Pervez Musharraf reportedly told Seymour Hersh of *The New Yorker* that Pakistan had constructed a huge tunnel system for the transport and storage of nuclear weapons. "The tunnels are so deep that a nuclear attack will not touch them," he said, adding that it was impossible to monitor the movements of nuclear components by satellite (Hersh, 2009). One potential underground facility is near Tarbala in northern Pakistan.

India

As with Pakistan, we have found little reliable information that indicates where India's nuclear warheads are stored. Based on available unclassified sources and satellite imagery, we cautiously estimate that India stores nuclear weapons at five locations.

India is thought to keep its nuclear warheads and bombs in central storage locations rather than on bases with operational forces. Yet India is putting the final touches to its first nuclear submarine, to be able to deploy a secure second strike capability. One of the key questions is whether India will begin to deploy nuclear weapons on its subs under normal circumstances. Although not yet on our list (because it is not complete), the first submarine base is under construction near Rambilli in Andhra Pradesh on the Indian east coast.[16]

Israel

Israel is a wild card because of the opacity of its nuclear weapons program. Like other nuclear-armed states, however, Israel has been modernizing its nuclear arsenal and probably also its storage facilities. Israel's nuclear weapons are not believed to be fully operational under normal circumstances, but are estimated to include 80 to 85 warheads.[17] We estimate that Israel might store nuclear warheads at five locations.

North Korea

Although North Korea has conducted three nuclear tests, we are not aware of credible public information that North Korea has weaponized its nuclear weapons capability, much less where those weapons would be stored. We also take note that a 2013 US Air Force intelligence report did not list any of North Korea's ballistic or cruise missiles as nuclear-capable (US Air Force, 2013).

▶ **Notes and references are available at souce's URL.**

Scottish independence could leave UK nuclear weapons homeless

By James McKeon

Source: http://thebulletin.org/scottish-independence-could-leave-uk-nuclear-weapons-homeless7395

On September 18, the residents of Scotland will determine whether to remain in the United Kingdom or become independent for the first time since 1707.

On the surface, this referendum seems to only affect those living in the United Kingdom, but a more detailed look reveals an issue of significant international importance—the future of Great Britain's nuclear deterrent.

The Scottish independence debate has been fiercely fought on both sides since First Minister of Scotland Alex Salmond and his Scottish National Party won the Scottish Parliamentary elections in 2011 on a platform that promised to hold an independence referendum. Accepting the democratic legitimacy of the election, British Prime Minister David Cameron and his government said they would allow the referendum to occur, pledging to respect the vote regardless of outcome.

Cameron and his Conservative Party are opposed to Scottish independence, as are the two other major UK political parties, Labor and the Liberal Democrats. The three political parties formed a coalition—Better Together—that is united in its opposition to Scottish independence, even though they have divergent views on other issues. Another policy all three parties agree upon, albeit with extreme hesitance from the Liberal Democrats, is the need for a nuclear deterrent in Britain. This is where the independence vote gets tricky.

Since the mid-1990s, the UK Trident program has been the only nuclear deterrent in Britain's arsenal and its successor is scheduled to enter service in 2028. Here's the issue: All active **Vanguard** submarines and accompanying **Trident** nuclear weapons are stationed at **Her Majesty's Naval Base Clyde in Scotland** (photo). The Scottish government, led by Salmond, has pledged to safely remove and permanently ban nuclear weapons from Scottish territory within the first term of a newly independent parliament.

To be sure, the polls are not currently in favor of independence. It could happen, though, and if it does, Scotland will remove Trident nuclear weapons that have no destination in what will remain of the United Kingdom. The UK government and Ministry of Defence have repeatedly argued that they believe Scots will vote against independence, and thus Britain is not preparing for the possibility of Scottish disarmament. But it is risking a tricky situation: unilateral disarmament of the British Isles.

In addition to rejecting a backup plan for independence, the Ministry of Defence has said that removing Trident to the English coast would be extremely difficult and abhorrently costly. Great Britain has thus staked out its position as having no fallback, arguing that even if one did exist, it would be a logistical and financial nightmare. This would be all well and good—if the Scottish government was not especially clear that it will remove the weapons as quickly and safely as possible after independence. With Scotland at that point an independent state, the remaining United Kingdom would have no legal authority to prevent this from happening.

If moving Trident nuclear weapons to England would be that much of an ordeal, only one realistic alternative exists. That would be to place them in Kings Bay, Georgia, in the United States, where Britain already stores and maintains some nuclear warheads, thereby disarming the British Isles altogether. But this situation wouldn't really be necessary. Multiple analysts—including Malcolm Chalmers of the respected think tank the Royal United Services Institute and Francis Tusa of the newsletter Defence Analysis—

have suggested that the entire Trident system could be moved to England relatively quickly and at an affordable cost. So why is the Ministry of Defence arguing that any move would be catastrophic? The answer is simple: politics.

The UK Government is not encouraging the Ministry of Defence to acknowledge or publish a backup plan for independence because it is sticking with its policy of "no pre-negotiations." This might be a good line for those opposed to the Scottish National Party, but talking points are not enough for the severity of any situation involving nuclear weapons. It is almost laughable that the government of one of the most powerful nations on Earth is trying to dismiss its opposition by keeping the fate of some of the most powerful weapons on Earth uncertain.

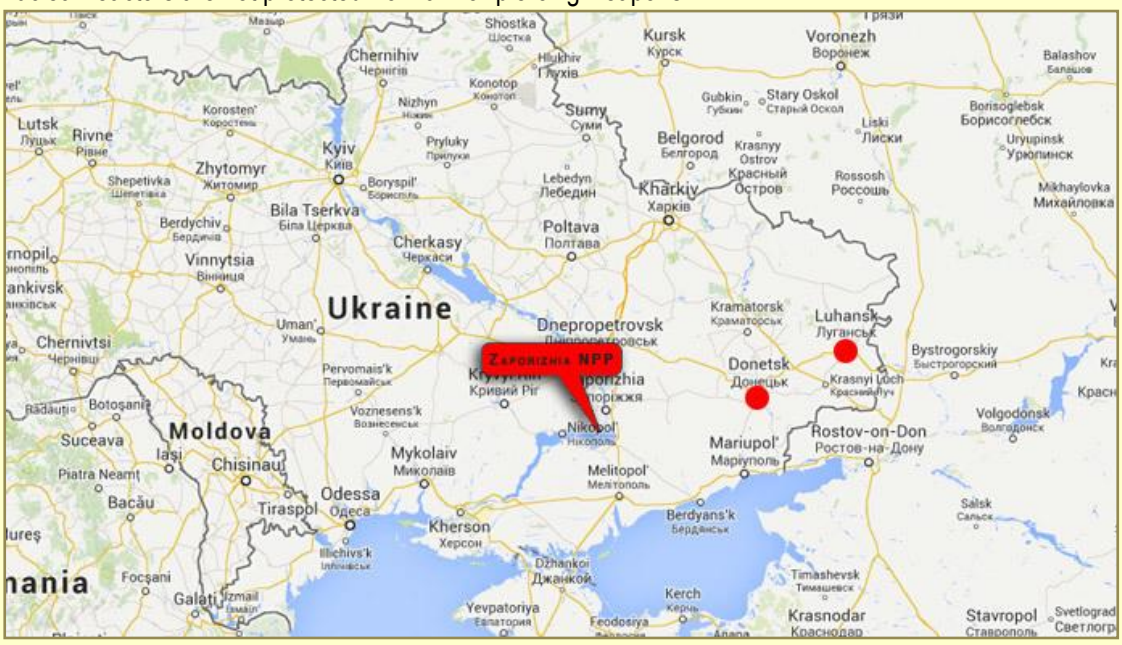
Right now, the choice is clear. Britain must stop playing games and acknowledge or publish a backup plan for its Scotland-based nuclear weapons, even if it has to be heavily redacted for national security purposes. Most of the independence debate has been caught up in political maneuvering. But the UK government must stop using nuclear weapons as political pawns.

***James McKeon** is a Herbert Scoville Jr. peace fellow at the Stimson Center's Managing Across Boundaries program.*

Ukrainian nuclear plant vulnerable to Kiev's artillery

Source: http://rt.com/news/184004-greenpeace-zaporizhia-npp-danger/

August 31 – Europe's largest nuclear power plant is vulnerable to 'direct bombardment' in Ukraine if caught in the conflict, a Greenpeace nuclear energy expert told a German newspaper, claiming that its nuclear reactors are not protected from armor-piercing weapons.



Greenpeace nuclear expert Tobias Münchmeyer revealed his concerns over the six-reactor Zaporizhia Nuclear Power Plant in eastern Ukraine to Westdeutsche Allgemeine Zeitung. **He said the plant was insufficiently protected against a direct bombardment and that 1.2-meter thick reinforced concrete shells surrounding each reactor are strong enough to withstand only a small aircraft crash.**

"There are many armor-piercing weapons in the region, which could penetrate these protective covers," Münchmeyer said, as cited by Deutsche Welle on Saturday.

The Soviet design reactors at Zaporizhia are largely dependent on Russian expertise and spare parts, the expert also said.

Zaporizhia is the largest nuclear power plant (NPP) not only in Ukraine, but also in Europe and also the fifth largest NPP in the world. It is situated on the bank of the

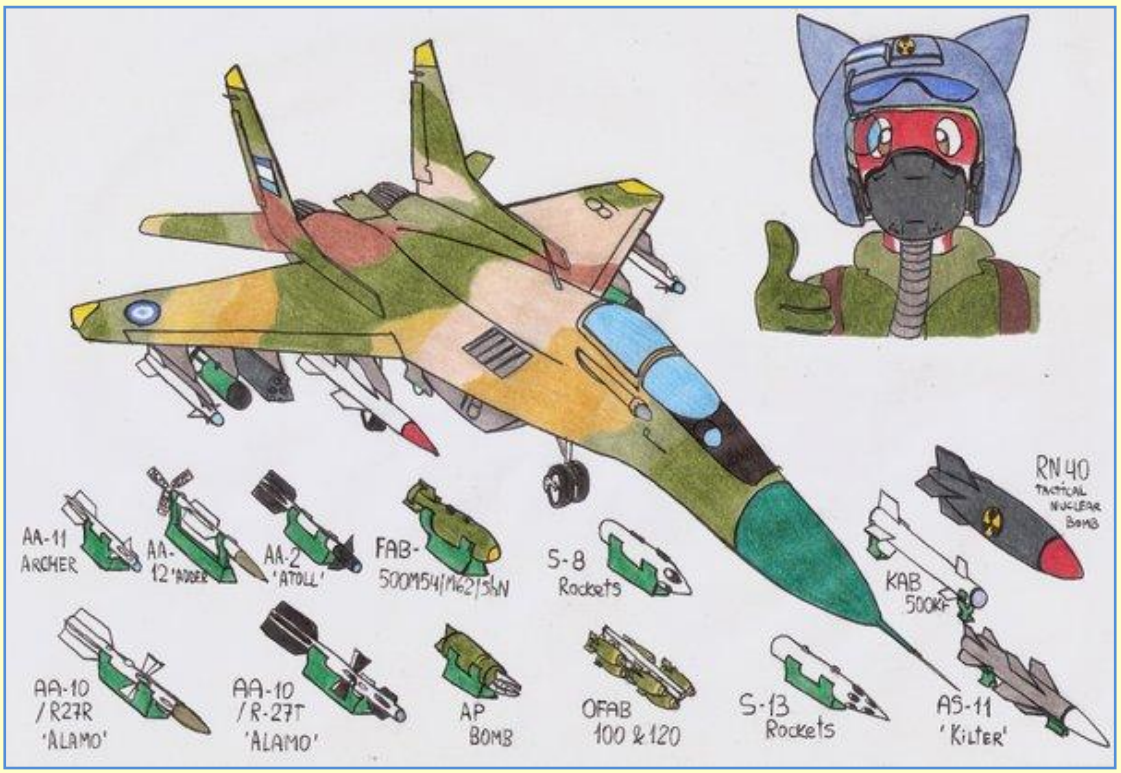
Kakhovka water reservoir on the Dnieper River. This is some 200 kilometers from the warzone in Donetsk region.

The plant's six VVER-1000 pressurized light water nuclear reactors with nominal capacity of 1000 MWe generate 40-42 billion kWh per year each. This accounts for one-fifth of the average annual

electricity production in Ukraine and almost 47 percent of electricity generated at Ukrainian nuclear power plants.

The website of the Zaporizhia Nuclear Power Plant maintains that the station can withstand an earthquake of up to 7 on the Richter scale. The station is guaranteed to withstand an explosion of five tons of TNT blown up 200 meters from the facility – such an explosion would completely eliminate a city block.

As for sustaining an impact of the "small aircraft" mentioned by the Greenpeace expert, the nuclear facility's website says that according to the project, Zaporizhia NPP could in fact sustain **a direct hit of**



a frontline tactical fighter Mig-29, which someone might consider a small one, yet not as small as it might appear from Greenpeace expert's evaluation.

While it is impossible to expect direct bombardment of a nuclear plant, especially in Ukraine which saw the 1986 Chernobyl disaster, attempts to break into the Zaporizhia Nuclear Power Plant have already taken place.

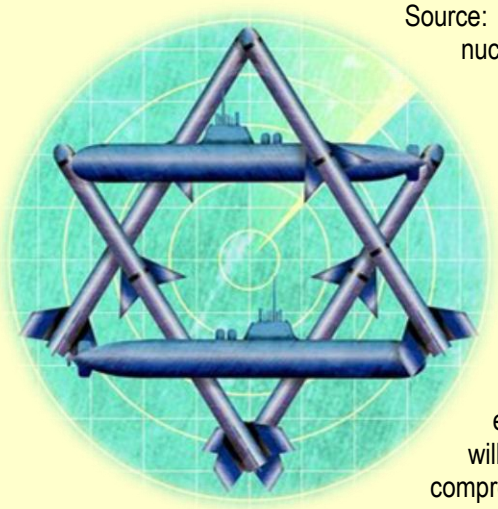
In May, Ukrainian police prevented a group of armed men from entering Europe's largest nuclear power plant. The men said they were members of the Right Sector group, though their intensions remained vague.
Now Right Sector, which praises neo-Nazi ideology, does not need to break into a nuclear power plant. The National Guard, whose core includes Right Sector members, has been assigned by Kiev to guard all country's nuclear objects, nuclear fuel and nuclear waste, along with national missile and space booster production.
A law enabling the National Guard to protect nuclear energy industry facilities and other security-sensitive installations was published on Kiev government's official website on August 13.

EDITOR'S COMMENT: Just a short question: we suppose that the Mig-29 (Fulcrum E) would be ***without*** its weapons? … [photo above]

A sea-based nuclear deterrent for Israel

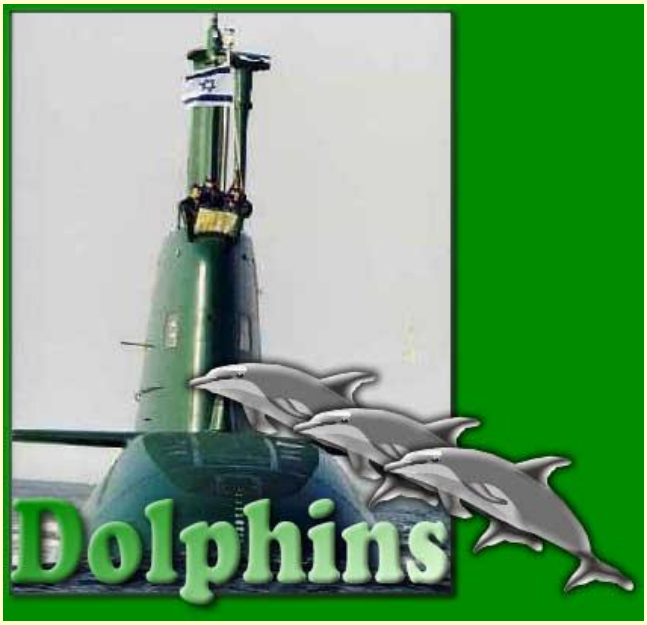
By Louis Rene Beres and Leon Edney

Source: http://www.washingtontimes.com/news/2014/sep/5/beres-edney-a-sea-based-nuclear-deterrent-for-isra/



September 05 – For Israel, an overriding long-term security requirement must be to deter future attacks with weapons of mass destruction (WMD) by enemy states, especially Iran. Israel will need to fashion a comprehensive and calibrated strategic doctrine that identifies and correlates all available options (deterrence, pre-emption, active defense, strategic targeting and military use of nuclear weapons) with enumerated national-survival goals.
The challenges of an Israeli nuclear-deterrence posture needs discussion, with special reference to twin requirements of perceived ability and perceived willingness. Before any rational adversary could be deterred by an Israeli nuclear threat, that enemy would first need to believe that Israel had both the capacity to launch a nuclear-weapons response for any WMD aggression, and also the will to take such an action. Where it is facing a prospectively irrational strategic enemy, Israel's deterrence posture would then need to be based upon credible pre-emptive capabilities.
Since its statehood was formally established following World War II, Israel has experienced many periods of intensive rocket and mortar attacks launched intentionally against its cities. In response, with significant American financial support, Israel developed and deployed the Iron **Dome system**. **David's Sling** would defend against the midrange rocket and missile threat; **Arrow,** against the longer-range, higher-lethality WMD ballistic-missile threat.
During Operation Protective Edge, Iron Dome performed with distinction. In this Gaza War conflict, a less than 100 percent reliability of intercept was judged acceptable. Still, nothing less than a 100 percent reliability of intercept could be tolerable when facing enemy nuclear missiles. The prospective task for Arrow, in any possible future encounters with long-range Iranian ballistic missiles, would be far more complex and demanding.
Israel has always understood the critical need to develop a "great equalizer," which became its undisclosed nuclear-weapons posture. Doctrinally, Israel has plausibly rejected any notions of nuclear war-fighting; nonetheless, there are still some circumstances where an Israeli nuclear response could be the sole rational option. In any event, nuclear exchanges between Israel and particular enemies could fall under the following comprehensive possibilities: First, enemy-state first strikes launched against Israel would not destroy Israel's second-strike nuclear capability; second, enemy-state retaliations for an Israeli conventional pre-emption would not destroy Israel's nuclear counterretaliatory capability; three, conventional Israeli pre-emptive strikes would not destroy enemy-state second-strike nuclear capability; and

fourth, Israeli retaliations for enemy-state conventional first strikes would not destroy



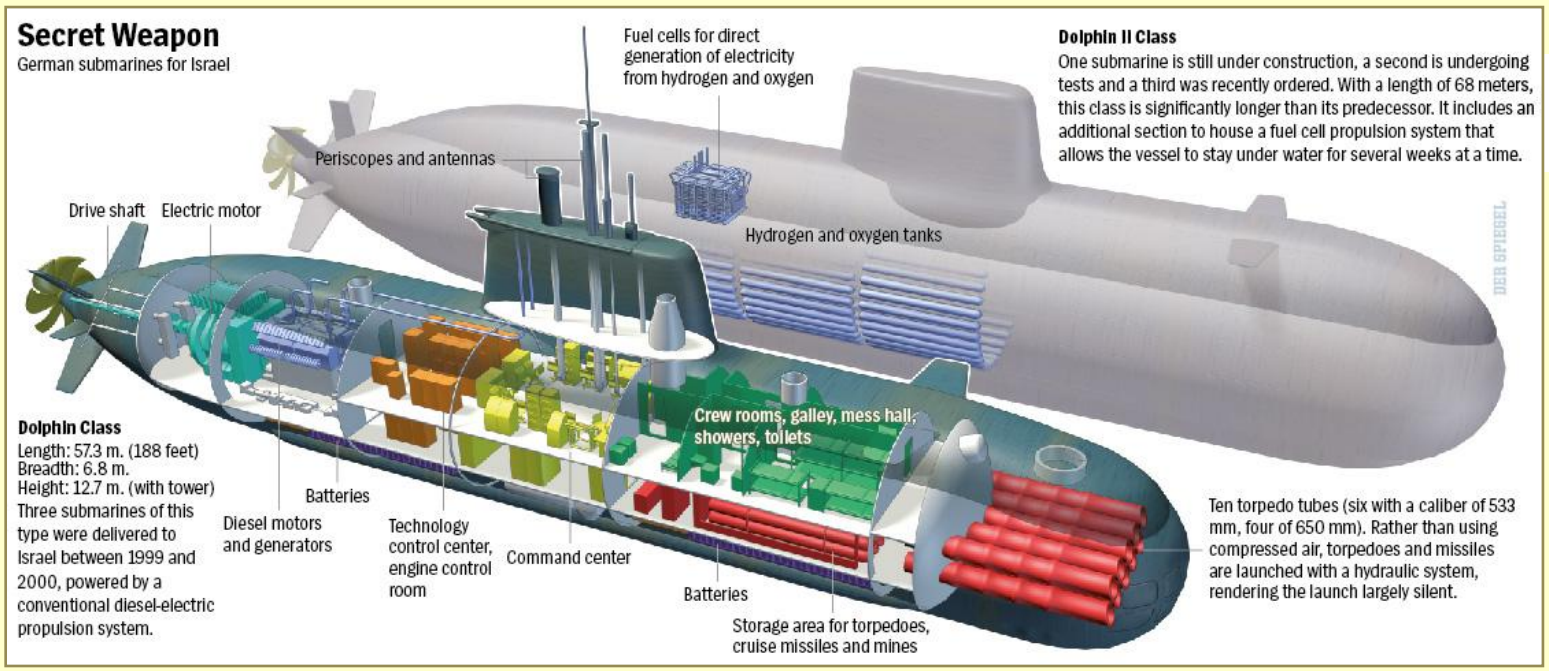
enemy-state nuclear counterretaliatory capability.

What this means is that Jerusalem must take appropriate steps to ensure the plausibility of the first and second possibilities above, and also the implausibility of the third and fourth.

This brings us to sea-basing. Submarines are the ultimate stealth weapon. A small Israeli submarine-launched ballistic-missile force could essentially guarantee the ability to unleash a catastrophic retaliatory strike for any pertinent threat situation. Owing to Israel's inherent lack of strategic depth, a submarine element with nuclear-weapons capability would best represent an assured capacity to utilize Ben-Gurion's "Great Equalizer" as a core element of its strategic deterrence.

Israel is upgrading its three Dolphin I submarines, purchased from Germany, with three additional Dolphin II boats. These diesel-powered submarines have been designed and built for specific Israeli requirements, and are larger than the German Type 212 submarines. The larger size may be to most suitably accommodate the "Great Equalizer."

It is not sufficient that enemies will merely acknowledge Israel's nuclear-weapons status. Israel's enemies must also realize that Israel has secure nuclear weapons, and that it would be ready and willing to employ these weapons should the survival of the state be at evident risk. This could require Israel, at some point, to consider a selective loosening of its "deliberate nuclear ambiguity."



Israel cannot reasonably assume that its enemies will remain non-nuclear. There is, moreover, a plausible prospect that hatred and religious fanaticism could sometime lead to one form or another of nuclear exchange. Among other core elements of an enhanced Israeli nuclear strategy, a more fully acknowledged Israeli submarine-based nuclear-weapons retaliatory capability

could help prevent this plainly intolerable form of international conflict.

__Louis Rene Beres__ is professor of political science and international law at Purdue University.
__Retired U.S. Adm. Leon Edney__ is a former vice chief of Naval Operations; NATO supreme allied commander, Atlantic; and commander in chief, U.S. Atlantic Command.

No Fukushima radiation found in California's coastal areas

Source: http://www.homelandsecuritynewswire.com/dr20140908-no-fukushima-radiation-found-in-california-s-coastal-areas

September 08 – It was raining when Eric Norman, Berkeley Lab physicist and University of California (UC) Berkeley professor of Nuclear Engineering, heard about the nuclear-reactor meltdown in Fukushima, Japan. "I immediately thought of Chernobyl," he says, referring to the "**nuclear rain**" that fell in the days that followed the 1986 disaster in Ukraine.

Norman wanted to know whether, following the 11 March 2011 Fukushima breach, radioactivity could be found in Bay Area precipitation. He and his students collected weeks' worth of rainwater around Berkeley Campus to find out.
A Berkeley Lab release reports that the results were: low levels of a number of different radioactive nuclei produced by the fission of uranium-235 including, cesium-134, cesium-137, and iodine-131 (the number after the element represents the total number of protons and neutrons in the atom's nucleus). "The levels we saw were detectable, but low and not a health hazard to anyone," Norman says. With findings in hand, he informed the local media that there was nothing to worry about, he says, and did his best to stress the lack of dangerous radioactivity in the rainwater.

Fast-forward a couple years. "I thought that was the end of it until I started seeing reports on the Internet and elsewhere," he explained at last month's 2014 meeting of the American Chemical Society in San Francisco, California. People were again concerned about health hazards caused by the radiation.
"I think part of the reason for that was there were reports of continuing leaks and releases of radioactivity — it wasn't just a one-time thing — and people began to think of the idea of

radiation being transported across the Pacific, which of course will happen," Norman says. "I don't know where they got the numbers, but they were claiming very high numbers that were causing health effects on people especially children."
Norman didn't immediately dismiss these new claims, but he could not find any up-to-date measurements of environmental radiation. So he decided to conduct his own study. In 2013, he and his students tested radiation levels in fish, plants, milk, seawater, and salt from a variety of locations throughout the Pacific Ocean and coastal regions.
They compared the ratio of radioactive isotopes in the new samples to a sample Norman had collected years before: about a month after the Fukushima disaster, he noticed his backyard weeds had grown high from all the rain. Upon testing these

weeds he found extremely low but detectable levels of cesium-134 and cesium-137, still well below limits for safety and health concerns.

If any of the new samples contained these two isotopes in the same ratio as that of the weeds from 2011, it would indicate the presence of Fukushima radiation.

With the help of Al Smith, physicist at Berkeley Lab and one of the world's experts on background gamma ray counting, and Keenan Thomas from UC Berkeley, the team analyzed and interpreted the results. They especially expected to find at least some cesium isotopes in the seaweed since it concentrates potassium, an element that's in the same column of cesium on the periodic table. "We looked very hard," Norman says. The scientists sampled their fish, seaweed, and other Pacific products from Hawaii, the Philippines, the West Coast areas, and Japan. But none of these samples showed any indication of radiation from Fukushima, Norman says.

Why were radiation levels in these samples so low? "Many radioactive isotopes we saw in the rain water were very short lived," Norman explains. Iodine-131, for instance, has a half-life of just eight days. Additionally, dilution from ocean water plays a significant role. "We're a long way from Japan and there's a lot of water in the Pacific," he says. "Whatever gets dumped in the ocean will get diluted by enormous factors."

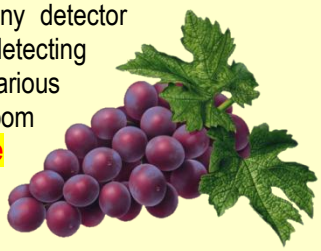
Even so, Norman and his team continue to test samples so that they'll have up-to-date data to counter any scare claims of Fukushima radiation. Recently he's grown grapes in his yard and analyzed leaf samples. **The isotope levels from his backyard flora, so low to begin with in 2011, have now completely faded away**.

— Read more in Eric B. Norman et al., "Observations of Fallout from the Fukushima Reactor Accident in San Francisco Bay Area Rainwater," PLOSOne *(21 September 2011) (DOI: 10.1371/journal.pone.0024330); A. R. Smith etal., "Measurements of Fission Products from the Fukushima Daiichi Incident in San Francisco Bay Area Air Filters, Automobile Filters, Rainwater, and Food,"* Journal of Environmental Protection *5, no. 3 (2014): 207-21*

New device improves radiation detection

Source: http://www.homelandsecuritynewswire.com/dr20140908-new-device-improves-radiation-detection

In a move that could have huge implications for national security, researchers have created a very sensitive and tiny detector that is capable of detecting radiation from various sources at room temperature. **The detector is eight to nine orders of magnitude —100 million to as high as 1 billion — times faster than the existing technology,** and a Texas A&M University at Galveston professor is a key player in the discovery.



Luke Nyakiti, assistant professor in marine engineering technology and Materials Science and Engineering at Texas A&M University at Galveston, is part of the research team that has had its work published in the current issue of Nature Nanotechnology.

A Texas A&M release reports that Nyakiti and colleagues from the University of Maryland, the University of Massachusetts, the U.S. Naval Research Laboratory and Monash University in Australia fabricated the tiny photothermoelectric detector following successful growth of graphene at the Naval Research Laboratory in Washington, D.C. The project was funded by the office of Naval Research and the National Science Foundation.

The team's goal was to utilize the exceptional electronic carrier properties of graphene to create a photo detector device that could detect radiation at room temperature with the fastest response, which previously has been extremely difficult to do. **The researchers used a two-dimensional material called graphene that is made of carbon atoms that are arranged in a honeycomb-like geometrical structure (the diameter of a human hair is 300,000 times thicker than a two-dimensional sheet of graphene).**

Graphene was chosen because it conducts electricity with ease, it is

nearly transparent, and it is remarkably strong (100 times stronger than steel). Also, it is very sensitive to energy absorbance.

"The problem before is that there has always been a 'slow response' when it came to detecting radiation in the terahertz frequency range, especially at room temperature, and the technology that currently exists operated at very cold temperatures, subsequently requiring supportive electronic systems that adds to the cost," Nyakiti explains.

He says the benefit of using this detector is that its signals do not pose a health hazard to the people using it. Also, besides the extremely high sensing speeds reported by the device, the team anticipates further improvements in sensing ability.

"We are very excited that our detector system provides a unique answer to fast, subtle detection capabilities that are a million to a billion times faster in its detection capability, without posing short-term or long term health hazards to those who are operating it," Nyakiti reports .

"It was indeed an exciting time for all of us when this happened. Because it is much more effective in detecting radiation, the device could be very promising for homeland security purposes. It also might have applications in mobile devices, medical imaging and other uses.

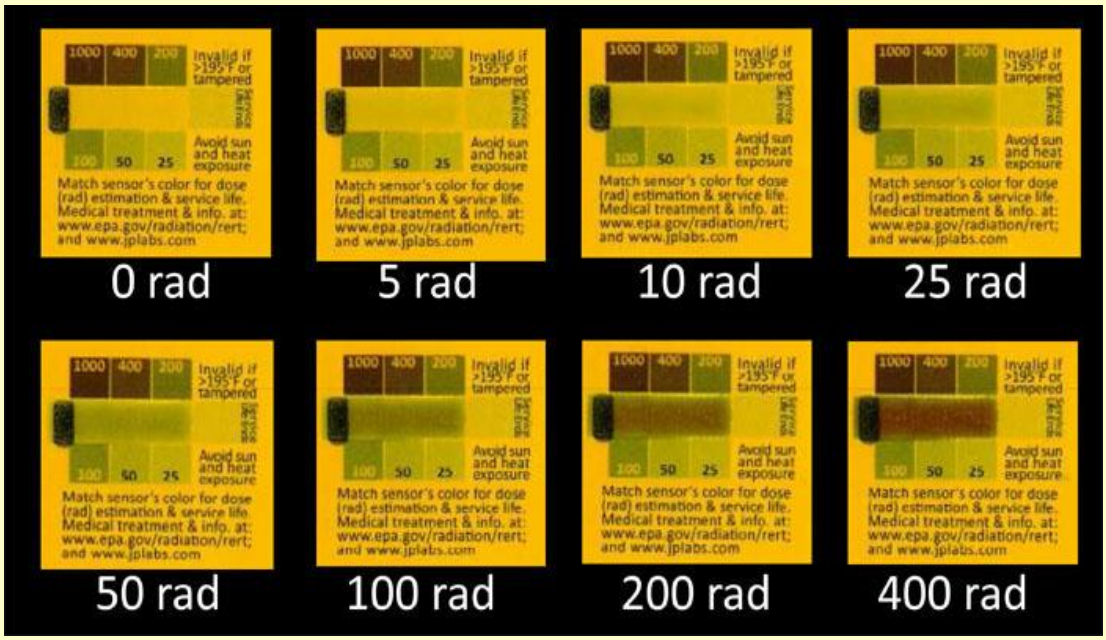
"This has the potential to open up other device possibilities in medical applications. This is a huge first step."

RADSticker™ - Emergency Radiation Exposure Detector

Source: http://thekeytosurvival.com/storetitles/terrorismfire/radsticker.html

In the event of a nuclear attack or radiological "dirty bomb" event:
HOW WILL YOU KNOW IF YOU ARE IN A SAFE AREA?
HOW WILL YOU KNOW IF YOU NEED TO MOVE TO A SAFER AREA?
HOW WILL YOU KNOW IF YOU NEED TO SEEK MEDICAL ATTENTION?

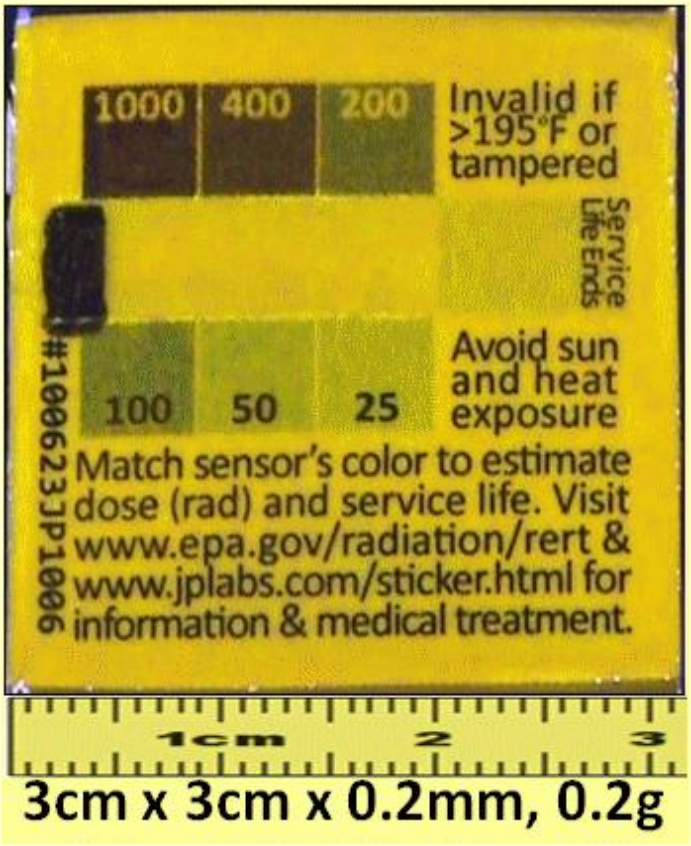
The RADSticker is a peel & stick, postage stamp sized, instant color developing dosimeter, which will



instantly tell you if you are in danger of a high radiation risk. It will always be ready and with you, 24/7, as it can be stuck onto the back of your drivers license or anything else that you keep close.

Since it is non electrical, it is impervious to an EMP attack situation. This rugged & reliable exposure detection meter will allow you to monitor yourself out of dangerous levels of radiation exposure. It will also allow medical personnel to determine levels of treatment, should you suddenly become exposed to a major radiological, nuclear or dirty bomb attack, nuclear power plant accident or any situation where radiation sources might be mishandled. The

RADStickers both quell public fear & panic and allows our First-Responders and medical resources to then focus where it is most urgently needed.



RADSticker can help you to minimize additional radiation exposure to as low as reasonably achievable, ideally, this is <100 rads, which can be 100% survivable for healthy adults, if not exceeded. "Very few of those receiving acute doses (received within 24 hours) of less than 100 R would become sick, even briefly." However, government agencies advise to try to limit your normal exposure to 5 rad per year and 25 rad for lifetime and emergency workers to 50 rad. (Limits lower for children & fetuses.)

In any future nuclear emergency, there will be many people that are not in harms way, but without knowing this, will worry needlessly or possibly even panic. Others, who *should* be rapidly moving to a safer area, will not know to do so, nor will they be able to confirm that it is indeed safer, without such specialized devices. The key to assuring that your family and others are safe, having moved to safer grounds, and knowing later to seek medical attention, is only possible if you have your own radiation detection dosimeter with you, at the time of emergency.

- Instant - Self Indicating Reading
- Inexpensive - Reliable
- Lightweight - Only .2 grams
- Monitors 1 - 1000 rads
- No batteries - always ready
- Pre calibrated - maintenance free
- Rugged -practically non destructible
- Shelf Life - 2-3 yrs. @ 77 degrees F
- 10 yr. shelf life if kept in freezer (keep till ready to carry)
- Humidity and Water Resistant
- Max operating temp - 195 degrees
- User Friendly

Abu Dhabi gets licence for third and fourth reactors at Barakah

Source: http://www.thenational.ae/uae/abu-dhabi-gets-licence-for-third-and-fourth-reactors-at-barakah#ixzz3DTVG3enZ

The construction licence for Abu Dhabi's third and fourth nuclear reactors at Barakah in the Western Region was granted on Monday, the Federal Authority for Nuclear Regulation (Fanr) said.

The Government body said it was also about to establish its resident inspection office at the site to ensure a continuous presence for the remainder of the construction.

"We look on this as a big milestone," said Dr William Travers, director-general of Fanr. "We put a lot of effort into the review.

"It follows on, and is complementary to, the review that we performed for units 1 and 2. It's another significant event because it really does represent one of the first times a so-called 'new entrant' country

embarking on its first nuclear power plant project has received a construction licence for nuclear power plant usage, so it's quite important."

Last month, Enec announced that more than 55 per cent of Unit 1 was complete.

"Today is an extension of a long effort to perform a very detailed technical assessment of the application that was provided by Enec in

March 2013," Dr Travers said.

"There's lots of follow-on to come. Inspection activities at the site are being performed by Fanr in connection with all four units. An important element in the licencing for a nuclear power plant is the fact that this is a two-step process, so while the construction licence is an important first step, it's not the last step."

The most important is the operating licence, which is yet to come.

"It's the point in time when all matters of regulatory significance, including safety and security, need to be resolved entirely," he said. "At the construction licence phase, some issues can be pending. So the construction licence is characterised as a final decision on the adequacy of the site to host another two units and it is a preliminary decision on the adequacy of the design of the units as they have been proposed by Enec."

This stage looks at issues that need to be resolved before they can start the safety-related construction of the plant.

"So we have high confidence that the design and site are adequate," said Dr Travers. "We look at many issues from a hydrological and seismic point of view, and check, for example, whether there is enough water to cool the reactors and whether there are issues like sandstorms that – if they were to be encountered – would create safety problems for the facility. We've come to a final determination that site is suitable and acceptable."

More frequent inspections will also take place.

"We're out there every other week with a team of people but we're just about to establish our resident inspection office at the site," he said.

Inspections will include important elements related to nuclear safety, such as correct implementation of the design, establishment of electrical feeds, equipment and a correct placement of the rebar, as well as further construction of the control room to support the operation.

The Environment Agency Abu Dhabi also undertakes inspections by looking at potential environmental effects that are not associated with radiation and radiological release.

"They might look at thermal discharge from the plants and how that might affect coral and sea life," Dr Travers said.

"We're obligated to look at the potential impact of any radiological releases both in the normal operational context, as well as theoretically postulating the possibility of an accident and what impact that might have. The site is viewed to be acceptable for those four units."

Fanr is expecting an application from Enec for an operating licence for units 1 and 2 within the next few months.

Hamad Alkaabi, the UAE Ambassador to the International Atomic Energy Agency, said the approval represented a green light for Enec to start the construction of reactors 3 and 4. "The UAE nuclear programme is well-recognised internationally for its transparency, fast-moving progress and strong safety framework. The project can now expand to the next phase."

A training programme was also launched on Monday by Enec and Abu Dhabi Polytechnic to develop a skilled Emirati workforce to support the UAE's nuclear energy industry. They will collaborate on a customised nuclear energy curriculum for students of Enec's Energy Pioneers scholarship programme.

Mohammed Al Hammadi, Enec's chief executive, said nurturing the next generation of nuclear energy leaders in the UAE was one of Enec's top priorities.

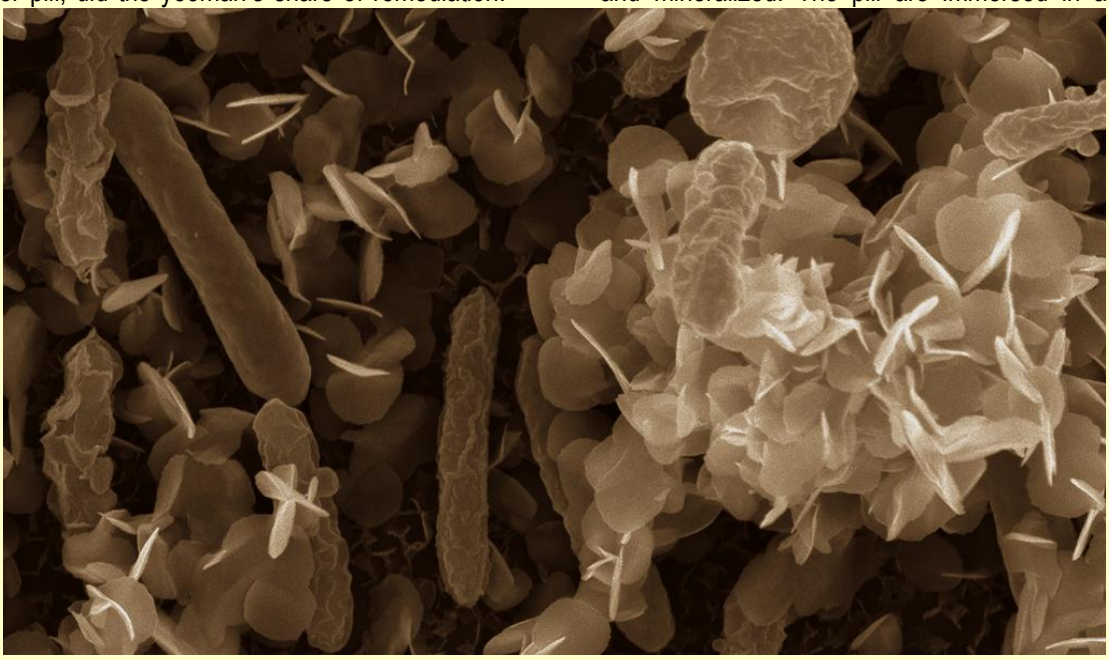
Strengthening the armor for nuclear-waste eating microbes

Source: http://www.homelandsecuritynewswire.com/dr20140916-strengthening-the-armor-for-nuclear waste-eating-microbes

A microbe developed to clean up nuclear waste and patented by a Michigan State University researcher has just been improved.

In earlier research, Gemma Reguera, MSU microbiologist, identified that Geobacter bacteria's tiny conductive hair-like appendages, or pili, did the yeoman's share of remediation, preventing the toxic material from leaching into groundwater.

Reguera's team had previously linked the conductive pili to the ability of the microbe to mineralize the soluble uranium. As the biofilm concentrates many nanowires around the Geobacter cells, more uranium can be bound and mineralized. The pili are immersed in a



By increasing the strength of the pili nanowires, she improved their ability to clean up uranium and other toxic wastes.

An MSU release reports that in new research, published in the current issue of *Applied and Environmental Microbiology*,

Reguera has added an additional layer of armor to her enhanced microbes.

The microbes also use the pili to stick to each other and grow a film on just about any surface, similar to the bacterial film that forms on teeth. The Geobacter biofilm, encased by a network of nanowires and slime, gives the bacteria a shield and increases their ability to neutralize even more uranium. The improvement also allows the bacteria to survive longer even when exposed to higher concentrations of the radioactive material.

Geobacter immobilizing uranium can be described as nature's version of electroplating. The beefed-up microbes engulf the uranium and turn it into a mineral, matrix of slime, which surrounds the biofilm cells and boosts the Geobacter's pili armor, so the biofilm now can pull double duty by helping mineralize uranium.

The shield keeps the uranium from penetrating deep into the Geobacter biofilm. By keeping this process on the surface of the film, the bacteria are not exposed to uranium and, as a community, they are able to clean up more toxic waste.

"The results surpassed our most optimistic predictions," Reguera said. "Even thin biofilms immobilized uranium like sponges. They reduced it to a mineral, all while not suffering any damage to themselves, for prolonged periods of time."

Even when exposed to extremely high and toxic concentrations of uranium, levels that would destroy individual Geobacter cells, the biofilms didn't just survive, they thrived, she added.

Reguera's future research on this front will focus on deciphering how the biofilm matrix that encases the cells shields them so effectively and how to improve its properties further.

— Read more in Dena L. Cologgi et al., "Enhanced uranium immobilization and reduction by Geobacter sulfurreducens biofilms," Applied and Environmental Microbiology *(15 August 2014)*

NETHERLANDS – Answers to parliamentary questions about concerns of British Defence Commission on threat of an EMP attack

Source: http://www.rijksoverheid.nl/ministeries/def/documenten-en-publicaties/kamerstukken/2012/04/04/beantwoording-kamervragen-over-zorgen-britse-defensiecommissie-over-dreiging-emp-aanval.html

Answers from Minister Hillen (DEF) to questions from MPs Hernandez and Kortenoeven (both PVV) about the news that MPs from the British Defence Committee are very concerned about the threat of an EMP attack (Electro Magnetic Pulse) for the national security of the United Kingdom.

EDITOR'S COMMENT: At the end of the source page there is a .pdf document with the questions and answers given. Open the document and then use Google Translate to translate it to English. I could have done that but I did not want to spoil the joy of discovering its contents by yourself! It is a genuine sample of thoughts from a representative of the generation "it will not happen to us!" ENJOY!

US Defenseless Against North Korean EMP Threat

Source: http://www.bignewsnetwork.com/index.php/sid/224901223

September 19 – **The electric grid in the United States remains largely unprotected, according to a longtime adviser to Congress on national security issues.**

Peter Vincent Pry told VOA he believes North Korea is ready to attempt a strike on the U.S. electric grid using an Electromagnetic Pulse (EMP). Pry said North Korea practiced an EMP strike against the U.S. last year when it orbited a satellite at the optimal altitude and trajectory to carry out such an attack.

Pry is in the northern city of Minneapolis to brief the National Council of State Legislatures this week on the EMP threat. He told VOA that three U.S. states - Arizona, Maine and Virginia - have passed legislation trying to guard against a lengthy power outage following an EMP.

Pry was a member of the former Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack

(2001-2008). He also is executive director of the Task Force on National and Homeland Security, a congressional advisory board dedicated to achieving protection of the United States from electromagnetic pulse and other threats.

An electromagnetic pulse (or disturbance) is a short burst of electromagnetic energy that can be natural or man-made. EMP interference generated by lightning, for example, can damage electronic equipment. At very high energy levels, an EMP can damage physical

objects such as trees, buildings and aircraft.

Pry said the North Korean test last year took place over the South Pole, which he called a strategic move.

"We are blind from the south. We don't have the Ballistic Missile Early Warning System or interceptors to protect us from the south," said Pry.

The congressional analyst said this was done after North Korea's third illegal nuclear test in February 2013 and after the country's leader, Kim Jong Un, threatened to strike the United States and its allies with a nuclear missile.

Re. Yvette Clark (D-N.Y.) said, "I cannot speak to the motives of the North Korean satellite experiment, but... we need to move with all deliberate speed to shore up our infrastructure."

A couple months later, a North Korean freighter, the Chong Chon Gang, was caught attempting to move through the Panama Canal with a cargo of nuclear capable missiles on their launchers. They were hidden under thousands of bags of sugar.

This was no mistake on the part of the North Koreans, Pry told VOA. He said he believes

Pyongyang was testing the United States to find out if it could traffic nuclear weapons through the Gulf of Mexico and the Panama Canal without detection. He said had the North Koreans gone the long way around South America, the U.S. never would have known what North Korea was shipping.

He said it was just by chance they were caught because no one was looking for nuclear missiles.

"We inspected the freighter not because anyone thought there were nuclear capable missiles onboard, but because this freighter is notorious for doing trade with drug cartels and terrorists, and so we were looking for illicit drugs that the freighter might be smuggling, and they found the nuclear capable missiles," said Pry.

Clark, who is the ranking member on the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, said "again, I cannot say whether it is a deliberate attempt by the North Koreans to test out or test run the capabilities of approaching the U.S." with nuclear capable missiles, but "they are looking for ways to approach the United States, and I am sure it is not for the sake of friendly trade, but to do our nation harm."

Clark, together with Rep. Trent Franks (R-A.Z.), tried to address the EMP threat in June 2013 when they introduced the Shield Act, which has stalled in the House Energy and Commerce Committee.

According to Pry, near the end of the Cold War, the Russians developed the technology for a super EMP. This is a class of nuclear weapon with a special design to produce a particularly powerful EMP field. **He says that in 2004 a delegation of Russian generals, including two of their top EMP experts, met with the EMP commission.**

"They told us proactively, lsquo, we have bad news. We developed this super EMP weapon, and during the post-Cold War brain drain, some of our scientists went to North Korea," he said.

At the time, Pry said, the Russian generals thought that within a few years, North Korea could develop a super EMP weapon.

A security threat calls for limited exposure of Israel's nuclear capabilities

Source: http://i-hls.com/2014/09/security-threat-calls-limited-exposure-israels-nuclear-capabilities/

"Israel must maintain its policy of nuclear ambiguity. Nevertheless, if, at some future point, Middle Eastern countries, notably Iran, shall develop nuclear technology which Israel would deem as a threat, then Israel should partially unveil its nuclear capabilities, as a deterrent". This is one of the main recommendations of the "Daniel Project" jointly established by security experts from Israel and the US in order to assess the threat to Israel's national security, posed by Middle Eastern countries, Iran in particular. The detailed, top secret recommendation of the "Daniel Project" were submitted on January 16 2013 to the prime minister at the time, Ariel Sharon.

The "Daniel Project" was set into motion based on the assumption that Israel's security must be constantly stepped up in view of the threat posed by "irrational countries" and non-governmental terrorist armed with non-conventional weapons. It is believed this threat represents the immediate danger to Israel's existence. Therefore, Israel must preserve its first strike capabilities and develop them further, in order to maintain its ability to launch a preemptive strike, primarily based on an airstrike and augmented with ground-based means.

Based on the report by "Daniel Project" members, the threats posed to Israel stem from two fronts. The first is a conventional war initiated by a coalition of Arab countries, whether joined by Iran or not, and the second – an unconventional attack using weapons of mass destruction (WMD) – atomic, biological or chemical, whether in the framework of a first strike or in the course of an escalation of a conventional armed conflict.

Due to both threats posed, the "Daniel Project" committee recommends as follows:

- Israel must do everything in its power to prevent a hostile coalition armed with weapons of mass destruction. One of the ways to prevent it from forming is to launch a preemptive strike against countries on the brink of arming themselves with WMDs.
- Israel must continue to uphold its policy of nuclear ambiguity in order to prevent its enemies from any future use of the argument 'if Israel can have nuclear weapons, surely we may too". Nevertheless, in the future, Israel might have to change its policy to a limited degree of disclosure of its capabilities. Such a change may only exist in case Israel's enemies succeed in developing nuclear capability or in acquiring it.
- Israel will not be able to survive unless it continues to maintain a policy of credible, decisive nuclear deterrence, complete with missile defense capable of providing counter measures against ballistic missiles. Such a policy can unfold in the framework of the premise deterrence is based on, rather than after a first strike had already been launched.
- Israel must prioritize at least 15 strategically important targets in hostile Middle Eastern countries.

When the "Daniel Project" members met with Prime Minister Sharon and presented their recommendations, they wanted to underscore the extent of the Islamist threat to Israel and cited the following figures: the Arab world comprises 22 countries and

a combined population of 144 million. Should a Palestinian state be established, it will be the 23rd. The Islamist world, however, comprises 44 countries and over one billion inhabitants. These countries' overall territory is 672 times larger than Israel's.

The team members argue that Israel's strategic future rests on the assumption that the threat of an annihilation attack against Israel stems from "a clash of civilizations" rather than on strategic disagreements. Both Israel and the US are caught up in an Arab/Islamist Jihad deeply rooted in religious faith. Moreover, Israel, they believe, has no chance of reaching a situation of 'living peacefully side by side' with the Palestinians, nor any 'settlement akin to peace'.

NOTE: This top secret US-Israeli issue had already been uncovered by *Nativ Online* back in April 2014. The full report has also been released on *Wikipedia* as well as in a lecture by Prof. Louis Beres at Bet Yeshurun, Huston, Texas. According to various publications, the members of the "Daniel Project" comprise of the following figures: Louis René Beres from the US; Na'aman Belkind, former "Aid on Special Means" to Israel's minister of Defense, a member of Israel's Atomic Energy Committee and adviser to Prime Minister Begin on the strike against Iraq's nuclear reactor; former MAFAT chief Prof. Yitzhak Ben Israel; Rand H. Fishbein, former advisor to Senator Daniel Inouye; Dr. Adir Pridor, mathematician, retired Lt. Colonel in the Israeli Air Force, where he served as senior systems designer and former chief military analyst at RAFAEL; retired MK Yoash Tzidon, retired Colonel in the Israeli Air Force.

Ukraine may create nuclear bomb in 10 years

Source: http://en.itar-tass.com/world/749875

September 17 – **Ukraine which has large uranium deposits, nuclear power plants and the ability to enrich nuclear fuel as well as enterprises which produced ballistic missiles in the Soviet times may create a nuclear bomb in ten years**, Izvestia daily reported on Wednesday with reference to the opinion of Russian experts.

"Ukrainian Defence Minister Valery Geletei's statement that Ukraine may regain the status of a nuclear power and create weapons of mass destruction is a provocation, but this should be taken seriously," the daily quoted deputy chairman of Russia's lower house State Duma defence committee Frants Klintsevich as saying, noting that "This cannot be forgotten that science in Ukraine has always been developed and there won't be any problems creating a nuclear bomb."

Klintsevich recalled that the neighbouring country had 17 nuclear power units not designed for enrichment.

"If they assign several nuclear power units for the purpose and will get down to resolve this task the process will take quite a long period of time. But they will cope with it for ten years,"

the lawmaker believed, noting that "It is very strange if Europe will not give any response to such statements. Double standards became normal for them and this may end deplorably for all."

"Ukraine's turning in a nuclear power contradicts all international regulations on non-proliferation of nuclear weapons," because "any nuclear weapons are an instrument of deterrence and parity, but not blackmail," the daily noted.

"Ukraine has inherited a major potential from the Soviet Union. These are nuclear technologies used in peaceful ends and nuclear scientists. They should not begin from scratch," the daily quoted military expert Andrei Klenov as saying, adding that "Meanwhile, western Ukraine and a larger part of eastern Ukraine has plants which produce missiles Satana [third-generation Soviet strategic missile system]. Before the start of hostilities in Ukraine these plants were mothballed and all technical documentation, charts and technologies were transferred to Kiev."

Meanwhile, Ukraine has **Tochka U** (photo), a tactical missile system which uses conventional ballistic missiles with a fire range of 120 kilometres and more that can carry nuclear warheads, the daily recalled. Meanwhile, according to international classification the so-called 'dirty bomb', the simplest variant of weapons of mass destruction that contaminates the territory with radioactive materials, belongs to nuclear weapons.

"If the Ukrainian president decides to create nuclear weapons, 'the dirty bomb' with conventional explosives and radioactive element which can be generated at Chernobyl nuclear power plant can be produced literally in a few days," Klenov said with confidence.

On September 14, Ukrainian Defence Minister Valery Geletei stated the possibility to develop nuclear weapons, if the West refuses to help Ukraine: "If we cannot protect [Ukraine] today, if the world does not help us, we will have to return to creation of these weapons to protect ourselves from Russia."

This is quite illustrative that "officials of the International Atomic Energy Agency (IAEA) and the US ambassador in Ukraine refused to comment on possible after-effects of Ukraine's turning in a nuclear power.

Islamic State terrorists transporting nuclear weapons through Kazakhstan unlikely

By Tatyana Dronzina

Source: http://en.tengrinews.kz/military/Islamic-State-terrorists-transporting-nuclear-weapons-through-Kazakhstan-256177/

Last week the head of the Anti-Terrorism Center of the Commonwealth of Independent States (CIS ATC), **Colonel General of Police Andrey Novikov** declared that the territory of Kazakhstan, along with other Central Asian countries, could potentially be used by terrorists to transport nuclear weapons.

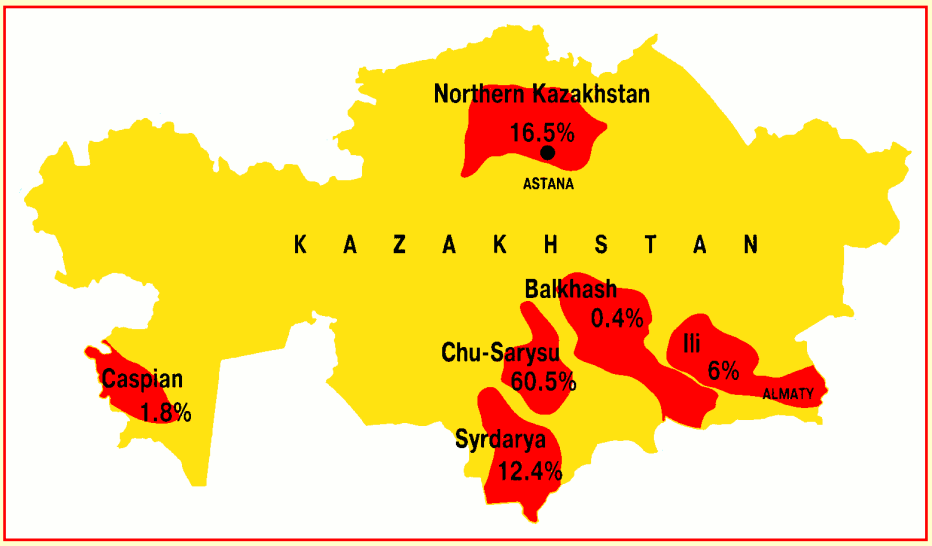
"We also take into account another potential threat – this is the possibility that the territories of the CIS states and, in particular, the Central Asian region, will be used for transit of nuclear and other hazardous materials, as well as

technologies and equipment related to weapons of mass destruction," he said.

In particular, Novikov spoke about the **Islamic State terrorist organization, who claimed they had captured dozens of kilograms of**

nuclear compounds and assets worth a billion dollars. Novikov suggested the threat was quite real.

This week, an expert in terrorism and studies of conflicts **Dr. Tatyana Dronzina said that transportation of nuclear weapons through Kazakhstan by militants of the terrorist organization *Islamic State* was unlikely.**



Member of the International Association for the Study of Terrorism, she also believes there are no clear-cut negations of the fact they can actually develop any nuclear weapons. "Specialists of *Manhattan*, for example, say it is possible. According to them, if the terrorists manage to find a sufficient amount of plutonium or highly enriched uranium, they will be able to construct a crude nuclear weapon. (...) Others are skeptical of this possibility and estimate it as unlikely due to the complexity of the technological aspects of the production process," she said.

"In general, I believe that transportation of nuclear weapons by the *Islamic State* through Kazakhstan is unlikely. **But I do not rule out the possibility completely for the near future.** (. ..) Transportation of nuclear weapons and transportation of compounds bearing technology for nuclear weapons are two completely different things. I admit that there is a possibility of transportation of materials and technologies related to production of nuclear weapons," Dronzina said.

According to Drozina, international terrorist networks have their cells in Kazakhstan but they are currently inactive. She also explained why Kazakhstan could be of interest to terrorists.

"Kazakhstan has the world's third largest proven reserves of uranium, which is also "cheap". Kazakhstan's reserves constitute 12 percent of world reserves. Kazakhstan also ranks first in the production of uranium in the world. (...) The terrorists have every reason to consider the country as a potential source of the raw material," the expert said.

Another factor pointed out by Dronzina was the **start of production at the joint Russian-Kazakh project Uranium Enrichment Center in 2013. The first commercial shipments have already been made.**

Kazakh uranium reserves.

The final factor is the large area of Kazakhstan and its long, not always well-protected borders. **Kazakhstan is the ninth largest country in the world and the largest landlocked country with a small population of 17 million people.**

Due to these, Dr. Dronzina believes that Kazakhstan has to take all the appropriate measures to report, control and physically protect nuclear materials.

"Implementation of these measures is a very difficult task," she said.

There are 1,400 tons of highly enriched uranium in the world, which is enough to produce 25 thousand simple nuclear bombs, the expert said. Much of the uranium is concentrated in the United States and Russia, while most of the plutonium is concentrated in the United Kingdom, Russia, USA, Japan and France. Dr. Dronzina pointed out that **only half of the entire amount was intended for civilian purposes.**

Doctor Tatyana Dronzina *is a Professor at St. Kliment Ohridski University of Sofia in Bulgaria, Guest Professor at the Carlos III University of Madrid and Granada University in Spain, and Gumilev Eurasian National University in Astana. As a researcher, she has practical experience and has carried out fieldwork in several European countries, Central Asia and the Caribbean.*

Preparing the next generation of nuclear emergency responders

Source: http://www.homelandsecuritynewswire.com/dr20140918-preparing-the-next-generation-of-nuclear-emergency-responders

The catastrophic failure of Japan's Fukushima I Nuclear Power Plant in March 2011 was a turning point in how the scientific community viewed nuclear emergencies. Up to then, the emphasis had been on prevention, not response. Virginia Tech's Sonja Schmid has won a 2014 National Science Foundation Faculty Early Development (CAREER) Award to study the prospects and problems of creating a global nuclear emergency response plan. Key issues to be addressed in her research are how to convince the world that any nuclear accident is everybody's problem and how to mobilize an effective international response.

Sonja Schmid, an assistant professor in the Department of Science and Technology in Society in the College of Liberal Arts and Human Sciences at Virginia Tech, has won a 2014 National Science Foundation Faculty Early Development (CAREER) Award to study the prospects and problems of creating a global nuclear emergency response plan.

The catastrophic failure of Japan's Fukushima I Nuclear Power Plant in March 2011 was a turning point in how the scientific community viewed nuclear emergencies, said Schmid, who is based in the National Capital Region. Three of the plant's six nuclear reactors melted down after the facility was hit by a tsunami in the aftermath of an earthquake.

"Up to then, the emphasis had been on prevention, not response," said Schmid. Key issues to be addressed in her research are how to convince the world that any nuclear accident is everybody's problem and how to mobilize an effective international response.

"Nuclear disasters don't respect national boundaries," Schmid added.

"The NSF has a track record of picking scholars with bright futures for its CAREER awards," said Elizabeth Spiller, dean of the College of Liberal Arts and Human Sciences. "Sonja's collaborative project is urgently relevant to the human condition with its policy implications for any future nuclear disaster situations."

Schmid said her grant of about $420,000 over five years will give her the means to develop a research, education, and outreach program for the next generation of nuclear emergency responders.

A Virginia Tech release reports that the award, one of the nation's most prestigious for junior faculty members, recognizes outstanding and innovative research integrated with educational components that support the mission of the recipient's university.

Schmid's four objectives are:

- To create a global map of nuclear disaster expertise.
- To interview experts with experience at incidents like Chernobyl and Three Mile Island to learn what plans they followed and how they improvised.

- To develop criteria for what makes an effective international response.
- To write a curriculum to teach engineers and policy students how to respond when existing plans don't work.

The fourth factor is the educational component of her work.

"If the available tools fail, then what? This objective will teach engineers and policy students to think outside the box," said Schmid. "It will rely on scenarios, role playing, and simulations. The aim is to give students a handle on how to react when not everything goes according to plan."

Schmid will partner with Virginia Tech's Nuclear Engineering Program in the College of Engineering and the Center for Public Administration and Policy in the College of Architecture and Urban Studies for the curriculum development portion of her grant and in organizing a speaker series.

She will spend time this month in Vienna, where she will serve as an invited conference panelist on "New International Nuclear History, International Organizations, and the International Atomic Energy Agency." In addition, she will participate in the second meeting of the International Nuclear Risk Assessment Group.

The release notes that Schmid, who joined the Virginia Tech faculty in 2008, teaches courses in social studies of technology, science and technology policy, qualitative studies of risk, and nuclear nonproliferation. She has studied the history and organization of civilian nuclear industries in the former Soviet Union and Eastern Europe, and how national energy policies, technological choices, and nonproliferation concerns shape each other.

Fluent in Russian, she has done extensive archival research in Russia and numerous interviews with nuclear experts. **Her book, *Producing Power: The Pre-Chernobyl History of the Soviet Nuclear Industry*, will be published by MIT Press early in 2015.**

How the Iranian media distort that country's nuclear lens

By Ariane Tabatabai

Source: http://thebulletin.org/how-iranian-media-distort-countrys-nuclear-lens7604

Few topics preoccupy Iranians more than the ongoing nuclear talks between their country and the P5+1 (the United States, the United Kingdom, France, Russia, China, and Germany). The nuclear issue is on every single Iranian's radar. This is not because they really care about the number of centrifuges spinning at Natanz, their country's controversial enrichment plant. **But the nuclear dossier has impacted every aspect of their lives.** It has dictated Iran's approach to foreign policy and governed domestic politics for over a decade. Yet most Iranians know very little about the nature of the nuclear program or its costs, benefits, and challenges.

Very broadly speaking, Iran's stated goal in the international negotiations is to be allowed to enrich uranium for nuclear energy development, while the foreign powers wish to limit uranium enrichment out of concern that it could be diverted to a weapons program.

Iranians receive most of their information on the subject from two sources: Persian-language media based abroad—mainly BBC Persian and Voice of America Persian—and domestic media outlets, including newspapers and television. Most Iranian news websites have a "nuclear" section that covers the negotiations. While the controversy over Iran's nuclear program has entered its second decade, though, the country's media outlets still fall short of reporting accurately on the matter. This is true for the legal, political, and technical dimensions of the nuclear program, the ongoing negotiations, and, more generally, nonproliferation.

Why are inaccuracies and distortions prevalent? First, during Mahmoud Ahmadinejad's presidency from 2005 to 2013, many journalists stayed away from the nuclear issue. The topic was so politicized and linked to national security that it was virtually impossible to cover it without getting into trouble. This was partly due to the threat of Israeli or US military action against Iran. Questioning nuclear policy became synonymous with supporting the enemy and strengthening it at the expense of national unity.

Today, the nuclear program remains a sensitive topic. News outlets have to be careful not to challenge it too much. But since

President Hassan Rouhani took office, the debate around the nuclear program and ongoing talks with the P5+1 has opened up. In recent months, some reformist newspapers have started to publish American experts' views, even those unfavorable to Iran's program and enrichment activities. Some newspapers ask foreign-based experts to write

articles for them, while others merely translate existing pieces into Persian. They find these pieces **by using anti-filtering systems to go around the filters blocking most foreign news websites, newspapers, magazines, and think tanks**—but the views they translate are not always presented fully and accurately. This inaccuracy is sometimes caused by a political decision to change or remove certain points from an article or broadcast, but it also often occurs because a journalist or translator is simply unable to accurately translate technical words or understand the context in which they are used.

For instance, there are separate words in Persian for "safety" and "security," but most Persian-language outlets mix the two up. This is the case for both foreign-based Persian language media and domestic outlets (links in Persian). This in turn means that the Iranian public receives misleading or partial information on one of the most important issues shaping its life.

Second, the nuclear issue has become an emotional one in Iran. Most Iranians don't care about the right to enrich. Nor do they care how many centrifuges spin in their country. Most are not able to say how many centrifuges are currently operating, or what they think a reasonable number would be in a comprehensive deal. But many Iranians do feel that their country is being treated differently and unfairly by the international community, led by the West.

This is not to say that they believe their government has handled the nuclear issue competently. **"Ten years of sanctions and misery, for what?** [Iranian officials] could have concluded this deal eight years ago and saved us all the trouble," a middle-aged businessman told me in Tehran in June. A salesman at the Tehran Bazaar echoed the sentiment, saying, "I don't understand how [the government] wants to have nuclear energy when it can't even properly manage the Tehran metro. They've spent all this money, and for what?"

UAE and Saudi concerns about the safety of the Bushehr plant

Iranians don't agree on whether or not they need a nuclear program to begin with. In 2009, during the presidential campaign, I spoke to a stylish young man from north Tehran—a generally wealthier and more liberal part of the city—who had supported Ahmadinejad, a hardliner who was largely unpopular with more liberal Iranians. When I asked him about this unusual decision, he told me: "I am voting for Ahmadinejad because I think we need nuclear energy." His sister jumped in: **"Nuclear energy to do what? Do you even know what nuclear energy is? We don't need nuclear energy, we need to sort out other things first."**

Regardless of these disagreements, many Iranians are also quick to denounce the West. "How come Israel and Pakistan are allowed to have nuclear weapons, but when it comes to Iran, we have to go through all this? And we have signed the Nuclear Non-Proliferation Treaty," said a typically pro-Western university professor.

The emotional aspect of the nuclear dossier makes it very difficult for most Iranians to think critically about it. After all, a lot of the country's political agenda has been governed by the issue, and because it has had such a big impact on the economy, many Iranians are loathing admitting that all their sacrifices may have been for very little. Because of this, the media fails to raise fundamental questions about the usefulness

and viability of the nuclear program, instead comforting Iranians by suggesting that their decision-makers are taking the best course of action.

Third, despite the nuclear issue holding such an important place in Iranian politics and policy, it is virtually absent from academia. Most students, including those in political science, international law, international relations, and journalism, can accumulate higher education degrees without knowing anything about nonproliferation.

The absence of nonproliferation and arms control from academic curricula has another implication: There are very few experts on the matter in Iran for journalists to consult. In the West, journalists can call academics and think tankers for independent analysis of governmental decisions and events. But in Iran, think tanks are generally linked to a body of government, and academia changed deeply after the 1979 Islamic revolution, with independent professors and researchers replaced by those with ties to the regime. This means that journalists can only get one side of the story: that told by the government. But it also means that the "experts" they consult often lack nonproliferation and arms control background, and can only speak about some aspects of it, without necessarily managing to provide details or the wider context.

Two trends have made the nuclear issue into a sensitive one in Iran. First, the Iranian government views the problem as one of national security and has historically not welcomed it being challenged or questioned. This closed debate on the subject. Since Rouhani's inauguration in August 2013, things have started to change. News outlets have been able to present and cover critical views on the nuclear program. Even so, there is a fine line between acceptable criticism and questioning that can get one into trouble (link in Persian). **Second,** the nuclear program has become a sensitive topic for the Iranian population in general. Beyond the red lines fixed by the government, the Iranian people find it difficult to think critically. This is because they have been paying the price for the program politically and economically.

Politically, pressure on Iran's nuclear program has often translated into pressure domestically, including in the form of censorship and arrests. **Economically**, sanctions have impacted every facet of Iranians' lives. Many Iranians can't afford basic goods. **Pollution** resulting from substandard gasoline is causing blood cancer and other diseases, according to Tehran city officials. Sanctions have also prevented Iran from replacing its aging aircraft and purchasing parts for them, leading to several **crashes** in the past few months. All these issues make sanctions and, consequently, the nuclear program into a highly emotional topic for Iranians, regardless of political affiliation. Citizens view sanctions on their country negatively, regardless of whether they are hard-line regime supporters or liberals who denounce the very existence of the Islamic Republic.

Thus, for practical reasons like translation problems and censorship and for more personal reasons—in particular the emotional lens through which most Iranians inevitably see the nuclear issue—it's very difficult for journalists to report objectively on the subject. And when Iranian officials say that there's a consensus around the nuclear program in their country, they are in effect presenting this lack of an informed and nuanced discussion on the matter as a unified view. **The media have provided a vehicle for this deficient discussion, contributing to the lack of depth and accuracy in Iranian accounts of the nuclear program and talks.**

Ariane Tabatabai is an associate (and former Stanton nuclear security fellow) at Harvard Kennedy School's Belfer Center for Science and International Affairs.

The RODOS project

Source: http://www.rodos.fzk.de/Overview/moreinfo.html

The developement of the Real-time online decision support system RODOS is a major item in the area of radiation protection of the European Commission's Framework Programmes. In parallel, the German Ministry of Environment, Nature Conservation and

Reactor Safety (BMU) financially contributed to the project with emphasis on early emergency response. The main objectives of the RODOS project have been:

- to develop a comprehensive and integrated decision support system that is generally applicable across Europe,
- to provide a common framework for incorporating the best features of existing decision support systems and future developments,
- to provide greater transparency in the decision process as one input to improving public understanding and acceptance of off-site emergency measures,
- to facilitate improved communication between countries of monitoring data, predictions of consequences, etc., in the event of any future accident, and, the overriding consideration,
- to promote, through the development and use of the system, a more coherent, consistent and harmonised response to any future accident that may affect Europe.

The project began modestly in 1989 with a small number of partners. Participation and geographical coverage increased progressively during the 3rd and 4th European Commission Framework Programmes. By the end of the 4th Framework Programme, some 40 institutes from about 20 countries in the Union and in Eastern Europe (CEEC and NIS) were actively involved in the project. The RTD has been carried out within seven separate, but fully integrated, contracts. Forschungszentrum Karlsruhe has coordinated the project throughout and, inter alia, has overall responsibility for developing the system and integrating the software products of the other contractors. A comprehensive description of the RODOS project and system is given in the Final Report at the end of the European Commission's 4th Framework Programme.

The RODOS system is being further developed under the European Commission's 5th Framework Programme within the following contracts:

- "Migration of RODOS to practical applicability for supporting decisions in operational emergency response to nuclear accidents - RODOS MIGRATION" (FIKR-CT-2000-00077), co-ordinated by Forschungszentrum Karlsruhe (until 9/2003)
- "Data assimilation methods and uncertainty for off-site nuclear emergency management - DAONEM" (FIKR-CT-2000-00025), co-ordinated by SCK/CEN Mol (10/2000-6/2004)
- "Information requirements and countermeasure evaluation techniques in nuclear emergency management - EVATECH" (FIKR-CT-2001-00193), co-ordinated by STUK (until 12/2004
- "Monitoring data and information exchange among decision support systems" - MODEM" (FIKR-CT-2001-00144), co-ordinated by SCK/CEN Mol (until 2/2005)

In addition, an international network has been established on

- "Improvement, extension and integration of operational decision support systems for off-site nuclear emergency management - DSSNET" (FIR1-CT-2000-40076), co-ordinated by FZK (until 9/2004)

Future work

The RODOS system will be further enhanced for operational applicability in national emergency management centres under the EURANOS Project of the EC's 6th Framework Programme (FI6R-CT-2004-508843), co-ordinated by Forschungszentrum Karlsruhe (4/2004 to 3/2009). The main objective of EURANOS is to bring together best practice, best knowledge and best technology to provide an enhanced foundation for Europe's future response to any radiation emergency. It fully integrates 17 national emergency management organisations with 33 research institutes.

The RODOS Consortium

Those institutes who have commonly developed the RODOS system under the 5th and/or 4th Framework Program by providing software components together with the corresponding documentation, build the RODOS Consortium. These are currently:

- Forschungszentrum Karlsruhe GmbH (FZK), Karlsruhe (D)
- Centre d`Etude de l`Energie Nucléaire (SCK/CEN), Mol (B)
- RISØ National Laboratory (RNL), Roskilde (DK)
- University of Warwick (UK)
- GSF Forschungszentrum für Umwelt und Gesundheit GmbH (GFS), Neuherberg (D)

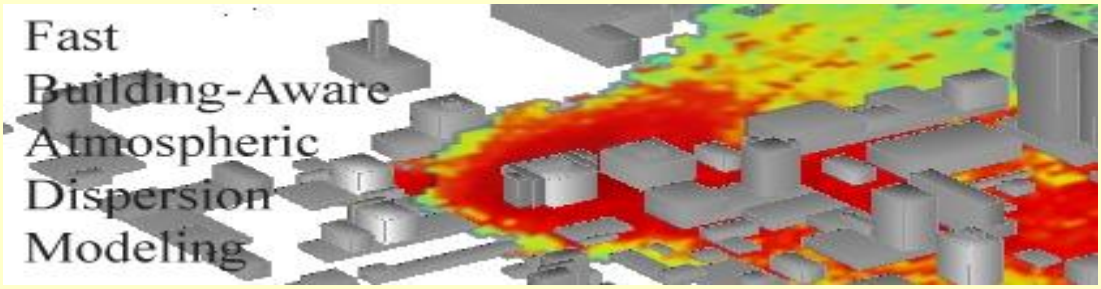
- Leopold-Franzens-Universität, Innsbruck (AU)
- Danish Hydraulic Institute (DHI), Hoersholm (DK)
- Institute of Mathematical Machine and System Problems (IMMS CC), Kiev (Ukraine)
- Scientific Production Association Typhoon (SPA TYPHOON), Obninsk (Russia)
- National Radiological Protection Board (NRPB), Chilton (UK)
- **National Centre for Scientific Research Demokritos (NCSR), Athens (GR)**
- Radiation and Nuclear Safety Authority (STUK), Helsinki (FIN)
- CEC, Joint Research Centre (JRC), Ispra (I)
- Swedish Meteorological and Hydrological Institute (SMHI), Norkoeping (S)
- University of Manchester (UK)
- NRG-Department of Radiation and Environment, Arnhem (NL)

RODOS version PV6.0

The RODOS Version PV6.0 for operational use in emergency centres has been released in May 2004. They run on Hewlett Packard workstations and servers with processor architecture HP-PA2.0 with UNIX 11.0; only FORTRAN 90 is accepted. A LINUX version of RODOS PV6.0 is planned to be released within the first half of 2005.

Quick Urban & Industrial Complex (QUIC) Dispersion Modeling System

Source: http://www.lanl.gov/projects/quic/



The Quick Urban & Industrial Complex (QUIC) Dispersion Modeling System is a fast response urban dispersion model that runs on a laptop. QUIC is comprised of a 3D wind field model called QUIC-URB, a transport and dispersion model called QUIC-PLUME, a pressure solver, QUIC-PRESSURE, and graphical user interface called QUIC-GUI. **Chemical, biological, and radiological (CBR) agent dispersion can be computed on building to neighborhood scales in tens of seconds to tens of minutes.** QUIC will never give perfect answers, but it will account for the effects of buildings in an approximate way and provide more realism than non-building aware dispersion models.

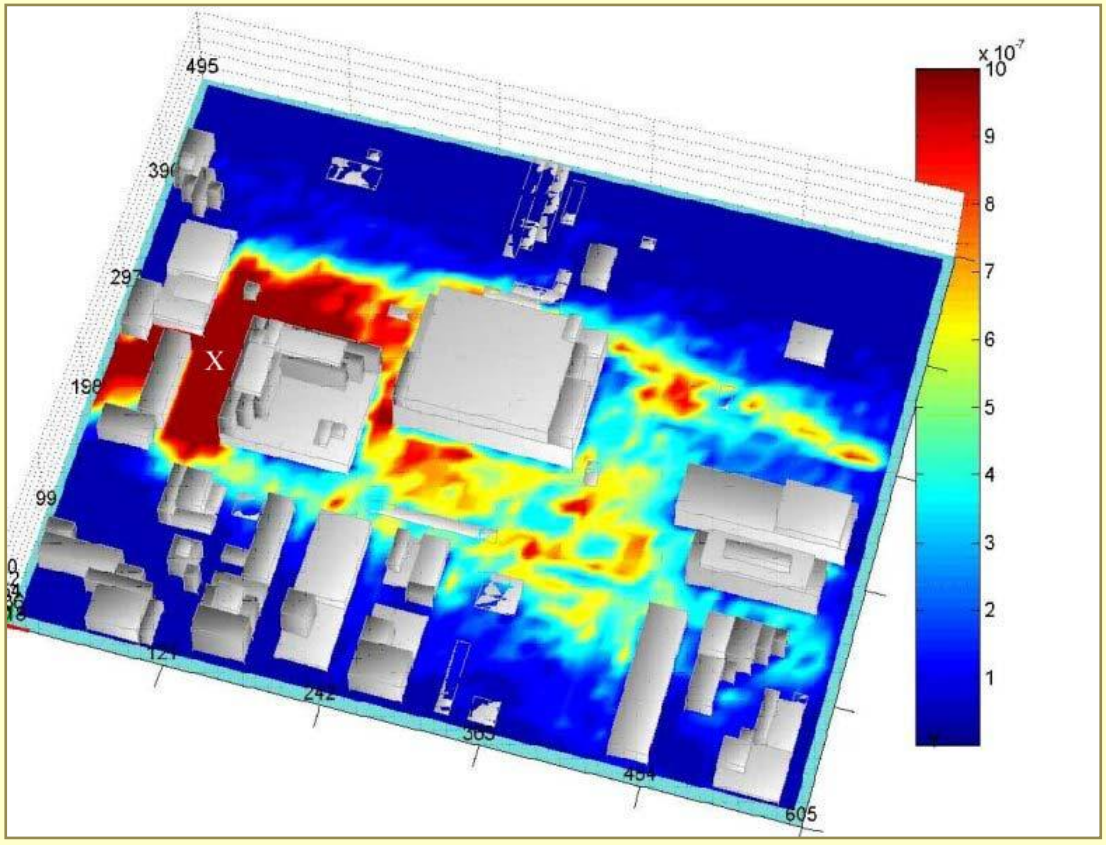
QUIC Capabilities

- Radiological dispersal devices (RDD's) with buoyant rise
- Dense gas chemical agent dispersion with topographical effects and two-phase droplet thermodynamics
- Evaporating liquid pool with 2D shallow water pool spread algorithm
- Multi-particle size biological agent dispersion
- Bio slurry (evaporating droplet) dispersion
- 2-phase (droplet/vapor mixture) dispersion with secondary evaporation from surfaces
- UV decay
- Inhalation model to estimate the amount of agent deposited in various regions of the respiratory tract
- Toxic load
- Line, area, volume, and moving point sources
- Building infiltration and exfiltration
- Deposition on building surfaces

- Nested grids
- Meteorological data assimilation
- Vegetative canopies
- Pressure distribution on buildings
- 2D and 3D graphics visualization
- Affected population calculator with an included CONUS population database

QUIC-PLUME

QUIC-PLUME is a Lagrangian random-walk dispersion model for computing concentration fields around buildings. It has been adapted to work in the inhomogeneous environment of cities. It includes more terms than the normal random-walk model in order to account for the 3D gradients in turbulent and mean flow fields. It includes reflection terms for building and street surfaces. The dispersion of aerosols and gases can be simulated, including deposition, gravitational settling and health properties. Point, moving point, line, area, and volume sources can be simulated. An explosive buoyant rise and multi-particle size capability has been added for dealing with Radiological Dispersal Devices (RDD's).



Near-surface X-Y plane of concentrations produced by QUIC-PLUME (x denotes the ground-level release point).

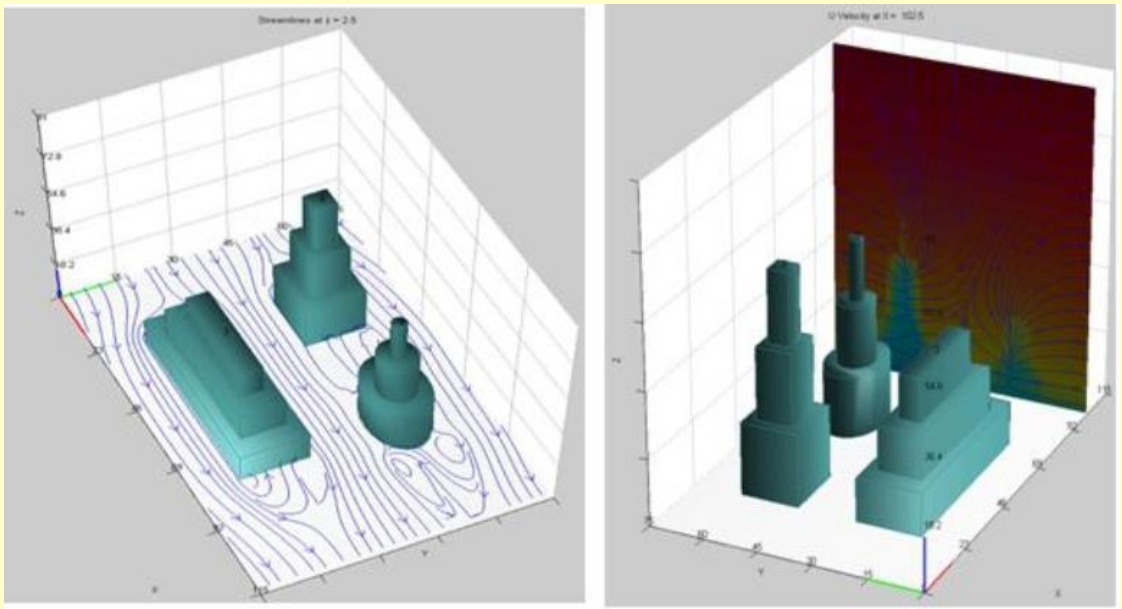
A dense gas cloud model has been incorporated in order to evaluate the effects of heavier-than-air chemical industrial gas dispersion. QUIC-PLUME also has the option of adding the effects of two-phase (vapor/droplet) thermodynamics on dense gas dispersion. There is also a model for UV agent decay which incorporates the effect of time of day, day of the year, geographic location of the release, and cloud cover. The model contains a simple outdoor-to-indoor infiltration parameterization that allows for calculation of indoor concentrations inside of single zone buildings. QUIC-PLUME can run in tens of seconds for smaller problems, but may take up to 30 minutes for large problems where a half million or more particles are to be released. The code has been tested for both idealized and real-world cases (e.g., Gowardhan et al., 2006; Williams et al., 2004). For more information on the specifics of the code, see the QUIC-PLUME Theory Guide.

Capabilities

- Simulates chemical, biological, and radiological agents
- Several source geometries including:
  - spherical shell or volume
  - segmented line
  - moving point
  - circular or rectangular area
  - cylindrical or rectangular volume
  - explosive
- Dense gas (with or without two-phase thermodynamics)
- Radioactive dispersion devices (RDD) with buoyant plume rise
- UV agent decay
- Toxic load
- Surface deposition on horizontal and vertical surfaces
- Building Infiltration
- Lognormal particle size distributions
- Evaporating bio-slurry aerosol source
- Evaporating two-phase chem weapon aerosol source with secondary surface evaporation
- Evaporating liquid pool with 2D shallow water pool spread algorithm

QUIC-URB

QUIC-URB is a fast running model for computing mean flow fields around buildings. It uses empirical algorithms and mass conservation to quickly compute 3D flow fields around building complexes. The underlying code is based on the work of Röckle (1990). Flow parameterizations for the downwind cavity and wake, upwind cavity, rooftop recirculation zone, the street canyon vortex, and intersections are applied to buildings based on the prevailing wind direction and their height, width, length, and spacing. Mass conservation is then imposed and a 3D wind field is produced. Some of the original Röckle schemes have been modified to better agree with experimental data and new schemes have also been introduced (see QUIC Reports). QUIC-URB has been modified to account for dense urban areas, semi-complex building shapes, and forest-induced drag.



Streamlines around stacked buildings.

The model can assimilate wind measurements (e.g., SODAR profiles) and has a nested grid capability so that larger problems can be run (i.e., the inner grid resolves buildings and the outer grid does not). For small problems of a few buildings, the code runs in seconds on a standard single processor laptop. For larger problems with a few million grid cells encompassing several square kilometers in a downtown built-up area, the code may take

from 5 to 15 minutes to run. Numerous evaluation studies have been performed and can be found on the QUIC Reports page.

Capabilities

- Assimilates multiple meteorological data sources or mesoscale meteorological model data to initialize wind fields.
- Wind profiles can be produced from point measurements using logarithmic, power-law, or urban canopy logarithmic parameterizations.
- Vegetation Canopies

Evidence of a Turkish nuclear weapons program

By Hans Rühle

Source: http://elderofziyon.blogspot.gr/2014/09/report-evidence-of-turkish-nuclear.html#.VCEIHxb5nrM

Die Welt has put together a pretty good case that Turkey is seeking to build nuclear weapons.

That Turkey is obviously working on nuclear weapons is hardly discussed publicly. The western intelligence scene, however, is largely in agreement about it.

The model for the strategy of the Turks is clearly Iran. Tehran seeks nuclear weapons by creating bomb material in secret under the cover of a civilian nuclear program. And Turkey has launched a large-scale civilian nuclear program in recent years. The official reason for this: The domestic economy is growing and needs more power.

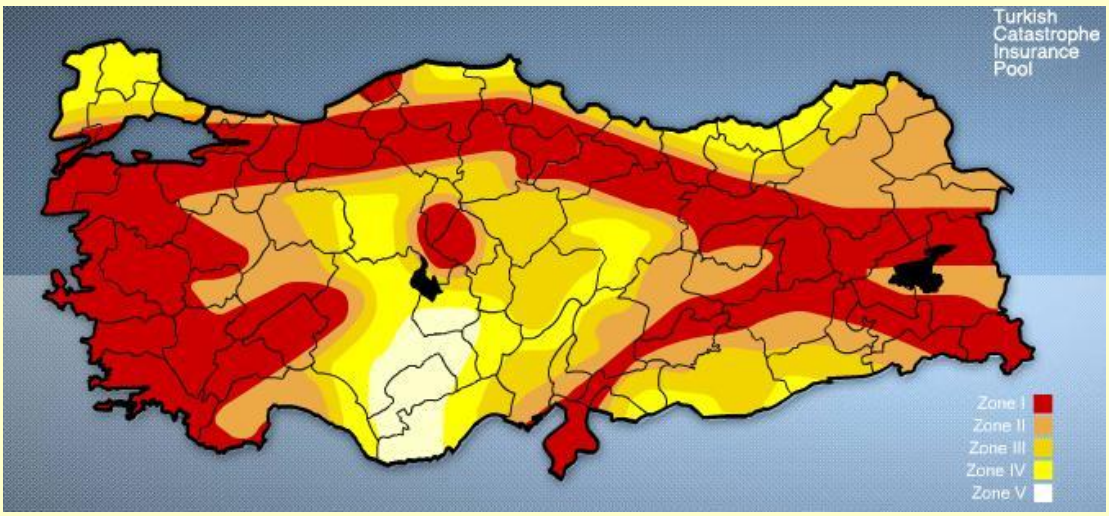
In 2011 they contracted the Russian company **Rosatom Ankara** for 15 billion euros to build a large reactor complex on the Mediterranean coast, about 300 kilometers east of the tourist center of Antalya. Two years later, a similar agreement with a **Japanese-French** consortium for the price of 17 billion. **Even more interesting than these figures are the contracts - and especially what is not in them.**

When companies build a light-water reactor, they usually agree with the Government that the project will operate for 60 years and they will provide the necessary

uranium for the operations and then take back the spent fuel. This was offered in the case of Turkey by both Rosatom and the Japanese-

French consortium. So far nothing special.

But Turkey has waived in both cases to fix the supply of uranium and the disposal of spent fuel from the contract. She insisted on the contrary, to regulate this separately later. Ankara explains that this is not an unusual maneuver in the negotiations. But the intention behind it is easy to see: The Turkish leadership wants to keep these parts of the nuclear program in their own hands - and **they are crucial to any State that wants to develop nuclear weapons.**



First, there are the fuel rods: All over the world, the disposal of nuclear waste is discussed as a problem. Turkey on the other hand does not want to give up their spent fuel. The only logical explanation for this: they want to make preparations for the construction of a plutonium bomb.

And this is a civilian nuclear power plant so after burning off the bars they contain only 90 percent of waste, but in addition nine percent is permanently contaminated with uranium and plutonium. A plant that can isolate the plutonium from the highly radioactive material from the rods can be built within half a year and is about the size of a normal office complex. This has been shown in the United States system studies.

The fuel rods could theoretically be processed for reuse in a civilian reactor. But this is much more expensive than buying new. If Turkey still wants to keep the spent fuel rods, then there's just one reasonable explanation: She wants to gather material for a plutonium bomb.

The gaps in the contracts open yet another way to the bomb, namely directly with uranium. For Ankara uses the same technology that is also used to make the ore for a civilian reactor fuel available: uranium enrichment.

For the power plant operation, it must be enriched to 3.5 to five per cent, for nuclear weapons on at least 80 percent. The technical process is the same in principle. And so, it is a suitable cover for those who want to say that they are using it for power to in truth produce nuclear weapons.

According to the Federal Intelligence Service..., the Turkish Prime Minister Erdogan has already arranged in 2010 to secretly prepare for the construction of facilities for urainum enrichment. According to other intelligence findings Turkey already has a significant number of centrifuges. **Where they come from, can be guessed, after all: Pakistan.**

The Turks had a leading role in the activities of Abdul Qadeer Khan, the Pakistani nuclear smuggler who provided 1987-2002 Iran, North Korea and Libya

with thousands of centrifuges. The electronics of all Pakistani assets came from Turkish partners. Khan temporarily had even the intention to relocate its entire illegal centrifuge production in Turkey. 1998 offered the then Pakistani Prime Minister Nawaz Sharif the Turks even a "nuclear partnership" in research.
Turkey had finally been helped in the construction of Pakistan's nuclear weapons program in the 80s. At that time many components, which could not be procured openly, were delivered via Turkey to Pakistan. Therefore it is not surprising that intelligence reports to date say there is brisk nuclear scientific exchange between the two countries.
But probably it's about more than this. AQ Khan has proven to give his customers not only the centrifuges, but also with complete blueprints for the construction of nuclear weapons [like he did with Iran, Libya and North Korea.]

Another important indication in the chain is the Turkish missile program.....

Tthere is the question of the meaning and purpose of such accelerated missile development. The answer is relatively simple: medium-range missiles are suitable, due to their low accuracy and payload, only for weapons of mass destruction. A program for their preparation is a strong - a very strong - indication of an ongoing nuclear weapons program.
But why exactly does the political leadership of Turkey want the nuclear option? Again, you have to know to read hints and omissions. In August 2011, the Turkish ambassador to the United States, Namik Tan, said: "We can not let Iran have nuclear weapons." Two years later, the then Turkish President Abdullah Gul clarified this position in an interview with the magazine "Foreign Affairs": **"Turkey will not allow a neighboring country to have weapons which Turkey does not have."**
Given the already established nuclear power of Israel and the nascent nuclear-armed Iran, the Turkish prime minister has no choice but to arm his country with nuclear weapons as well, if he wants to carry out his vision of building a great Turkish power. Because otherwise, Turkey remains to his understanding of secondary importance - and therefore Erdogan cannot and will definitely not be satisfied.

__Hans Rühle__ was from 1982 to 1988 the Head of the Policy Planning Staff in the Department of Defense.

EDITOR'S COMMENT: Not a word on the sismic activity (see map) of the area of the new nuclear plant. Then in 2012 Turkey started a middle range (500-5.000km) missile program mostly aiming to a 2.500km missile by 2015. They also have a certified for nuclear weapons F-16 squadron. If everything goes according to plans then Turkey might pocess a nuclear bomb by 2022.

Explosives

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

Most commonly, terrorists have used explosives to inflict casualties and damage. Home-made explosives, fabricated from certain easily accessible chemical precursors, are a preferred tool for perpetrators of terrorist attacks. The Europol TE-SAT reports indicate that these continue to pose a serious threat to the EU. Therefore, the Commission's efforts concentrate on ensuring greater security of explosives, bomb-making equipment and technologies that contribute to the perpetration of terrorist acts.

EU Action Plan on the security of explosives

While the usefulness of explosives for industrial purposes is beyond doubt, policy-makers must reduce the possibility of their misuse for terrorist purposes to ensure the security of citizens. This can only be achieved through the active contribution of all stakeholders at EU, national and industry level. This rationale formed the basis of the 2008 EU Action Plan on Enhancing the Security of Explosives. The Action Plan contains 48 measures related to prevention, detection and response, as well as horizontal measures, such as the development of information sharing mechanisms and platforms, supporting research and working with partners both in and outside the EU. A review of the EU Action Plan was undertaken in 2012. An overview of its implementation by the Member States and EU bodies is provided in the 2012 Progress Report on the Implementation of the EU Action Plan on Enhancing the Security of Explosives .

The Stockholm Programme emphasised the need to implement the Action Plan and to provide better information on the security of explosives. In addition, it called for the development of a legislative framework to address the dangers associated with the use of chemical precursors in explosives. On 2 September 2014, Regulation (EU) No 98/2013 on the marketing and use of explosives precursors will enter into force with a view to enhancing protection of citizens from the threat of terrorism. The Regulation, which shall apply from 2 September 2014, establishes a tighter regulatory regime for high-risk chemical explosives precursors to reduce their accessibility to the general public (private individuals). The Commission, in consultation with Member states and relevant stakeholders, has issued a Guidelines document to facilitate its implementation.

The future policy approach to improving the security of explosives is set out in the May 2014 Communication on a new EU approach to the detection and mitigation of CBRN-E risks . The revised approach is the first step towards implementing the Council conclusions adopted in December 2012 , which encouraged the Commission to create a new CBRNE Agenda identifying and using synergies between the Action Plan on Enhancing the Security of Explosives and the EU Chemical, Biological, Radiological and Nuclear Action Plan of 2009. The new Communication sets key priorities to be addressed at EU level and proposes a number of practical actions to bring about progress in the area of detection and mitigation of CBRN-E risks..

Reducing risks

Work on reducing the risk of misuse of certain chemicals to fabricate home-made explosives is carried out within the Standing Committee on Precursors (SCP). The SCP has already contributed to the amendment of the Limitations Directive (now incorporated into the REACH legislation) that reduced access to highly concentrated ammonium nitrate

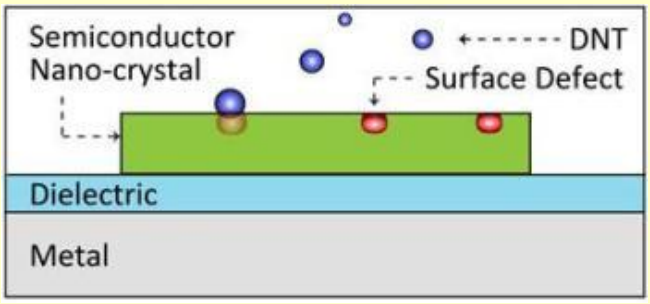
fertilisers, which have been misused to produce home-made explosives. In addition, the SCP assists the Commission in its work to further reduce the risks related to the misuse of precursors. The Action Plan promotes other preventive measures, such as the tightening of security along the entire supply chain of commercial explosives in the EU, including in production, transport, storage, commercialisation and final use.
An expert working group consisting of representatives from national security institutions and EU bodies has been set up to deal with the specific issue of detecting explosives and their precursor chemicals. It develops relevant detection scenarios to identify possible technology gaps.

New BOMB detect-o-tech 'could give sniffer dogs competition': TRUE

But so could a magic eight-ball

Source:http://www.theregister.co.uk/2014/07/21/new_bomb_detectotech_could_give_sniffer_dogs_competition_true/

Researchers working on a new type of bomb detector technology have made the rather underwhelming boast that their kit "could soon give bomb-sniffing dogs some serious competition".
“Bomb-sniffing dogs are expensive to train, and they can become tired,” said study co-lead author Ren-Min Ma, one of the boffins who came up with the new gear. “The other thing we see at airports is the use of swabs to check for explosive residue, but those have relatively low-sensitivity and require physical contact. Our technology could lead to a bomb-detecting chip for a handheld device that can detect the tiny-trace vapor in the air of the explosive’s small molecules.”



Ma and his colleagues fashioned their **"plasmon sensor"** by placing a layer of cadmium sulfide semiconductor on top of a sheet of silver with a layer of magnesium fluoride dielectric in the middle. It seems that even very tiny amounts of explosive nitro-compounds (TNT and related substances such as PETN, a known terrorist favourite) can have detectable effects on such a setup.
“We think that higher electron deficiency of explosives leads to a stronger interaction with the semiconductor sensor,” said Sadao Ota, one of the development team.
We are told:

The engineers put the sensor to the test with various explosives – 2,4-dinitrotoluene (DNT), ammonium nitrate and nitrobenzene – and found that the device successfully detected the airborne chemicals at concentrations of 0.67 parts per billion, 0.4 parts per billion and 7.2 parts per million, respectively. One part per billion would be akin to a blade of grass on a football field.
“PETN has more nitro functional groups and is more electron deficient than the DNT we detected in our experiments, so the sensitivity of our device should be even higher than with DNT,” said Ma.
Ma and his chums would have found it difficult to arrange a test with actual PETN or TNT as these are genuine high explosives, fairly sensitive stuff, and regulations require elaborate and expensive precautions when they are being handled. The comparatively inert substances the researchers did use - none of which are much good as explosives as they stand, though they all can be (and are) made into proper bomb-type stuff by further processing - will have been much easier to obtain.
It's easy to see, in fact, that the research team's expertise doesn't lie in explosives and security as such, or they wouldn't have chosen to lead with the claim of their tech being as good bomb-sniffer dogs. Anyone who has worked in the field knows that explosives dogs are more or less useless as detectors - not really much better than random chance in most circumstances, and wildly prone to false positives - and that their main job is to deter terrorists, make people feel

safer, and also perhaps to offer an excuse for searching people.
And, no matter how sensitive your detector is, if the molecules of explosive to be detected are confined inside a container which is not permeable to them (not difficult to arrange in the case of quite large molecules like these), the chance of one drifting off to hit the detector is going to be really very slim indeed. And that's before we even get into the problem of false positives, which is evidently going to be a big one when the detector can pick up agricultural fertilizer (for that is what ammonium nitrate is mainly used as) at 0.4 parts per billion.
So, probably not much of a flyer at the airport, then. But the suggestion that the kit might be some use for finding old landmines is perhaps more credible. Antipersonnel mines are often non-metallic in construction and frequently employ TNT as a main charge. Particularly as they get old, they are likely to leak explosives into the soil around them and the air above it.
So the new plasmon sensors could well be useful: just not, probably, against the tiny, rare problem of terrorists using PETN. The press release should probably have emphasised the huge, serious issue of landmines.

Explosive Bootnote

Pentaerythritol tetranitrate (PETN) is a relatively stable explosive but - attractively, to terrorists - still sensitive enough that it doesn't necessarily require a separate detonator. In regular munitions it is used in detonating cord, and as a secondary explosive between detonators and main charges. PETN was used unsuccessfully by the wouldbe airliner shoe bomber Richard Reid and the pants bomber Umar Farouk Abdul Mutallab.

Morphix Technologies' Explosives Detection Kit Scores High in NTOA Review

Source: http://www.policemag.com/channel/technology/news/2014/07/09/morphix-technologies-explosives-detection-kit-scores-high-in-ntoa-review.aspx

Morphix Technologies, a manufacturer of detection devices for dangerous chemicals, has announced that its **TraceX Explosives Detection Kit** has received a 4.32 out of a possible 5 points from the National Tactical Officers Association Member Tested and Recommended Program. Morphix Technologies can now display the NTOA Member Tested and Recommended Logo on its marketing materials.

The TraceX Explosives Detection Kit was developed by Morphix Technologies under contract from the U.S. Department of Defense and meets its demanding requirements. Designed small enough to fit into a cargo pocket, lightweight and rugged, both testing field officers commented on how "very durable, safe and easy-to-use" the kit proved to be.

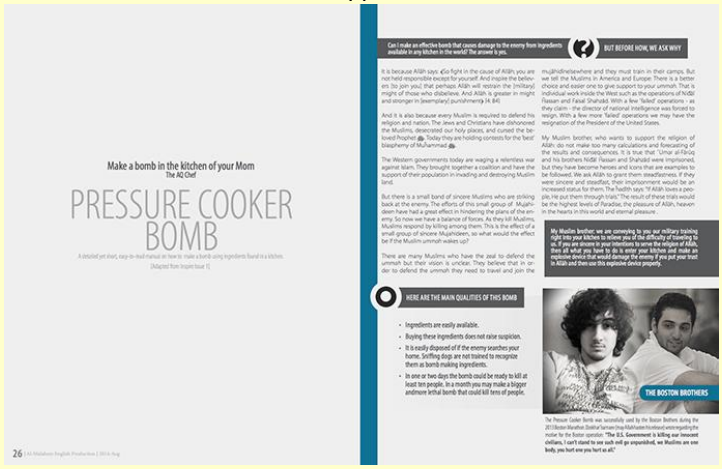
One field testing officer continued, "the self-contained testing kit keeps all testing chemicals contained within itself, providing no harmful exposure to users. The test and results are all conducted and displayed within the unit, simplifying the procedure and removing the possibility of user error and the resulting consequences. With one sample, the kit is able to test for nine different explosives in one easy-to-use test. The kit is small enough to carry on your person and is durably constructed."

Each kit comes in its own disposable protective plastic case, so the handler will be ready to use it when needed. With a single swab, the TraceX Explosives Detection Kit detects all the major families of explosive materials and their precursors.

Al-Qaeda publish car bomb 'shopping list' and suggest UK targets

Source: http://rt.com/uk/183656-al-qaeda-manual-attacks/

August 29 – Al-Qaeda this week published an online magazine featuring instructions on how to build homemade car bombs and an appeal to Muslims to attack UK and US targets in the vein of the Boston bombers.



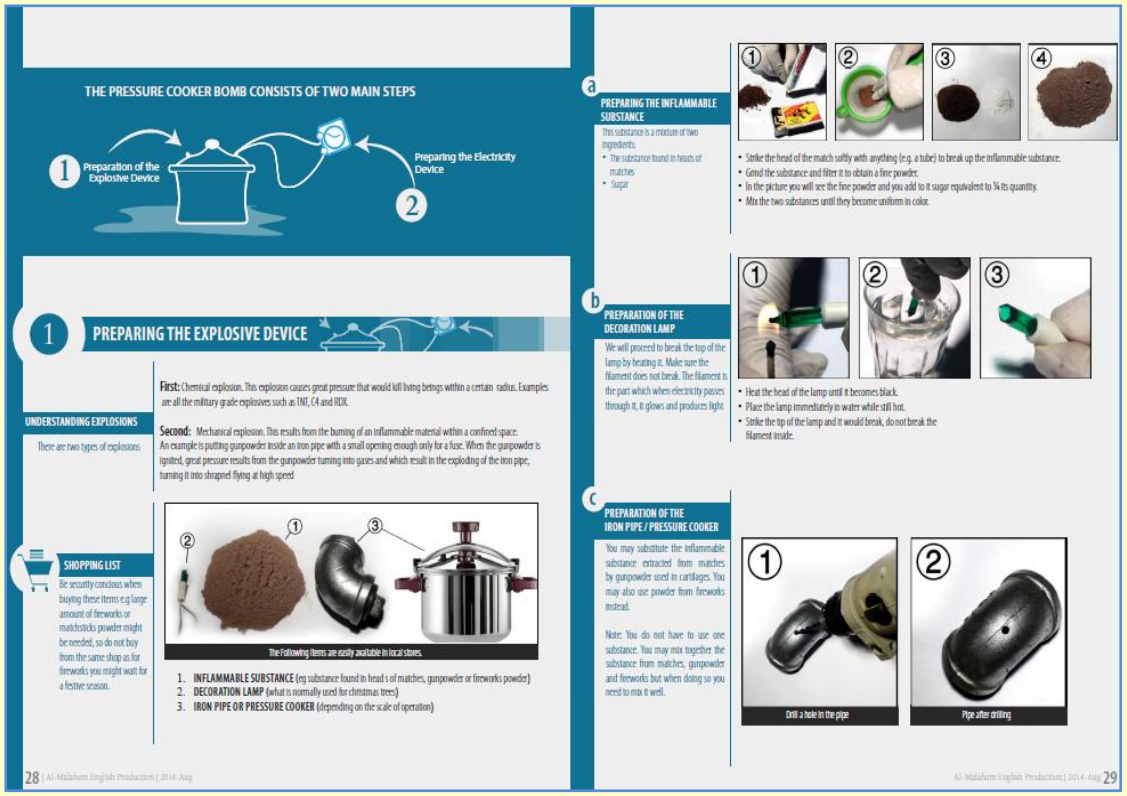
The English-language magazine, entitled *'Palestine: Betrayal of the Guilty Conscience Al-Malahem'*, urges Muslims in the West to assemble pressure cooker bombs like those used to attack the Boston marathon last year.

In a list of *"examples of targets,"* the magazine suggests attacks on the UK's Royal Military Academy at Sandhurst, MI5's Thames House and Marks & Spencer department stores during Friday prayers, so as to avoid harming Muslims.

The list features US targets including Times Square, casinos in Las Vegas, Georgia Military College, the US Air Force Academy in Colorado Springs and the General Atomics

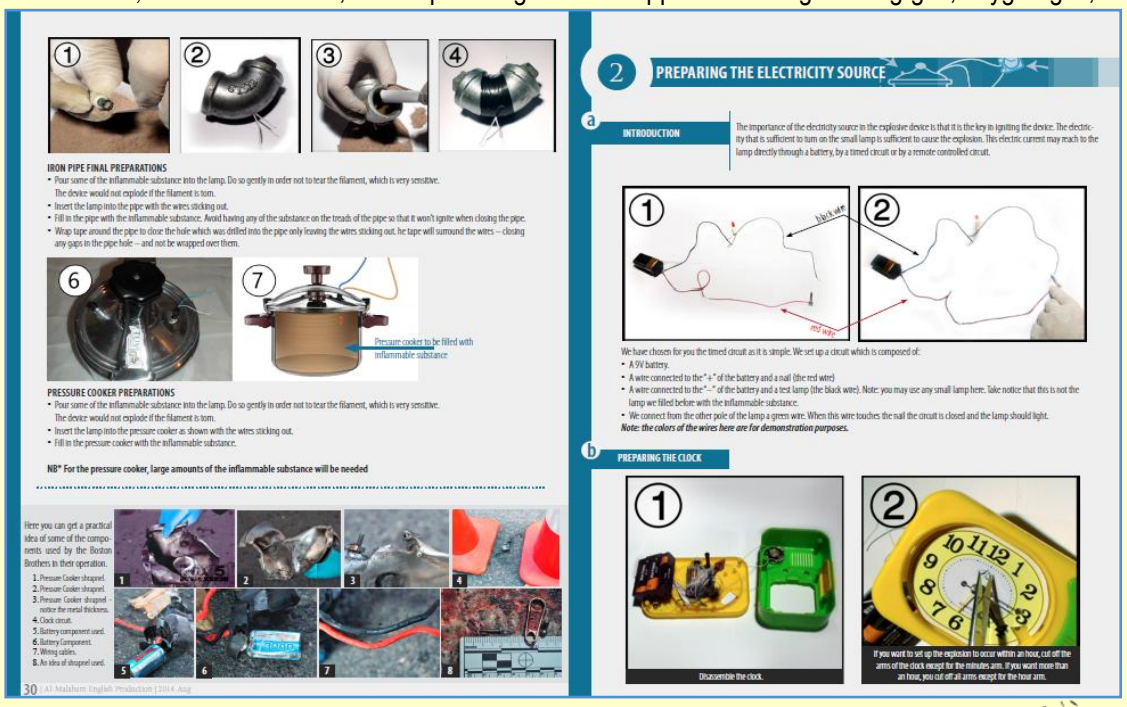
headquarters in San Diego. It also suggests attacks on Israeli, British and American company headquarters and holiday destinations abroad, oil tankers and busy train stations.

A nine-page spread offers instructions on how to *"make a bomb in the kitchen of your Mom,"* step-by-



step photographs, a shopping list, and admiring words about Boston bombers the Tsarnaev brothers.

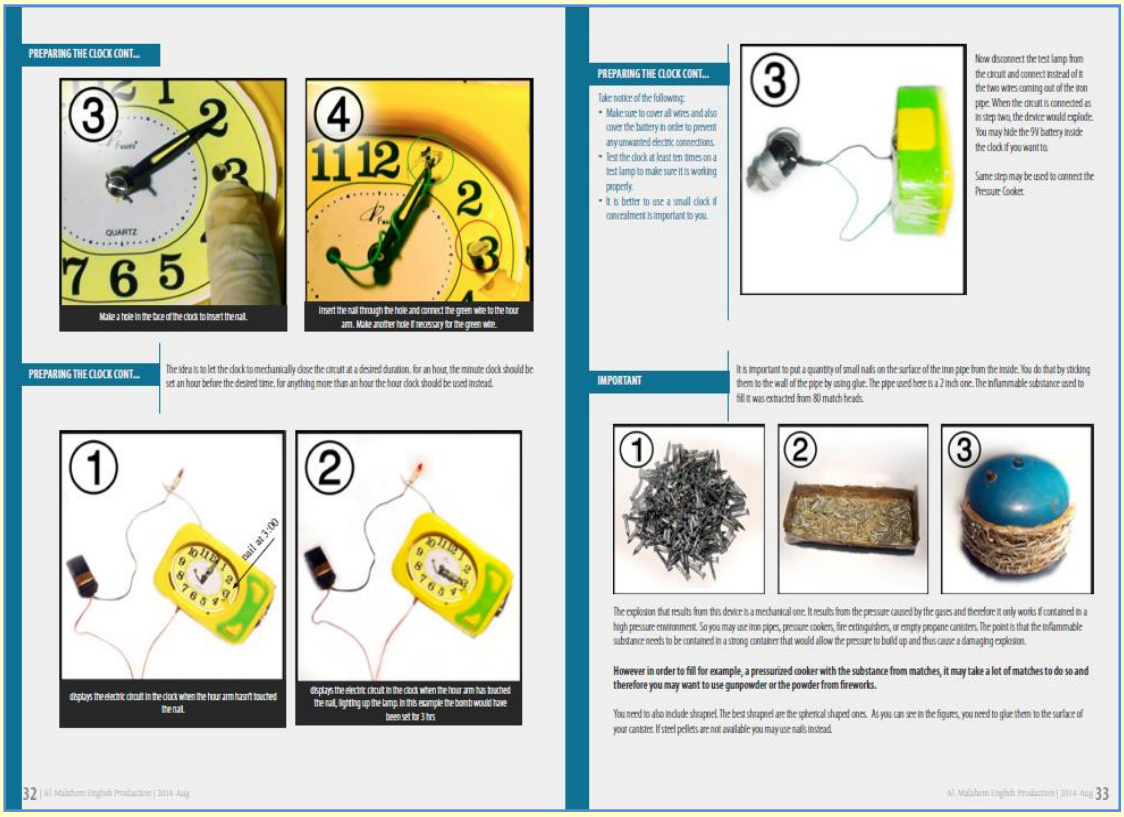
"This recipe gives you the ability to make a car bomb even in countries with tight security and surveillance," one article reads, before providing a list of supplies including cooking gas, oxygen gas, a



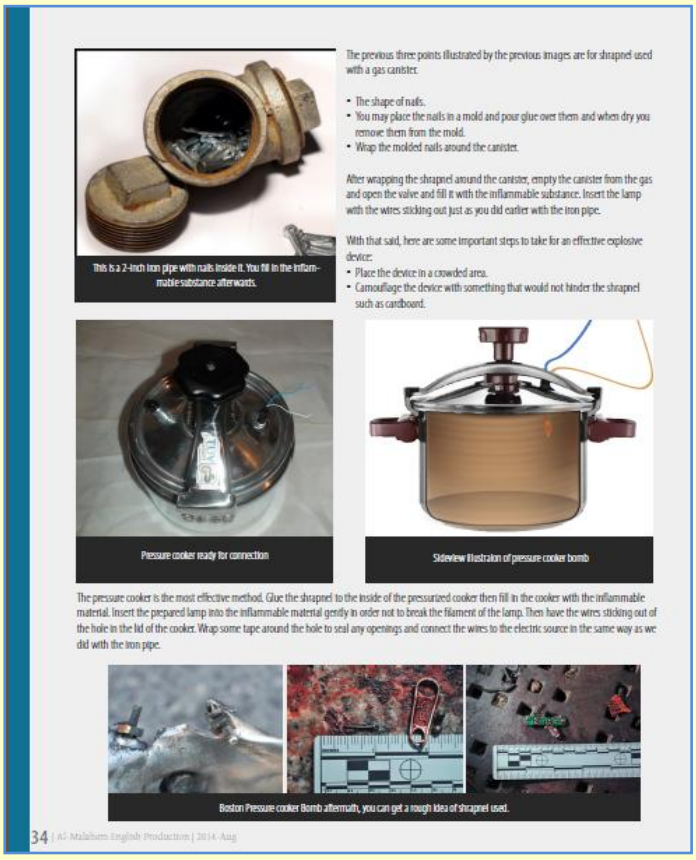
barometer, decoration lamps and matches.

"My Muslim brother: we are conveying to you our military training right into your kitchen to relieve you of the difficulty of traveling to us," it reads.

"If you are sincere in your intentions to serve the religion of Allāh, then all what you have to do is enter your kitchen and make an explosive device that would damage the enemy if you put your trust in Allāh and then use this explosive device properly."



A timeline of terror attacks, including 9/11 and the Boston bombings is concluded with a blank entry marked '201?' implying a terror attack on American or British soil is planned for the near future.



"The timeline concludes with the date 201?' and blank spaces and question marks for the photo and information of the next attack - implying that it is coming soon," Steve Stalinsky, of the Middle East Media Research Institute, told Fox News.

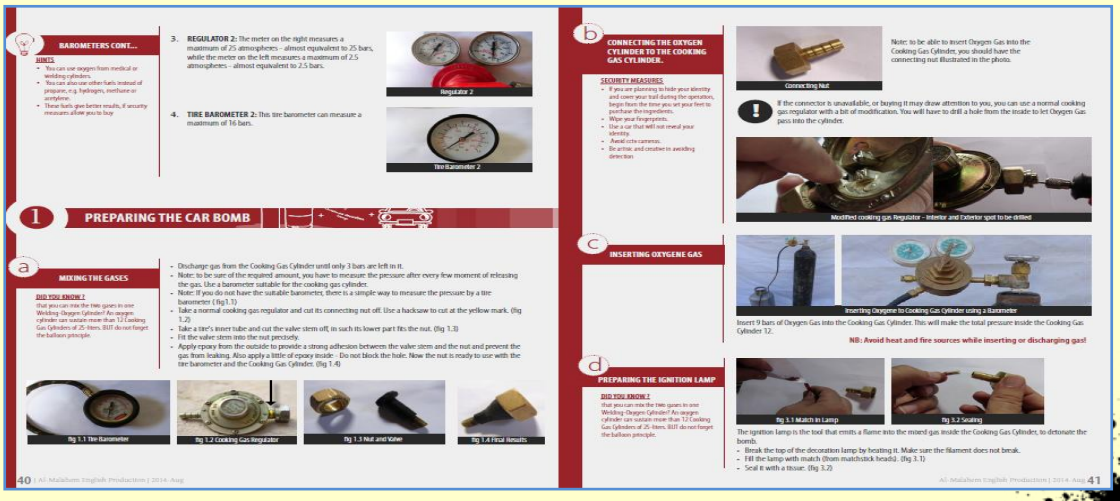
"Both AQAP [Al-Qaeda in the Arab Peninsular] and IS [Islamic State], as well as every other al-Qaeda branch and offshoot, is relying on US social media companies including Twitter and YouTube for their cyber-Jihad efforts," Stalinsky said.

"There could be some envy by AQAP that IS is now getting all the headlines."

The magazine is a supplement to the terror group's Inspire magazine, aimed at encouraging Muslims in the West to carry out lone-wolf terror attacks. *"Inspire Magazine's goal is to empower Muslims. And*

what is empowerment without being strong, powerful and intelligent?" the publications reads.

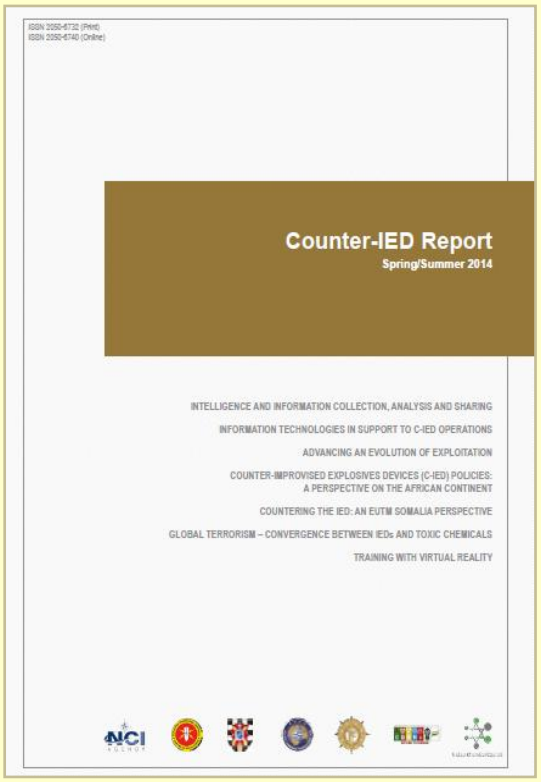
"In this section, we give you strength, power and intelligence. Believe me, using car bombs gives you all that."



Spring/Summer 2014 Counter-ID Report

By Rob Hyde-Bales (Consulting Editor)
Source: www.counteriedreport.com

2014 marks the end of ISAF involvement in Afghanistan. After three previous Anglo-Afghan wars all UK troops, less a small component that is scheduled to continue Afghan national officer training, will leave Afghanistan. The ISAF withdrawal is a huge logistic undertaking. The British force component is currently based in Camp Bastion in Helmand Province preparing equipment for transit back to the UK. Conversely US armed forces are in the process of destroying large amounts of equipment which are deemed either surplus to future requirements or too expensive to transport back to the US.
Defining features of the war in Afghanistan have been the constant use of Improvised Explosive Devices (IEDs) by insurgents and consequent ISAF Counter-IED operations. IED usage resulted in very high levels of both military and civilian casualties throughout the conflict. Prior to ISAF engagement in Afghanistan, the Afghan Mujahideen extensively used IEDs against the Soviets throughout their invasion of Afghanistan during the 1980s.



A very positive initiative in the UK Army resulting from the conflict has been the formation of 821 Explosive Ordnance Disposal (EOD) and Search Squadron. This unit includes elements of the Royal Engineers, Royal Logistic Corps and Royal Signals – all with critical C-IED roles - as part of 33 Engineer Regiment (EOD).
After the departure of ISAF, responsibility for C-IED operations will devolve in the main to civilian organisations – NGOs and commercial companies. Overall co-ordination will rest with the UN Mine Action Service (UNMAS). Thus a recent meeting at the Geneva International Centre for Humanitarian Demining that included the overall issue of IEDs in Humanitarian Mine Action (HMA) and Peacekeeping Operations was most timely. Representatives from OPTIMA Defence and Security Group Ltd. (see Counter-IED Report Autumn/ Winter 2013) attended this meeting. It was apparent that there is an urgent need within the humanitarian community for increased C-IED awareness and specialist personnel for IED disposal. It was agreed that an effective HMA global response to IEDs requires, *inter alia*, meaningful information sharing and a comprehensive IED threat database, accessible to all accredited organisations.
This Spring/Summer edition contains a broad cross section of topical and high quality articles highlighting global current technological, operational and training C-IED activities and initiatives.
The article from Captain Andrew Brady of the Irish Defence Forces on the development and implementation of C-IED procedures in support of the European Union Training Mission in Somalia highlights the significant challenges inherent in operating successfully in this war torn and dysfunctional nation. IED usage in Somalia has increased exponentially since 2007, and is the favoured weapon of the Somali Islamist Insurgent Militia Group Al-Shabaab that has terrorised Somalia since the mid-2000s.
Colonel (Retired) HR Naidu Gade of CBRNe Secure India in his article describes most comprehensively the ubiquitous and ever increasing threat from IEDs in India where they account for 70 per cent of deaths in counter insurgency and anti terrorist operations. This situation has compelled India to dramatically increase its C-IED capacity on a multi agency basis throughout this vast nation. It is planned that this process will be complete within the next couple of years.
Saab describes meeting an urgent operational requirement from MODUK for a C-IED training capability to validate individual and collective training detection drills. The resultant C-IED Collective Trainer earned plaudits and the British Ministerial Defence Award from MODUK, and proves again the value of the successful outsourcing of military training to credible contractors.

Szenaris GmbH demonstrates the utility of training systems based on virtual reality. Two examples are quoted; firstly a remote controlled diving robot and secondly IED Disposal remote controlled robots. Virtual reality allows challenging training environments to be configured to specific training requirements and conserves the actual equipments themselves.
These and other excellent articles constitute this edition of Counter-IED Report.

*During his career in the UK Royal Engineers, **Rob Hyde-Bales** was responsible for landmine clearance in Libya and, more latterly, Afghanistan in the running of the first United Nations humanitarian landmine clearance training programme – Operation Salam. The programme trained Afghan male refugees in landmine clearance techniques, and Afghan women and children in mine awareness and avoidance training. More recently he set up the Caribbean Search Centre in Kingston, Jamaica. The Centre is designed to train security forces across the Caribbean in modern search techniques. After retiring from the army he joined Cranfield University at Shrivenham, near Oxford, and undertook a research project on behalf of the UK Ministry of Defence that examined ways to improve the sharing of IED threat information between the military and civilian organisations in hazardous areas.*

3D Printed Landmines are Built for Military Training

Source: http://3dprint.com/10939/3d-printed-landmines/


EOD Life

Over the past few weeks, we have been reporting on all sorts of uses that the U.S. Army is considering for 3D printing. Everything from 3D printed food, to 3D printed clothing and armor, the U.S. Army is not leaving one stone unturned in their quest for excellence, both on and off of the battlefield. They are not alone though. A small company called **EOD Life** is also trying to merge 3D printing with potential military uses.
EOD Life is a small startup that has the intention of bringing more training devices and collectibles to the EOD (Explosive Ordinance Disposal) community. The owner of the company also happens to be an EOD, which he explains "is basically a military bomb squad that also deals with military ordinance".

The company recently announced the creation of a 3D printed YM-1 landmine, which has been printed for specific military training exercises. The top piece on the landmine pushes down, when stepped on. As this happens, an internal switch then sends a signal wirelessly, via a 315mhz RF board transmitter and receiver, to a recover box which then sets off a loud piezo siren.
For obvious reasons, military personel can not train with real live landmines, so this becomes an affordable alternative, when compared to their other options. EOD Life plans to sell these for $75 a piece, which is much cheaper than what other similar non-3D printed training landmines go for. Similar devices sell for upwards of $600-700 a piece.
While the design for this device is not open source, as EOD Life retains the files for business purposes, it isn't out of the realm of possibility that one day these could be printed right at the military training facilities, when needed. Without a doubt 3D printing will have a significant impact on the future of military life, education, training, and combat. The technology allows for more affordable, customized equipment that can be produced in a fraction of the time that it would take with traditional manufacturing methods.

After the Flood: microdrone is finding land mines

Source: http://i-hls.com/2014/09/flood-microdrone-finding-land-mines/

Airborne support in the search for survivors and land mines: in the wake of a natural disaster in

Serbia/Bosnia and Herzegovina, rescue teams have been using German-made drones.

This past May, flooding and landslides left many people homeless, blocked access to large areas, and brought wartime land-mines to the surface.

The potentially life-threatening hazards to which the populace is exposed continued long after the storms abated. The EU's ICARUS and TIRAMISU development projects are providing support for the search for survivors and land mines. And now the UN, too, is again using airborne support.

"We've conducted around 20 flights over a two week period, either manually or using automatic waypoints," notes Haris Balta. RMA development engineers carried out the mission on-site. "We've provided the other rescue teams with damage reports, detailed maps and pictures of the disaster region – the goal being to locate the countless landmines left over from the civil war."

According to sUAS **md4-1000 Quadrocopters** developed by Germany-based microdrones GmbH are being used by the Belgian Royal Military Academy (RMA) in the disaster area.

Airline passenger was accidentally given suitcase full of plastic EXPLOSIVES left at Sydney airport by the AFP a month ago... then took them home

Source: http://www.dailymail.co.uk/news/article-2751633/Airline-passenger-accidentally-given-suitcase-plastic-EXPLOSIVES-left-Sydney-airport-AFP-month-ago-took-home.html

A woman got more than what she bargained for when she was given a replacement suitcase at Sydney airport after her luggage was damaged on her flight.

The lady discovered 230g of a plastic explosive in a suitcase on Tuesday which had been hidden in an unclaimed suitcase used by police officers for canine training exercise almost a month ago on August 14.

The Australian Federal Police has been forced to apologise for the embarrassing and potentially dangerous mishap, however officers say the device was not live.

But the drama didn't end there for the shocked passenger, who immediately took the luggage to the Cessnock Police Station, two hours north of Sydney, where officers temporarily evacuated the building as a safety precaution.

AFP Sydney Airport Commander Wayne Buchhorn has apologised to the travelling public and all those involved in the unusual incident.

'The AFP takes this error seriously and the canine instructor who inadvertently left this device behind has been identified and will be the subject of a formal Professional Standards Investigation,' Commander Buchhorn said.

'Although the travelling public was not in danger at any time, we regularly review our processes in this area, and we will do again in the light of this incident.'

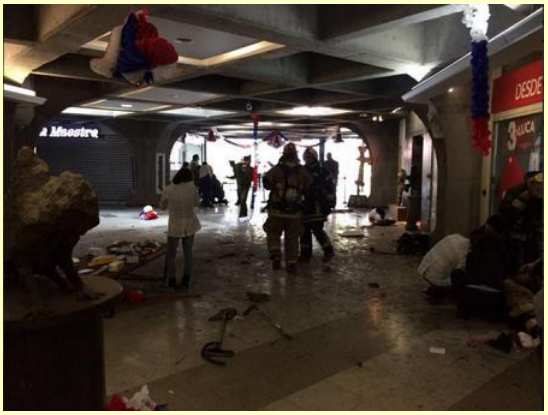
'This type of training is essential for our canine teams, allowing the dogs to experience potential threats in a real environment,' he said.

'On behalf of the AFP, I would like to thank the woman, her family and New South Wales Police, especially officers at Cessnock Police Station, for their assistance in this matter.'

Fire Extinguisher Used as Bomb in Chile

Source: http://i-hls.com/2014/09/fire-extinguisher-used-bomb-chile-14-hurt/

September 08 – A blast ripped through a fast-food restaurant next to a busy subway station in Las Condes, a neighborhood in Chile's capital Santiago, on Monday at lunchtime, injuring at least 14 people in the most damaging of nearly 30 bombings or attempted bombings in Santiago this year.



The injuries were apparently caused by fragments from a fire extinguisher filled with gunpowder that detonated in a trash bin, said fire department Commander Ivo Zuvic Garcia.

According to a report by AP, while no group claimed responsibility for the blast, many past bombings have been claimed by anarchist groups and Chile's government said it would invoke the country's tough anti-terror laws.

President Michelle Bachelet called it an abominable act of terrorism. "That's why we're going to use the full force of justice, including invoking the anti-terrorist law," Bachelet said.

The anti-terror law enacted during Chile's 1973-90 dictatorship lets suspects be held in isolation without charges and permits the use of phone taps and secret witnesses in investigations.

At least 14 people were injured in Monday's attack, according to a list released by local hospitals. The government's emergency medical service said that among those hurt in the blast was a cleaning woman who lost a finger.

Santiago is one of the safest capitals in Latin America, but Chileans have been shocked by at least 29 bombs that have been found across the city so far this year. Some have not gone off and none of the other bombs before this one caused any injuries.

In some cases anarchist groups have said the bombs were planted to demand freedom for two Chilean anarchists imprisoned in Spain for an explosion in a cathedral in Zaragoza last year.

EDITOR'S COMMENT: I think this is a "first" – a fire extinguisher bomb!

Responsibility claim for bombings in Los Dominicos metro station and the Escuela Militar Subcentro underground gallery

Source: http://en.contrainfo.espiv.net/2014/09/19/santiago-chile-responsibility-claim-for-bombings-in-los-dominicos-metro-station-and-the-escuela-militar-subcentro-underground-gallery/

September 18 – **Responsibility claim for bombings in Los Dominicos metro station and the Escuela Militar Subcentro underground gallery:**

Our fraction of the Conspiracy of Cells of Fire (CCF) decided to attack the station 'The Dominicans' of the Santiago Metro on July 23rd. The deed caused a large-scale political and media frenzy. Bureaucrats and the media coordinated their discourses to say that the attack was aimed at passengers who were traveling at that time, and therefore the use of the antiterrorist law was invoked. ***This action was planned taking into account the minutes when there would be no passengers, having calculated the moment that the metro would terminate its journey and the carriage would be stored. The driver moved the bag which contained the device to a different wagon of the metro train, under a seat, as in the other place in which it was initially installed; this situation was concealed by the media and agents of the government.*** *We interpret the foregoing as an attempt of the individual to take advantage of the situation, thinking that maybe he'd find valuables inside the bag, but he ran into our surprise, which turned out as expected.*

As always, any action tending towards attack will be prosecuted and punished by the economic power of businesspeople or members of the bourgeoisie, by the powers of the State with their laws, judges, politicians and cops. The principal function of the State is to protect the interests of the rich and powerful, of the well-off or benefited from this system of exploitation and domination. The metro transports people every day, acquiring huge profits on a daily basis. They transport us through the city that consumes our energy by its mode of life, in which the exploitation of other people's work sets the pace. We directly and symbolically attacked structures of Power on its own turf, in Las Condes. Normalcy by which the city operates has been the target and will remain so.

For this very reason we decided to attack the sub-centre of the 'Military School' metro station on the 8th of September. A shopping centre of the bourgeoisie, located in Las Condes, where businesspeople make their thing to get themselves established and to commercialize their merchandise which traps people in stupefaction of the spectacle and appearances. The society that walks in this direction is what we attacked. The society of domination that pervades all expressions of life. Let it be known that we made warning call to the 133 emergency number over 10 minutes prior to the detonation, waiting for the police to react by evacuating the place, but they ignored this information detonating the device and causing several injuries, which we lament; we make it clear that our target were not the consumers and/or workers, but the structures, properties and minions of Power. Police incompetence and ineffectiveness contributed toward the damage caused to

the injured persons. The greatest assassins and terrorists have always been the repressive apparatuses of the State.
We fraternize with all the comrades throughout the world that confront this reality of domination, and employ all means at hand to attack Power.
We send a greeting to all the comrades who are serving sentences in prisons of the world. Marcelo Villarroel, Freddy Fuentevilla, Carlos Gutiérrez, Juan Aliste Vega, Hans Niemeyer, Tamara Sol Farías, Mónica Caballero, Francisco Solar, Marco Camenisch, Gabriel Pombo da Silva, Alfredo Cospito, Nicola Gai, all the brothers of the CCF around the world, Giorgos Polidoros, Haris Hadjimihelakis, Christos Tsakalos, Gerasimos Tsakalos, Panagiotis Argirou, Michalis Nikolopoulos, Giorgos Nikolopoulos, Olga Ekonomidou, Damianos Bolano, Theofilos Mavropoulos. We greet all those who serve a prison sentence for confronting any domination in actual practice. We remember all those who have fallen in the social war, Mauricio Morales, Sebastián Oversluij, all those who have dared to act… No one is forgotten.
We make a call to all insurrectionaries to go on the offensive, to attack Power in all its forms of domination

***Conspiracy of Cells of Fire** (Chile)*

Who are the Conspiracy of Fire Cells?

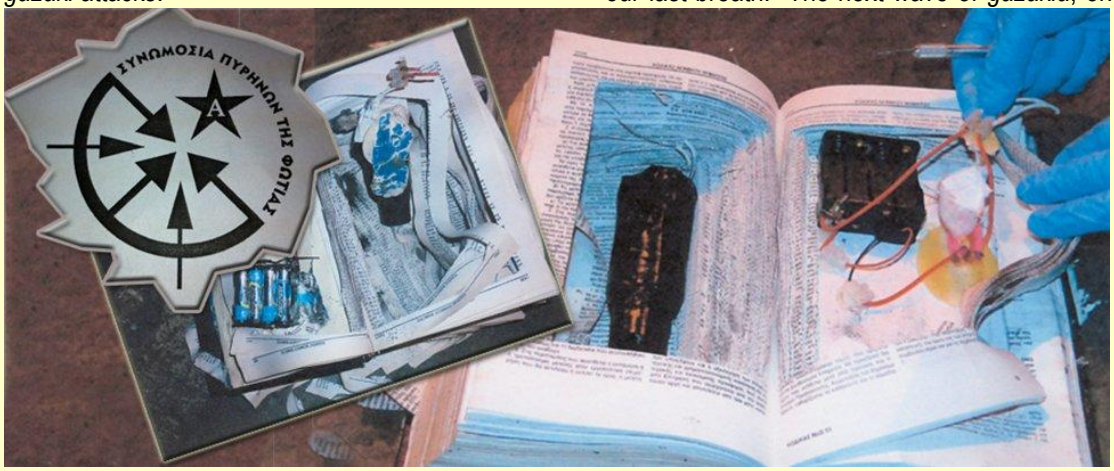
(Fire Nuclei, Synomosia Pyrinon tis Fotias (SPF) – Συνωμοσία Πυρήνων της Φωτιάς)
Source: https://athens.indymedia.org/post/1129729/

The Greek educational system pours thousands of aspiring artists into a status-obsessed, highly politicized society that cannot afford to employ them. Banding together in collective contempt for capitalism and consumer society is one short-term solution.

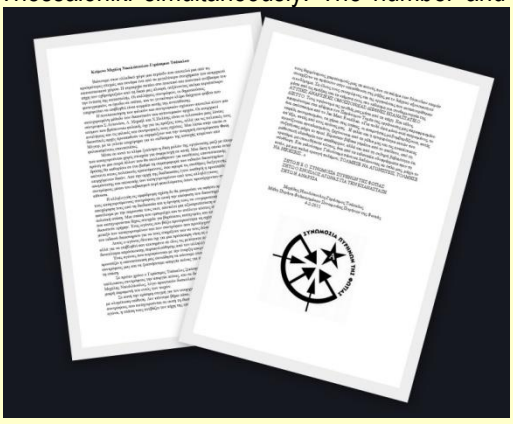
Members cut themselves loose from society's more onerous chains and hang out with age-mates in an abandoned building, ideally somewhere near Exarcheia, the anarchists' traditional neighborhood.
The anti-authority groups function essentially as artists' collectives, maintaining an inexpensive communal lifestyle through intermittent work, grants from tolerant relatives, or bank robbery. Within that counterculture, anti-authority violence is a rite of passage, multi-media performance art, and a chance for young males to rank themselves against their peers in an informal but intense status competition. Despite a rhetoric of self-liberation through destruction, the anarchist/antiauthority movement is too small, too anti-hierarchical, and (usually) too respectful of comrades' moral redlines to wage serious war on the system.
Since the end of the 1970s, antiauthority groups in Athens routinely engage in stone-throwing, window-smashing, and fire-raising whenever a protest has attracted sufficient critical mass to take shelter behind. On non-demonstration days, an uneasy ceasefire prevails, with police and "anarchists" avoiding each other's territory. When members or friends are arrested by police, or when a group's territory is infringed, that group retaliates by humiliating the police.
A small group on motorcycles, with an expansive view of what constitutes legitimate targets, can quickly prove the powerlessness of the police to defend private property or even their own police stations. Apart from gasoline bottles, the usual tool is a *gazaki* (in simplest form a propane gas canister wrapped in a petrol-soaked rag) placed to destroy a car or ATM. The better-organized groups

publish short proclamations on sympathetic web sites to explain those attacks.

The "Conspiracy of Fire Cells" (*Synomosia Pyrinon tis Fotias* -- SPF) was an attempt to increase the political impact of anti-authority violence. SPF appeared on January 21, 2008, with a barrage of 12 gas canister attacks against widely dispersed banks, car dealers, and the Public Power Company in Athens and Thessaloniki, during a half-hour period just after midnight. The declared purpose was solidarity with Thessaloniki anarchist Vangelis Voutsatzis, arrested in November 2007 for *gazaki* attacks.



For the next 20 months, SPF averaged one arson wave a month, usually in Athens and Thessaloniki simultaneously. The number and



coordination of SPF's attacks - presumably six or more 4-6-person teams on motorbikes - alarmed police. SPF's retaliatory capabilities were an additional reason for Greek police to think twice about arresting "anarchists" for any but the most blatant and serious crimes.

Solidarity with local and foreign anarchists and hatred of banks, police, prisons, the army, and consumer society are the themes of SPF's 22 (as of 30 October 2009) extant proclamations. SPF is uninterested in class struggle and the quest for a future utopia. The proclamation writers embrace urban warfare not as a means to an end but as an end in itself, resistance as art. Modern consumer society is "slow suicide." "The revolutionary element of arson is not only in its material destruction but also in the transgressiveness of the act."

The December 2008 events overwhelmed the anti-authority movement with new recruits hungry for a revolutionary program. Forced to broaden its aims, SPF pledged to join with other groups and wage a "new, rabid (*lyssasmeno*) urban warfare ... now and until our last breath." The next wave of *gazakia*, on February 11, 2009, was the first SPF attack to capture major public attention, because it served the media's breathless narrative of reborn Greek terrorism. SPF struck targets with (loose) connections to the 17N prosecution, and dedicated those attacks, in a long, newly sophisticated proclamation, to jailed 17N spokesman Dimitris Koufodinas.

Responsibility claim for parcel bombs in Greece

In May 2009 SPF escalated its capabilities with its first use of home-made explosives, causing minor damage to two police stations under construction in Athens and Thessaloniki. The proclamation was a more mature theoretical tract on upgrading "revolutionary terrorism" (*terorismos*, a word other groups rigorously avoid). In June, a small time bomb (home-made gunpowder in a glued-shut pressure cooker) was hung from a staircase outside the home of ex-deputy minister of public order Hinofotis. SPF and "Nihilist Fraction" jointly claimed responsibility. On September 2, a similar bomb caused trivial

damage to the heavily-guarded Ministry of Macedonia-Thrace in Thessaloniki. Another damaged the door of PASOK MP candidate Louka Katseli on September 23.

A presumed SPF safe house in Halandri was already being watched by police before the Katseli bomb. When police raided the house that same afternoon, they found one ready pressure-cooker bomb and various bomb-making scraps. Four young people, age 20-21, were arrested. One is a self-proclaimed revolutionary anarchist, Panagiotis (Panos) Masouras. The others are students from prosperous backgrounds: Haris Hatzimichelakis, the owner of the apartment; his cousin Manos Giospas, a design student who lives with his mother upstairs; Manos's girlfriend, a photography student. Six others, sought on the basis of fingerprints found there, have been hiding from police since the date of the raid. Police are detaining the three young men in in hopes the guilty will confess to spare (probably) innocent friends years in prison as members of a terrorist organization.

On October 2, 2009 SPF and "Nihilist Fraction" struck back with another pressure cooker bomb, that destroyed two motorbikes and broke windows while Prime Minister Karamanlis was giving his final election speech in the Pedio tou Areos 150 meters away. Their purpose was to deny the government any electoral benefit, proving the four arrests were not a breakthrough against SPF. A similar bomb protesting the educational system did minor damage to the entrance to the unguarded apartment building of MEP (former ND Education Minister) Marietta Giannakou on October 30, 2009.

On December 27, 2009, a four-person team struck again, with a much more powerful bomb that destroyed the entrance of a building on Syngrou Blvd. housing the **Ethniki Asfalistiki** insurance company and a National Bank of Greece branch. A warning call to a newspaper reduced the risk of casualties. The proclamation claiming credit was signed **Guerilla Team of Terrorists/SPF**. The group claimed to have gained access to powerful explosives through cooperation with other revolutionary comrades. This new combination of violent anti-consumerist ideology and powerful explosives is alarming.

It may be a mistake to look for a formal membership of SPF. A more likely model is groups of friends, each with a specific set of motivations, which seek the blessing of an original SPF nucleus before using the name. One of SPF's main writers is older than 25, capable of disciplined, analytical Greek and with enough historical knowledge to make valid comparisons with Greece and Italy of the 1980s and 1990s. Others are less mature, more "poetic" in their embrace of a Nietzschean cult of violence:

"We execute morality, prefacing catastrophe, whispering rabidly, biting the words: WAR ATTACK because only beauty and strength exist, but the cowards to balance [them] invented justice."

Links with Other Groups

Greek police routinely try to link armed groups into a single umbrella organization, ignoring the philosophical differences reflected in their manifestos. The upgraded SPF hoped to help form such an umbrella, writing in February 2009 "Here there is no room for agreement or disagreement on political correctness. The important thing is our eyes behind the hoods, shining so beautifully when we fight." SPF announced in May 2009 that it had joined a new "Arsonists' Cooperative." A month later the Cooperative had vanished. However, cooperation with the "Nihilist Fraction" continues. SPF may have absorbed **"Gangs of Conscience"** (*Symmories Syneidisis* - SymSyn), which surfaced in March 2008 with a molotov attack on the Aigaleo police station. SymSyn proclaimed the "new urban guerrilla war" in December 2008, but dropped out of sight after its March 3, 2009 torching of two metro trains prompted public fury.

SPF's pressure-cooker bombs resemble four bombs planted by **Armed Revolutionary Action** (Enopli Epanastatiki Drasi - ENEDRA) in 2007-9. ENEDRA, with its "collective vision" -- a self-governed society in harmony with nature -- would find SPF unpleasantly militarist. The real explosives used in the December 2009 bombing could point to help from Revolutionary Struggle (EA). However, ideological differences would impede close collaboration. EA would be uncomfortable with SPF's nihilism and rejection of class consciousness while SPF would find EA's proclamations unreadable.

SPF carefully refused (July 2009 Hinofotis proclamation) to criticize **Revolutionary Struggle** (EA) and **Sect of Revolutionaries**

(Sehta) for their deadlier violence. Still, SPF never echoed Sehta's ostentatiously brutal contempt for life, despite their shared rhetorical "nihilism." For bombs, SPF typically calls in two separate telephone warnings.

Most rebels of Exarcheia lack the sense of long-term mission (and also the memory of Junta-era police torture) that kept traditional leftist revolutionaries like 17N disciplined and vigilant. After the September 23 arrests, it became clear that SPF (or at least its suburban fringe) violated basic security rules of the underground armed struggle: using mobile phones, keeping incriminating materials where they lived, and being conspicuously involved in protests.

By their nature, anti-authority groups that espouse ambitious violence tend to be short-lived. Christos Tsoutsouvis and Mihalis Prekas, still the Greek poster children for "anarchist" violence, undervalued their own lives as well as others'. They were both shot dead by police mere weeks after their organizations were launched in 1985 and 1987 respectively. SPF has gone beyond the territorial/tribal goals of most anarchist groups to challenge the Greek political establishment. The September arrests will probably drive its members underground. If not, SPF is likely to be broken up relatively quickly.

*"Anarchist" is a generic term used by the Greek media and police to refer to ominously dressed youth who congregate in Exarcheia area (Athens' downtown) and throw rocks at police. True anarchists (as opposed to children who like to paint the symbol on walls) are a minority in Exarcheia's wide spectrum of anti-establishment ideologies from libertarian socialism to murderous nihilism. Members often use the term "antiexousiastes" (anti-authoritarians).

EDITOR'S COMMENT: Above description of this terrorist group is from an article written by an American diplomat stationed in Athens, Greece (Diplomacy Lessons John Brady Kiesling, former U.S. Foreign Service Officer Athens – Feb 7th, 2010). Indymedia/Athens (branch of international "Independent Media Center – IMC"), is the "official website" that hosts all "anarchists'" activities mostly in Athens metropolitan area. Its server is alleged to be "hosted" within Athens' Polytechnic School…

Cyber war needs cyber soldiers

By Nicholas Stuart

Source: http://www.brisbanetimes.com.au/comment/cyber-war-needs-cyber-soldiers-20140822-1072pd.html

Cyber war: the aim is not just to destroy; the requirement is for a carefully targeted campaign.

Major General Steve Day, deputy director Cyber and Information Security at our secretive Australian Signals Directorate (motto: "reveal their secrets, protect our own") reckons he's exactly the right person for his current job. Not because he's a computer geek though; nor because he's a former combat engineer. Not even because he's spent time in Iraq and Malaysia. As he told a University of Canberra National Security lecture last week, "I am an ordinary garden variety soldier. I have no special expertise in cyber ... I actually think that's an advantage."

His reasoning's simple, but it's an argument with big implications. Day believes it's vital the person looking after cyber-security can think broadly without being trapped in the minutiae of tactical issues. After all, cyber is just a means, not an end. Compare it to a bombing campaign: the aim is not just to destroy; the requirement is for a carefully targeted campaign. Cyber war won't occur as such – it's just one method of disruption and destruction.

I reckon he's right. But it's important to note this is not the approach of either superpower. The US Army Secretary has announced he's considering establishing a new branch or corps for computer warriors. This is forward-thinking. After all, entrenched institutional resistance inhibited the development of armour after World War I and stopped the US Airforce becoming independent. Soldiers jealously guard the old way of doing things – swords and plumes on parade, anyone?

The US won't be left behind again. So how can we reconcile the different thinking skills that are required at different levels of command? Why is it an advantage to think flexibly at a senior level when we demand uniformity from other junior ranks? The critical factor is the individual. As Day points out, this is where the ability to fight well resides. Military structures are vital for achieving defined missions; this doesn't mean they can work out what the political aims and objectives are or should be. This requires different skills. We churn out brilliant officers to the rank of Lieutenant Colonel. They've got exactly the right combination of time in command, training and other appointments. But then something happens. A mysterious fog descends, enveloping all those bright young officers in a mist. By the time they emerge many (although not all) are sclerotic, rigid individuals who can't think outside the square.

That's why there's an urgent need to rethink the training of officers and commanders. If it's another week, there's another ADFA sex scandal. But what's utterly bizarre

is that the military defend an education system that's not only out-of-date and irrelevant but was foisted on the services, against their will, to begin with.

Originally officers in all three services were (only) taught military skills required for war. Eventually the army decided it needed to lift its game to attract better quality applicants. It began offering degrees at Duntroon. The airforce and navy were later forced to send their cadets to the Academy in the interests of "jointery". Now it's an expensive anachronism with a reputation standing as a barrier that prevents good young people joining the services. ADFA provides nothing that isn't offered better at civilian universities, yet it costs us almost half a million dollars to graduate each and every officer cadet. Even that outlay doesn't guarantee progression to the highest ranks. Take the army, for example.

Lieutenant General Andrew Morrison has done more to restore its reputation with a single *YouTube* video appearance than any general since 1945 – yet he was educated at Melbourne University. Our former commander in Afghanistan, John Cantwell, began his military career as a soldier. Previous army chief Ken Gillespie began his service as an apprentice. Other senior officers, such as Angus Campbell, have transitioned through long careers wearing suits. To the best of my knowledge, only one of our current crop of generals possesses the ability to speak Ancient Greek. Now while I'm certainly not suggesting this should be a prerequisite for command, a detailed understanding of how the disciplined Macedonian phalanx with its cavalry overwhelmed the democratic city-states of the south probably illuminates the issues involved in fighting ISIS far more clearly than a thesis on the campaigns in North-West Europe in 1945. Even Day escaped the rigid, four-year indoctrination of Duntroon by graduating from Portsea. And this is the point that he was making. The skills required to win tactically won't deliver strategic victory.

This is something we might have learned after Vietnam. Or perhaps Iraq. Or maybe Afghanistan. Yet it seems we haven't. Our generals are the best trained who've ever left our shores in command of troops and yet somehow the structures and systems prevent them achieving their objectives. The structure needs to change.

The evidence is in. ADFA should, must, be re-purposed to provide something more appropriate. Dynamism needs to be injected in at a senior level. Our military needs to be allowed to thrive. It's sometimes difficult, when you're trapped inside the pyramid, to understand how it can be changed for the better, but the first step is simple.

***Nicholas Stuart** is a Canberra writer.*

Chinese Programmer Gained Access to Arizona's Terror Center

Source: http://www.hstoday.us/single-article/chinese-programmer-gained-access-to-arizonas-terror-center/e190e0bb8194fde35c1028b77901e2e2.html

For five months in 2007, an unvetted Chinese computer programmer plugged into law enforcement networks and a database of 5 million Arizona drivers in a possible breach that was kept secret for years, according to a new report.

▶ **Read the full report at:**
http://www.propublica.org/article/lizhong-fan

Black Hat 2014: The 10 Commandments of Modern Cybersecurity

By Hilton Collins

Source: http://www.emergencymgmt.com/safety/Black-Hat-2014-Commandments-Modern-Cyber security.html

At the Black Hat USA 2014 conference at Las Vegas' Mandalay Bay Resort and Casino, security is the main event. And in that vein, Dan Geer, the chief information security officer of nonprofit investment firm In-Q-Tel, shared 10 cybersecurity policy recommendations during his keynote speech on Wednesday, Aug. 6.

Geer, the conference's first and only keynote speaker, framed his recommendations within the context of today's confusing, precarious cybersecurity landscape amid diminishing personal privacy and increased government spying and surveillance.

He read an hour-long essay to thousands in attendance, addressing a crowd who represented, in his opinion, an industry that's becoming more and more prominent in public policy because of software's ubiquitous presence in every facet of modern life. The security of the technology that supports society is something no one can ignore, but cyberthreats are so constant and pervasive that accomplishing total privacy and security seems futile

Geer opened his talk by reading aloud the abstract for his speech, which summed up the importance of cybersecurity policy, even as strong cybersecurity itself seems almost impossible to achieve.

"Power exists to be used. Some wish for cyber safety, which they will not get. Others wish for cyber order, which they will not get," Geer said. "Some have the eye to discern cyber policies that are, 'The least worst thing.' May they fill the vacuum of wishful thinking."

Geer's cybersecurity advice was comprehensive and called for more accountability — and less legal leeway — for software vendors and their technology's source code.

Geer said that the following 10 policy proposals were his and his alone, based on his experience in the industry. He also gave a verbal disclaimer that listeners were free to disagree and attempt to prove him wrong on these ideas, in the interest of greater legal and personal agency in the never-ending cybersecurity effort.

1. Create a mandatory reporting system for severe breaches, similar to how the United States Centers for Disease Control and Prevention has a mandatory reporting system for medical diseases. If the breaches are less severe, then reporting should be voluntary.
2. Offer Internet service providers one of two net neutrality options. Providers can charge customers for service, but that also makes the providers responsible for the harmful content within that service. Providers can alternatively choose a "common carrier" option that frees them from liability for damaging content, but they're unable to inspect or act on the contents of what they carry.
3. Make software developers legally liable for their source code. Under the regulation procedures, developers should give buyers the ability to disable pieces of code they don't want to use, and the developers are held liable for any damage their software causes under normal usage.
4. Strike back at attackers when necessary with cyber counter attacks or targeting campaigns to truly identify the attackers. The ability to do this, however, will require entities to share infrastructure and resources because not every organization has the power of Microsoft or the federal government.
5. If people have no way to remotely shut down computer systems when necessary because those systems are too deeply embedded, then those embedded systems should be designed with the ability to self-terminate after a fixed amount of time has passed, and computer systems that can be remotely controlled should be

designed with the ability to refuse certain remote commands for security purposes.

6. The government should pay people competitively for finding vulnerability exploits, and then make those exploits public.
7. Uphold people's right to be forgotten and operate autonomously, even as a connected society makes this increasingly more difficult, and give people the ability to misrepresent themselves online under certain circumstances to confound those who would "watch" them digitally.
8. Voting online is a bad idea because it opens the process and results up to cyber manipulation.
9. Software code should be open sourced after companies discontinue it and stop releasing updates for it. The open source community can patch and update software code for the greater good if companies decide that the code is no longer useful.
10. Critical infrastructure systems' dependence on the Internet and electrical grid leaves them open to cyberattack, so their managers and network administrators should find ways to operate them off the grid, if necessary.

Geer concluded his speech by espousing political realism. The international world is anarchic when cyberspace is involved, and governments are the most important players in the digital world.

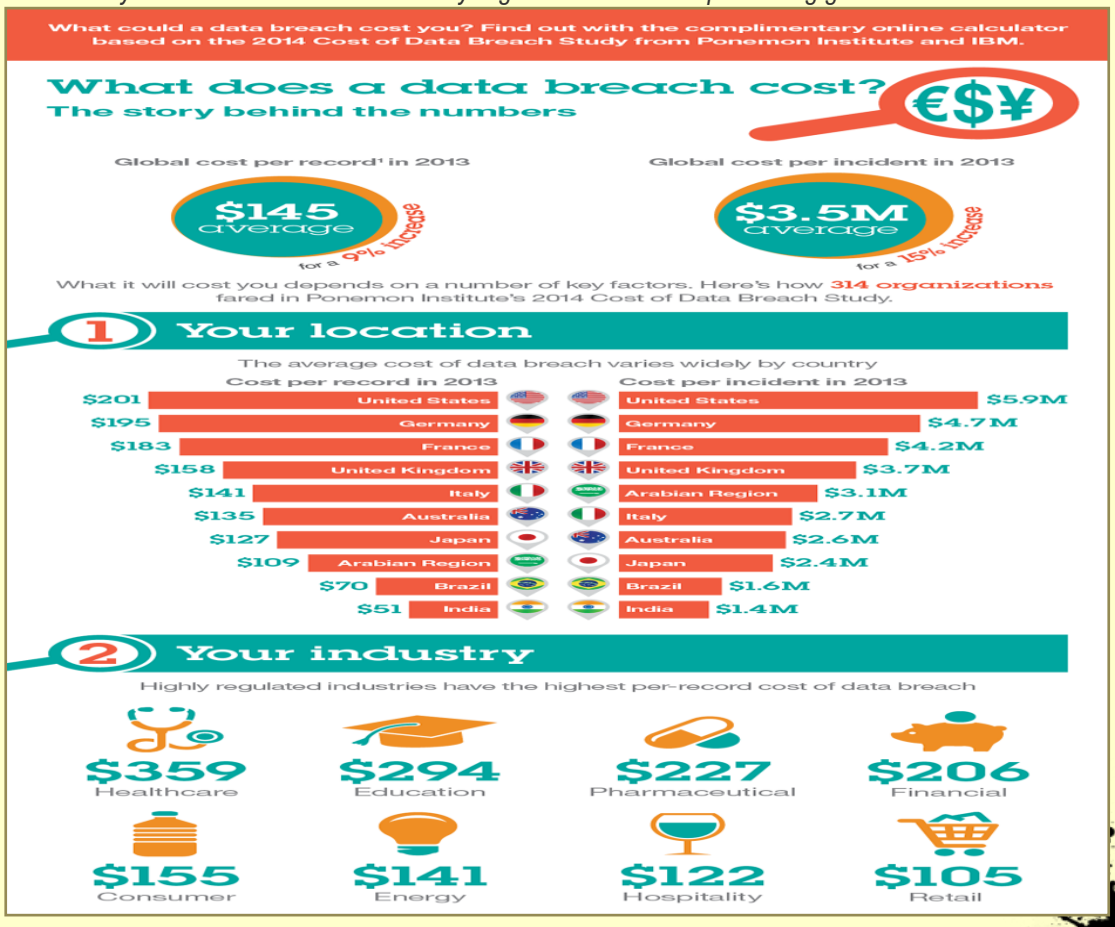
"States' investment in offensive cyber is entirely about survival in such a world," he said. **"States are driven to this by the dual, simultaneous expansion of what is possible and what their citizens choose to depend on."**

***Hilton Collins** is a staff writer for* Emergency Management *magazine.*

Data Breach Risk Calculator

Source: http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach-risk-calculator-infographic/index.html

This survey examines the costs incurred by organizations after experiencing genuine data loss incidents



Find out how much a data breach can cost your organization.

Social networks aim to curb terror posts

Source: http://www.homelandsecuritynewswire.com/dr20140828-social-networks-aim-to-curb-terror-posts

Following the posting of the beheading of American journalist James Foley by the Islamic State of Iraq and the Levant (ISIS), analysts are pointing to the emerging role of social media in the tactics and response to terrorism.

As the *Los Angeles Times* reports, as social media platforms such as Facebook, YouTube, Twitter, and Instagram have all become a staple of everyday Western lifestyles – and these avenues have also become more interesting for terrorists to exploit to advance their goals.

"Social media is at the heart of their jihad," said Steve Stalinsky, the executive director of the

Middle East Media Research Institute.
As was the case with the Foley execution

{Image produced by ISIS supporters}

video, the use of posting on these platforms is meant to instill fear, attract the eyes of those who might be recruited, and raise money through awareness.

Now, however, three of those large social media companies — YouTube, Twitter, and Facebook — are choosing to remove extreme examples of violence and terror. Users, too, are incorporating campaigns to filter and not give terrorists the upper hand with digital coverage.

Once the Foley video began to circulate, YouTube blocked the video, arguing the company prevents the posting of videos on many subjects, such as weapons construction and violence.

"YouTube has clear policies that prohibit content like gratuitous violence, hate speech and incitement to commit violent acts," said a company spokesperson, "We also terminate any account registered by a member of a designated Foreign Terrorist Organization and used in an official capacity to further its interests."

Twitter and Facebook users also aimed to curb the sharing of the video out of respect for the victims and prevent ISIS from gaining notoriety. The **hashtag "#ISISMediaBlackout** quickly began to trend on both services.

Facebook reports that it has "teams around the world" that are reviewing content related to the Foley beheading, and in certain cases leading to the company is removing the posts.

These companies admit, however, that curbing free speech and screening violent and hateful content does involve walking a fine line.

"The problem is that the boundary is hard to define," said Marvin Ammori, a First Amendment scholar and a fellow at the New America Foundation.

EDITOR'S COMMENT: Internet provides information as text, pictures and videos aiming to inform and wake up people and societies. So far thease means of info sharing did not manage to wake up civilized societies that still feel safe from a disease emerging far away from home. But this disease is viral and airborne and if we stop having this info we might think that local "medical" services managed to contain the epidemic. If that also serves terrorists goal (recruiting) and sustaining their illusion that they will change our world it is OK with us that we still need some time to wake up from our lithargy…

Researchers work to harden cyber infrastructure from WMD

By Kathleen Hickey

Source: http://gcn.com/articles/2014/08/27/unm-dtra.aspx

The Defense Threat Reduction Agency (DTRA) is funding a project by the University of New Mexico (UNM) to conduct field tests into recovery solutions for cyber-infrastructure attacks under realistic, real world conditions, including the threat of weapons of mass destruction.

Nasir Ghani, Associate Chair of the Electrical and Computer Engineering Department and Majeed Hayat, Associate Director of the UNM Center for High Technology Materials, received the 2-year award for a project titled, "Implementation Paradigms for Survivability of Cyber-Infrastructure Backbone Networks Against WMD Attacks Over Real Network Environments."

The testing is based on prior research done by UNM funded under an earlier DTRA Basic Research award. The contract covers research into the design/evaluation of robust

counter-WMD solutions "to implement novel survivability algorithms and validate their effectiveness in "live" distributed backbone networks under emulated WMD stressors," the FedBizOpps announcement said.

"Modern backbone cyber-infrastructures are comprised of multiple technology domains/layers and support scalable connectivity across large distances," a UNM article explained. "However, most existing recovery schemes focus only on single or limited dual node/link failures." The focus of this new research is to conduct field trials of new recovery paradigms and validate and harden their performance in realistic settings.

Multiple network failures, such as might occur during a natural disaster or WMD attack, would be a catastrophic event and jeopardize national security and the economy.

The first part of this effort focused on implementing detailed algorithms inside distributed networking protocol stacks. The latest research will focus on designing and running detailed test-case scenarios to validate these schemes for a wide range of disaster conditions over live network infrastructures.

As part of this effort, the UNM team will also partner with Tom Lehman and Xi Yang at the Mid-Atlantic Cross-Roads Gigabit Point-of-Presence facility (MAX) at the University of Maryland College Park. The MAX networking facility hosts and has access to a wide range of research cyber-infrastructures for detailed testing and evaluation purposes.

Cyber-infrastructure security has been identified as a top priority by the White House for years and has drawn the interest of Congress as well. Late last month the House passed three bills to address cybersecurity and critical infrastructure: H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act; H.R. 2952, the Critical Infrastructure Research and Development Advancement Act; and H.R. 3107, the Homeland Security Cybersecurity Boots-on-the-Ground Act.

"A successful cyberattack on our nation's water systems, oil and gas pipelines, power grids and mass transit systems on the scale of the recent retail breaches could cause crippling economic damage and could even cost lives. The reality of the threat is outpacing our readiness to combat it," said House Homeland Security Committee Chairman Michael McCaul (R-Texas).

CyberThreat Real Time map

"The cyber risk is among the most serious our nation faces today. Terrorist groups like Hamas, nation-states like Iran, China and Russia and criminal gangs across the world are constantly attempting to breach our systems. But existing laws that have been on the books for years are not designed to cope with the threat," added subcommittee chairman Patrick Meehan (R-Pa.).

Cyberthreats are becoming not only more dangerous, they are falling into the hands of more people, said former White House security advisor Tom Donilon, speaking at FOSE in May. Protecting critical infrastructure is the joint responsibility of the public and private sectors, he added.

A survey by Unisys Corp. and Ponemon Institute released in July found critical infrastructure

providers in the utility, oil and gas, energy and manufacturing sectors unprepared for both internal and external threats, with nearly 70 percent of survey respondents experiencing breaches in the past year.
Sixty-four percent of the 599 security executives surveyed expect one or more serious attacks in the coming year, yet only 28 percent ranked security as a top five strategic priority for their organization.
A visual representation of the scale of cyberattacks can be found on Kapersky Lab's site, which has a real-time global cyberthreat map based on its data.

▶ **Watch the Real Time CyberThreat Map at:** http://cybermap.kaspersky.com/

***Kathleen Hickey** is a freelance writer for GCN.*

Four DARPA projects that could change the world

Source: http://i-hls.com/2014/08/four-darpa-projects-change-world/

Forty years ago, a group of researchers with military money set out to test the wacky idea of making computers talk to one another in a new way, using digital information packets that could be traded among multiple machines, pointto-point circuit relays. The project, called ARPANET, went on to fundamentally change life on Earth under its more common name, the Internet.
Today, the agency that bankrolled the Internet is called the Defense Advanced Research Projects Agency, or DARPA, which boasts a rising budget of nearly $3 billion, according to the *defenseone.*
Split across 250 programs. They all have national security implications but, like the Internet, much of what DARPA funds can be commercialized, spread and potentially change civilian life in big ways that its originators didn't conceive.

Game Changers 66

The next four projects, led by DARPA may change the picture:

1. ATOMIC GPS

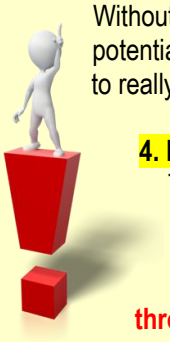
The Global Positioning System, is a great tool but maintaining it as a satellite system is increasingly costly. A modern GPS satellite can run into the range of $223 million. DARPA-funded chip-scale combinatorial atomic navigation, or C-SCAN, and Quantum Assisted Sensing. If you can measure or understand how the Earth's magnetic field acceleration and position is effecting individual atoms (reduced in temperature), you can navigate without a satellite. In fact, you can achieve geo-location awareness that could be 1,000 times more accurate than any system currently in existence.

2. TEREHERTZ FREQUENCY ELECTRONICS AND META-MATERIALS

The area of the electromagnetic spectrum between microwave, which we use for cell phones, and infrared, is the Terehertz range. Today, it's a ghost town, but if scientists can figure out how to harness it, we could open up a vast frontier of devices of that don't compete against others for spectrum access. Research into THz electronics has applications in the construction of so-called metamaterials, which would lend themselves to use in cloaking for jets and equipment and even, perhaps, invisibility.

3. A VIRUS SHIELD FOR THE INTERNET OF THINGS

The High Assurance Cyber Military Systems program, or HACMS, is trying to patch the security vulnerabilities that could pervade the Internet of Things. The agency wants to make sure that military vehicles, medical equipment and, yes, even drones can't be hacked into from the outside. In the future, some of the software tools that emerge from the HACMS program could be what keeps the civilian Internet of Things operating safely.



Without better security, many experts believe the Internet of things will never reach its full potential. In a recent survey, Internet pioneer Vint Cerf, said that in order for the Internet of things to really revolutionize the way we live it must be secure.

4. RAPID THREAT ASSESSMENT

The Rapid Threat Assessment, or RTA, program wants to speed up by orders of magnitude how quickly researchers can figure out how diseases or agents work to kill humans. Instead of months or years, **DARPA wants to enable researchers to "within 30 days of exposure to a human cell, map the complete molecular mechanism through which a threat agent alters cellular processes,"** Prabhakar said in her testimony.

Why Terrorists Love Twitter

Source: http://time.com/3319278/isis-isil-twitter/

In 2011, the Somali Islamist group known as Al-Shabab took to Twitter. Its official handle taunted the group's enemies, boasted of battlefield triumphs and shared images from the front lines of conflict zones. It sparred with political antagonists, rattling off missives in grandiose English. The terrorists—like the site's less murderous users—used Twitter to share news and promote their brand. In 2013, a Shabab account live-tweeted commentary as allied fighters carried out a terrorist attack at a Nairobi shopping mall.

Terrorists love Twitter. That includes the Islamic State of Iraq and Greater Syria (ISIS), the Sunni Muslim extremists whom the U.S. is targeting in an expanded military campaign. ISIS has emerged as the most sophisticated group yet at using the service to spread its bloodthirsty message. And when ISIS jihadists and tens of thousands of acolytes swarmed Twitter in recent months, it raised the question of how social media sites should respond when unsavory groups colonize their platform.

There are no easy answers. Social-media networks exist so users can share information; sites like Twitter are neither equipped nor inclined to police large numbers of rogue feeds themselves. And within the intelligence community, there is no consensus on whether the use of sites like Twitter as a propaganda tool hurts or helps U.S. interests.

To some observers, Twitter was derelict in allowing extremist accounts to flourish. "For several years, ISIS followers have been hijacking Twitter to freely promote their jihad with very little to no interference at all," says Rita Katz, director of the SITE Intelligence Group, which studies jihadi extremists' behavior online. "Twitter's lack of action has resulted in a strong, and massive pro-ISIS presence on their social media platform, consisting of campaigns to mobilize, recruit and terrorize."

Others say it's not so simple. "There is a case to be made for removing the content or removing the most prolific [jihadist] accounts online. Each time that happens, they had to rebuild their audience. It has a disruptive effect," says counterterrorism expert Clint Watts, who has studied ISIS's behavior online. But ISIS accounts may also, in some cases, be a boon to intelligence-gathering efforts. "Their braggadocio tells us what we don't know about what's happening in eastern Syria," Watts says. "In Iraq they show us every one of their successes. There is value in that."

For that reason, some government officials may prefer the accounts remain open. "There is some value to being able to track them on Twitter," says William McCants, a former State Department senior adviser who directs the Project on U.S. Relations with the Islamic World at the Brookings Institution. McCants recalls that a U.S. intelligence official described the site as a "gold mine" of information about foreign-fighter networks, better than any clandestine sources. The State Department is using Twitter itself, with a counter-propaganda campaign run through an

account, Think AgainTurn Away. It tries to nettle ISIS and neutralize their recruiting.

A Twitter spokesperson declined to comment for this article. The site's rules prohibit threats of violence, harassment and other abuses, and government agencies or law enforcement officials are able to request the removal of prohibited content. In 2013, it received just 437 such requests from governments worldwide; it received 432 in the first half of this year.

In recent months, Twitter has cracked down on some accounts, including those sharing macabre images or videos of the beheading of American journalists James Foley and Steven Sotloff. But it is not trawling for the content that some government officials believe has the greatest potential to convert potential conscripts. "This is not necessarily a bloody picture. It's somebody telling you to go kill," says Alberto Fernandez, coordinator of the State Department's Center for Strategic Counterterrorism Communications, whose digital outreach team is responsible for the Twitter counter-messaging campaign. "That discussion is not being taken down by Twitter."

It's easy to see why terrorists flocked to the platform. Beginning in the mid-2000s, al-Qaeda has been organizing online through bulletin-board forums, which were largely password protected and sometimes required special contacts to gain access. Moderators would scrub signs of dissension. In contrast, Twitter is something of a digital town square—a free megaphone to reach a mass audience, easily accessible on smartphones and largely unmonitored.

As ISIS fighters began capturing vast swaths of Syria and Iraq this summer, its network of online organizers—there are around 30 key players, according to analysts who study global extremism online—tweeted about territorial gains, posting photographic proof of their conquests. They softened their hard-edged image by sprinkling in common humanizing touches, like pictures of meals and cute cat photos. And they set about trying to recruit more conscripts—including Westerners—to the cause.

It may seem incongruous; religious extremism is in large part a renunciation of modern society, while the social-media platform is both emblem and enabler of the networked world. But since it is impossible to scrub all pro-ISIS sentiment from Twitter, U.S. analysts are trying to use the service to piece together a better understanding of the terrorist group's dynamics. Twitter's decision to silence some accounts but not all is fine, McCants says, and watching the group latch onto a new account when a big one is blocked can be instructive. "When you knock one of them down, it's interesting to see how quickly they reconstitute and who their earliest followers are," he says. "Those are the guys that are plugged in."

Back in time...

Developer: Adam Osborne;

Type: portable computer;

Release date: 3 April 1981;

Introductory price: US$1.795;

Discontinued: 1983;

Operating system: CP/M;

CPU: Zilog Z80 at 4.0 MHz;

Memory: 64 kB;

Weight: ~11kg

Growing cyberthreats lead to growing interest in cybersecurity insurance

Source: http://i-hls.com/2014/09/growing-cyberthreats-lead-growing-interest-cybersecurity-insurance/

The increasing sophistication and scope of cyberattacks on businesses – and the increasing damage such attacks are causing – have led to growing interest in cybersecurity insurance. The industry is urging the government to treat cyberattacks as acts of terrorism which should be covered under the Terrorism Risk Insurance Act (TRIA), while also looking into how the Stafford Actcould help companies after a cyberterror attack. At the same time, more private insurers are offering limited cyber-coverage, but many say they would discontinue selling cyber policies if TRIA is not renewed. As the term "cyber-coverage" continues to be defined by large insurers, the insurance product lines continue to change, the homelandsecuritynewswire reports.

Following last week's news of a cyberattack on JP Morgan, in which hackers stole gigabytes of data from the bank's network, U.S. regulators are stressing the importance of better cybersecurity measures, while bankers are calling for an improved federally backed cybersecurity insurance plan for the financial industry.

Former DHS chief Janet Napolitano said in her valedictory speech that the country will someday suffer a cyber 9/11 "that will have a serious effect on our lives, our economy, and the everyday functioning of our society." Since then, banks have hired security consultants and invested in top cybersecurity initiatives, but even the most secured institutions are vulnerable to hacking, so banks are requesting the federal government to play a larger role.

The Terrorism Risk Insurance Act (TRIA), enacted after 9/11, authorizes the government to cover up to $100 billion in losses due to a terrorist attack after insurers cover a fixed amount of losses. As recently as last year, insurers were asking Congress to include cyberattack coverage in the reauthorization bill.

The law, which is up for renewal in the House, would treat cyberterror as a physical attack, according to people involved in the renewal talks. Representative Jeb Hensarling (R-Texas), chairman of the House Financial Services Committee, which is holding discussions on TRIA, wants to limit and eventually do away with TRIA, so for now insurers have dropped their request of adding cybersecurity language to the law. "The industry doesn't want to open that fight up," said Mark Calabria, director of financial regulation studies at the Cato Institute. "It would jeopardize renewal altogether."

UK launches online course to promote security in cyber space

Source: http://www.out-law.com/en/articles/2014/september/uk-launches-online-course-to-promote-security-in-cyber-space/

The UK has launched the first government-supported online course to "inspire and educate" the next generation of cyber security professionals.

The free 'Massive Open Online Course' (MOOC) is backed by the UK's National Cyber Security Programme, which is investing £860 million over five years to protect and promote the country in cyber space.

MOOC, launched by the Department for Business Innovation & Skills on 3 September, has been developed with the Open University (OU). The University has worked with government agencies, including the UK intelligence and security organisation GCHQ, to develop the course, which will be available on FutureLearn.com, a platform

which hosts free online courses from a range of UK and international universities.

The course has the potential to reach 200,000 students and ensure the UK "has the knowledge and capability to meet current and future challenges", the Department said. "It will also help to raise awareness of cyber security amongst the general public."

The Department said the 'Introduction to Cyber Security' course is open to anyone with access to the internet and will cover subjects such as network security, the threat landscape, cryptography, malware and how to manage security risks. MOOC does not lead to a formal qualification.

"The course will enable anyone, from young people considering study or a career in computing, to existing employees wanting to improve their knowledge and skills, or members of the public interested in staying safe online, to gain an insight into cyber security and have the opportunity to take their interest to the next level," the Department said.

UK minister for culture and the digital economy Ed Vaizey said Britain's "vision for a vibrant, resilient and secure cyberspace, contributing to economic prosperity, national security and a strong society, can only become a reality if we have a strong cyber security skills base in the UK, both within government and the private sector."

Vaizey said: "Employers are looking for skilled people in the cyber security field, now and in the future and we're particularly keen to encourage more young people and women into the profession. It's vital that we have the people and the skills to ensure the UK remains at the forefront of the information revolution."

Tim Hamer, the director of knowledge at the UK's Institution of Engineering and Technology, which is supporting MOOC, said: "With increasing threats emerging daily, online courses such as this have a vital role to play in raising awareness of the need to improve our cyber security. The course will also help to fill the shortage of skilled cyber security professionals that the UK needs."

The UK's National Computer Emergency Response Team (CERT-UK), which began operations on 31 March 2014, has said weak passwords and unpatched software is enabling hackers to use organisations' own servers as the hosts of cyber attacks (20-page / 1.26 MB PDF).

CERT-UK, which helps operators of critical national infrastructure (CNI) handle cyber threats, said that most of the incidents (51%) reported to it between the beginning of April and end of June came from organisations that do not operate CNI. It said it "processes over 250,000 reports of 'abuse' every day".

In a speech earlier this year, a senior UK government minister revealed details of a cyber attack by "a state-sponsored hostile group" that infiltrated UK government systems.

Officials worry about 'cyber Fort Hood'

By Joseph Marks

Source: http://www.politico.com/story/2014/09/it-cybersecurity-threat-110753.html

The most dangerous cybersecurity threat facing U.S. military and intelligence agencies might not be another Edward Snowden aiming to steal secrets, **but rather a rogue IT administrator bent on destruction of critical infrastructure,** a senior Intelligence official told POLITICO.

The official, who requested anonymity, described such an attack as a potential "Fort Hood in cyberspace," recalling the 2009 shooting rampage by Islamic extremist Maj. Nidal Hassan at the Texas Army base. Given the right access and skills, a federal IT administrator or other computer worker who had turned against America would be able to shut down government computers, disable military navigation systems, or even destroy critical infrastructure like power plants or oil refineries causing extensive loss of life.

"The one thing I'd say is becoming increasingly a concern for me is the possibility of the insider threat: Someone who is ideologically motivated and, depending on the ideology that's driving them, you might call them a self-radicalized insider," the official said in a recent interview.

"We're becoming increasingly dependent on IT," the official continued. "You've got [system administrators] everywhere. You've got empowered users who could do something catastrophic to their organization and depending on how and why they did it — and, of course, they're doing it for maximum effect and even maximum publicity — it's likely to be labeled cyber terrorism. But it's not coming from a discrete group that you can track and preempt."

Law enforcement and intelligence officials have long been concerned about so-called home-grown, or lone-wolf Islamic extremists, who become radicalized on the Internet and who — because they are not in contact with known foreign terrorists or recruiters — generally cannot be identified as a threat before they act. Carlos Bledsoe, a Muslim convert who shot and killed a U.S. soldier outside an Army recruiting office in Little Rock, Ark., in 2009 is an example often cited by counter-terror analysts, though officials say the U.S. could face a similar threat from self-radicalized adherents to domestic militias or hate groups.

Private sector insider threat watchers echoed the intelligence official's concerns but noted that the universe of people who could launch an insider cyberattack is much smaller than those that could launch a conventional insider attack, such as the Fort Hood or Little Rock shootings.

While thousands of people may work in a computer system every day, there are only a handful of system administrators and other highly skilled computer technicians who have both the access and technical knowhow to cause major damage.

"For a user to do something spectacular to a computer requires computing skills," said Martin Libicki, a senior management scientist at the Rand Corporation, who focuses on cybersecurity. "Any fool can grab an AK-47, but not any fool can hack a computer with any degree of effectiveness."

Nonetheless, intelligence officials are concerned, in part because digital monitoring systems designed to spot the next Snowden are ill-equipped to uncover this different, arguably more dangerous form of insider threat, the official said.

The latest employee and contractor monitoring systems in the defense and intelligence worlds are divided into two categories known as "continuous monitoring" and "continuous evaluation."

Continuous monitoring, which is already operational in a large number of classified computer systems, audits what employees are doing on the network and watches for anomalous behavior. The system might alert, for example, if a China analyst is accessing Intelligence documents focused on Iran or if someone on the day shift is accessing documents at night.

Continuous evaluation, which will only cover about 5 percent of cleared intelligence personnel by the end of 2016, is designed as a supplement to employee re-clearance investigations that take place every five or 10 years. Continuous evaluation systems scan government and public documents looking for arrests, bankruptcies, divorces or other indicators of personal or financial distress.

The idea is the program will alert agencies when an employee is hiding things he or she should be disclosing to superiors, acting strangely or suffering from excessive stress. Intelligence officials have assured members of Congress the systems are only meant to alert agencies when an employee should be investigated further — they're not designed to act as judge and jury on their own.

The problem is that a "self-radicalized insider" who's become an adherent to a jihadi terrorist ideology may leave no digital trail for those systems to pick up. If they do leave signs, they would likely be postings to online chat rooms or visits to extremist Web sites on a personal computer. Those aren't accessible by either monitoring system — and it would cause an uproar from privacy advocates if they were.

"Unless you buy into the idea that you're going to have the government monitoring everybody's social media interactions, if you have someone who self radicalizes they're otherwise still not manifesting [danger] signs," the official said.

The best way to protect against a cyber insider threat, the official said, is to design computer systems so that a single user couldn't wreak too much havoc, for instance, **by requiring two-person approval for some major actions.**

"You've got to rely on the resilience of your cybersecurity enterprise to stop one person from being in a position of

causing that much harm," the official said.
Part of that resiliency involves spotting a cyber-insider threat before damage can be done. For example, continuous monitoring systems could spot anomalies as the insider investigates which systems might be vulnerable, makes a dry run of the attack or walks to the brink but steps back.
"Generally, this isn't something where there's an automatic trigger and someone goes from zero to 100," said Mark Fallon, director of the Law enforcement consultancy ClubFed and a former deputy assistant director and special agent in the Naval Criminal Investigative Service. "Generally, you'll see an advance, some type of probing behaviors, some type of limit testing. There's always some type of surveillance or casing before an attack."
Just as likely, Fallon said, someone who's adopted an extremist philosophy will exhibit behavior changes that might be noticed and reported by coworkers — especially if the coworkers have been trained to be observant for insider threats.
When that happens, Fallon said, there's a chance to pull the insider back from the brink, limit his responsibilities or put him on leave.
"Experience tells me that if you've got a detection system, whether it's through automated means or better awareness of behaviors that indicate someone might be on the path to more extreme types of actions," he said, "at some point you need to introduce trained personnel to talk to that individual about it, to interdict or dissuade that person."
Even a combination of training, awareness and monitoring, however, will not be capable of tracking every cyber insider threat, he said.
"There's no failsafe system," Fallon said. "To me, the key is identifying the signs early so it doesn't get to be an active shooter scenario."

***Joseph Marks** covers cybersecurity for POLITICO Pro. He previously covered government technology issues for Nextgov, part of Atlantic Media, and covered local and state politics and higher education for the Grand Forks (N.D.) Herald and the Albert Lea (Minn.) Tribune. He interned for Congressional Quarterly's Homeland Security section and The Associated Press's Jerusalem Bureau. He holds a bachelor's degree in English from the University of Wisconsin in Madison and a master's degree in international affairs from Georgetown University.*

EDITOR'S COMMENT: Well said but in the case of Fort Hood, TX ALL the signs and symptoms were there infront of their eyes and nobody bother or take care of them. Perhaps because Dr Nidal was an Army physician and they did not want to play doctors themselves!

New approach to computer security: Wrist-bracelet

Source: http://www.homelandsecuritynewswire.com/dr20140923-new-approach-to-computer-security-wristbracelet

Bracelet replaces PINs, passwords, and logouts // Source: xinhuanet.com

In a big step for securing critical information systems, such as medical records in clinical settings, Dartmouth College researchers have created a new approach to computer security that authenticates users continuously while they are using a terminal and automatically logs them out when they leave or when someone else steps in to use their terminal.
Dartmouth's Trustworthy Health and Wellness (THaW) researchers recently presented their findings at the IEEE Symposium on Security & Privacy.
Common authentication methods based on passwords, tokens, or fingerprints perform one-time authentication and rely on users to log out from the computer terminal when they leave. Users, however, often do not log out, which is a security risk. The most common solution,

inactivity timeouts, inevitably fail security (too long a timeout) or usability (too short a timeout) goals.

One solution is to authenticate users continuously while they are using the terminal and automatically log them out when they leave. Several solutions are based on user proximity, but these are insufficient: they confirm whether the user is nearby but not whether the user is actually using the terminal. Other proposed solutions based on behavioral biometrics (for example, keystroke dynamics) may not be reliable, as a recent study suggests.

A Dartmouth College release reports that to address this problem, Shrirang Mare, a Dartmouth computer science Ph.D. student, developed an approach called **Zero-Effort Bilateral Recurring Authentication, or ZEBRA**. In ZEBRA, a user wears a bracelet with a built-in accelerometer, gyroscope, and radio on his or her dominant wrist; such bracelets are commonly sold as fitness devices. When the user interacts with a computer terminal, the bracelet records the wrist movement, processes it and sends it to the terminal. The terminal compares the wrist movement with the inputs it receives from the user via keyboard and mouse and confirms the continued presence of the user only if they correlate. Because the bracelet is on the same hand that provides inputs to the terminal, the accelerometer and gyroscope data and input events received by the terminal should correlate because their source is the same – the user's hand movement.

In experiments, ZEBRA performed continuous authentication with **85 percent accuracy** in verifying the correct user and identified all adversaries within eleven seconds. For a different threshold that trades security for usability, **ZEBRA correctly verified 90 percent of users and identified all adversaries within fifty seconds.** Thus, ZEBRA can recognize (in under a minute) when an unauthorized person steps in to use the terminal if the original user has stepped away from the terminal. This kind of quick reaction can prevent mistakes — such as clinical staff accidentally entering information into the wrong patient's medical record — or inappropriate behavior, such as a bystander examining personal medical information or financial data by taking advantage of a computer left open by an authorized user.

"In this work, we focused on the deauthentication problem for desktop computers because we were motivated by associated problems faced by healthcare professionals in hospitals," says the study's senior author Professor David Kotz. "It would be natural to extend ZEBRA to mobile devices, such as smartphones or tablet computers, and we believe this is possible despite some different challenges."

In principle, ZEBRA could also be extended to other devices such as TV remotes, game controllers or **medical devices** – any device where the user provides frequent inputs with his or her hand. For these devices, however, the application may be more for improving usability than security. For example, if the TV remote could identify who is holding it, it could provide personalized functionality, which could lead to a better user experience. Identifying who is using a particular medical device or sensor could help provide a secure user-attestation that is useful for healthcare professionals.

The Impact of the 22nd February 2011 Earthquake on Christchurch Hospital

Source:http://ir.canterbury.ac.nz/bitstream/10092/7284/1/12641198_McIntosh%20et%20al.%202012%20NZSEE%20-paper%20124-FINAL%20%281%29.pdf

The Impact of the 22nd February 2011 Earthquake on Christchurch Hospital

J.K. McIntosh[1], C. Jacques[2], J. Mitrani-Reiser[2], T.D. Kirsch[2], S. Giovinazzi[1], and T.M. Wilson[1]

[1]*University Of Canterbury, Christchurch, New Zealand.*

[2]*Johns Hopkins University, Baltimore, United States of America.*

2012 NZSEE Conference

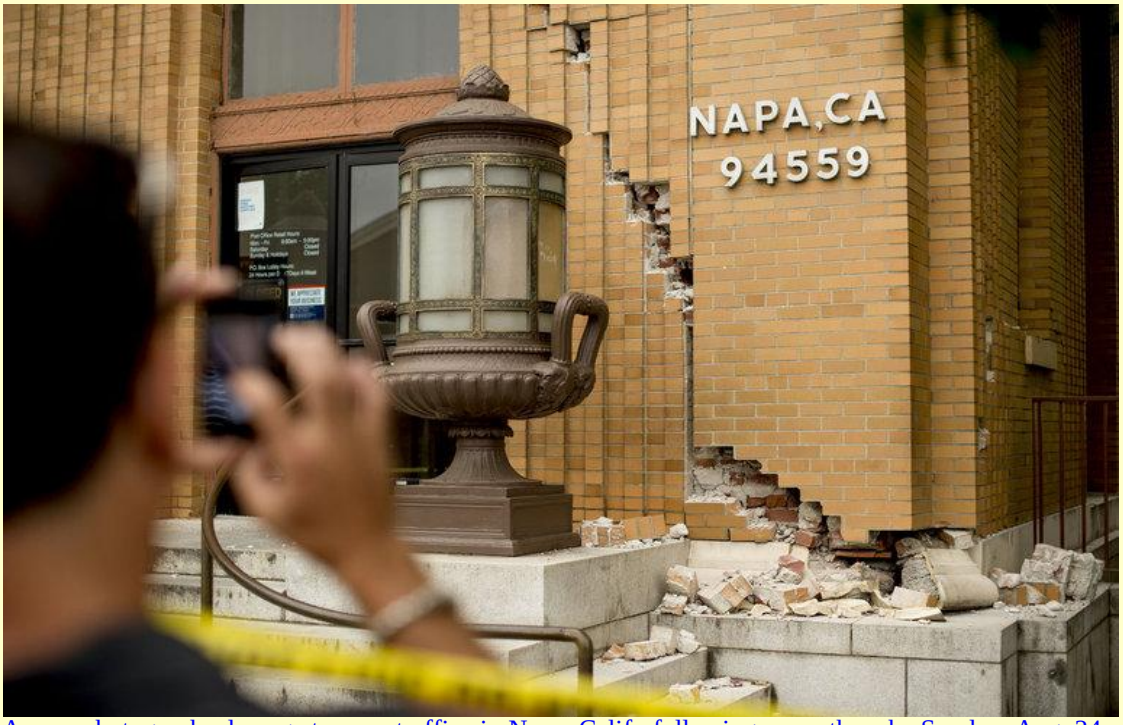
ABSTRACT

The 22nd February 2011, M_w 6.3 Christchurch earthquake in New Zealand caused major damage to critical infrastructure, including the healthcare system. The Natural Hazard Platform of NZ funded a short-term project called "Hospital Functions and Services" to support the Canterbury District Health Board's (CDHB) efforts in capturing standardized data that describe the effects of the earthquake on the Canterbury region's main hospital system. The project utilised a survey tool originally developed by researchers at Johns Hopkins University (JHU) to assess the loss of function of hospitals in the Maule and Bío-Bío regions following the 27th February 2010, M_w 8.8 Maule earthquake in Chile. This paper describes the application of the JHU tool for surveying the impact of Christchurch earthquake on the CDHB Hospital System, including the system's residual capacity to deliver emergency response and health care. A short summary of the impact of the Christchurch earthquake on other CDHB public and private hospitals is also provided. This study demonstrates that, as was observed in other earthquakes around the world, the effects of damage to non-structural building components, equipment, utility lifelines, and transportation were far more disruptive than the minor structural damage observed in buildings (FEMA 2007). Earthquake related complications with re-supply and other organizational aspects also impacted the emergency response and the healthcare facilities' residual capacity to deliver services in the short and long terms.

Napa Earthquake Highlights California's Need for an Early Warning System

By Colin Wood

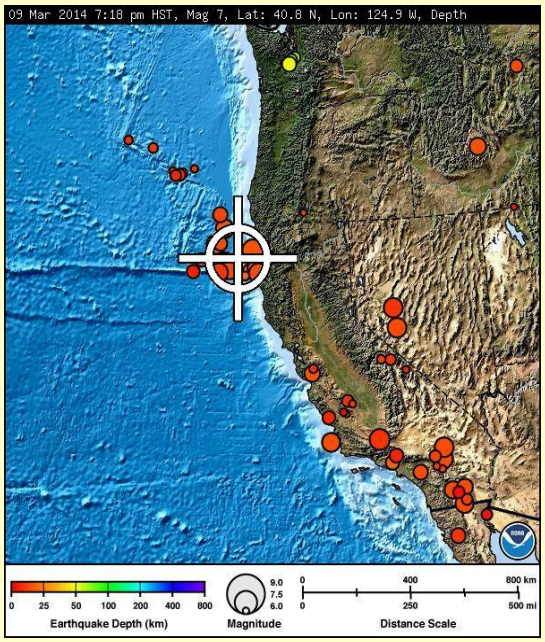
Source: http://www.emergencymgmt.com/disaster/Earthquake-Highlights-Californias-Need-Early-Warning-System.html



A man photographs damage to a post office in Napa, Calif., following an earthquake Sunday, Aug. 24, 2014. *AP/Noah Berger*

Just after 3 a.m. on Aug. 24, thousands of sleeping Californians wearing their Jawbone fitness monitors suddenly woke up.

That morning, a magnitude 6.0 earthquake hit Napa Valley, causing electric and gas outages, damaging buildings, injuring more than 200 people, and leading Gov. Jerry Brown to declare a state of emergency. For researchers at UC Berkeley, however, the quake wasn't a complete surprise -- they detected the event 10 seconds before it happened through ShakeAlert, an early detection and warning system that's giving officials a preview of capabilities that might someday be available to emergency services throughout the state, should adequate funding be located.



Early Earthquake Warning

Last fall, Brown signed a bill ordering the system's creation so that officials would have a chance to notify the public and shut down critical infrastructure prior to the earthquake's arrival. Though the bill received unanimous bipartisan support, the project has struggled to find funding, so far receiving about $10 million of the $83 million needed to finance the project for five years. But the earthquake in Napa could prove to be the relatively gentle

warning that California needs to get the project funded.

Because ShakeAlert isn't yet tied to a public notification system, the advance notice was of no practical value in this particular earthquake, but those 10 seconds represent how California could become safer when the next big earthquake hits, said Douglas Given, national earthquake early warning coordinator with the U.S. Geological Survey (USGS).

"It performed as expected, but not as well as it could have [if] we had better instrumentation in the area," Given said, adding that California still relies on an old network of sensors that need replacing and augmentation -- and to do those upgrades, its program needs funding.

"What we've seen in other countries that have early warning systems is that they built them after large killer earthquakes," Given said. "In Mexico, after the 1985 earthquake killed 10,000, and in Japan after the 1995 earthquake killed 6,400 people. In China, they're now seriously building systems based on when the China earthquake killed over 80,000 people, so it's our hope that we can build our system here before, and not after, the big killer earthquake."

And even just a few seconds' notice is enough time to make a big difference, Given said, and 10 seconds is enough to take a number of important actions. "The most obvious for the public is to drop, cover and hold on, which only takes two or three seconds to do," he said. "If you're in surgery, it wouldn't take very long to secure the patient and maybe stop whatever you're doing, turn off a machine, or stop an elevator. Every small earthquake like this that brings earthquakes to mind and gets people remembering the hazard that we have here makes it more likely we'll get the support we need to complete the system."

State Sen. Alex Padilla, who introduced the earthquake early warning legislation, said everyone saw the value of an early warning system when it was proposed.

"What I'm hoping is yesterday's event reminds us of the urgency with which we need the system deployed, sooner rather than later," Padilla said, adding that while he recognizes people were hurt during this earthquake, it could have been much worse. "I shudder to think what the consequences would have been if the earthquake was at 3 o'clock in the afternoon on a Wednesday as opposed to 3 o'clock in the morning on a Sunday, and if the epicenter was in San Francisco versus Napa. Fortunately it was a minor impact for an earthquake of this magnitude, but we know the next big one, whether it's in San Francisco or Los Angeles or anywhere else, it's only a matter of time."

Gas Leak Detection

The earthquake disrupted electricity service to 70,000 Pacific Gas and Electric (PG&E) customers in Napa and Sonoma counties, but the utility restored power to almost everyone the same day. PG&E also received hundreds of calls reporting the smell of natural gas, but reported that there was no major damage to its natural gas transmission and distribution lines -- and only 20

customers had lost gas service. Identifying leaks is made much easier today by leak detectors introduced in 2012 that are 1,000 times more sensitive than traditional detectors.
PG&E spokesperson Donald Cutler said that since rolling out the program, the sensors have been useful in detecting leaks quickly and more efficiently. In one field test, a large crew equipped with the new sensors was able to check 35,000 locations in 17 days and fix more than 2,200 leaks, a project that would have taken four months using traditional technologies and methods, according to PG&E.
And the Napa earthquake gave PG&E an opportunity to test the technology in an emergency setting. "It's definitely been helpful," Cutler said. "It's more sensitive and works well. Everything that keeps our customers and communities safe is always something that's useful to us."
An early detection system would do little to protect gas and power infrastructure, but could give people a chance to get to a safer location or brace themselves. In April, Mexican agencies and citizens were notified of an impending 7.2 earthquake via the Seismic Alert System of Mexico (SASMEX), giving some cities as much as 74 seconds advance notice.

***Colin Wood** has been writing for* Government Technology *and* Emergency Management *since 2010.*

Flying cameras following earthquake

Source: http://i-hls.com/2014/08/flying-cameras-following-earthquake/

Flying cameras help teams assess damage, search for survivors and clear roads following earthquake in Ludian, Yunnan, China. Disaster response team incorporates aerial technology into their relief efforts for the first time.
Relief workers are using aerial imaging to address two of the greatest challenges in the Ludian earthquake zone – identifying areas amidst the rubble areas to focus the search for survivors, and clearing roads for supplies to get to the disaster area, according to sUAS News.
Following the magnitude-6.5 earthquake in Ludian on August 3, 2014 which caused more than 600 deaths and forced 200,000 individuals to relocate, the China Association for Disaster & Emergency Rescue Medicine (CADERM) has incorporated small unmanned aerial systems (sUAS) into their relief work for the first time.

The team is using the **UAV DJI S900** (top) and DJI Phantom 2 Vision+ (bottom) flying platforms to provide workers with an overhead view, assisting post-disaster assessment and enabling them to focus their work in the most efficient way.

Aerial images captured by the team were used by workers in the epicenter area of Longtoushan, where most of the traditional buildings in the area collapsed. The dense rubble and vegetation have made ground surveying extremely difficult, so using aerial images has helped identify where relief teams can focus on searching for survivors.

Aerial view of the disaster area

The team has also used aerial images to assist rescuers to clear a road from Guangming Village to Tiansheng Bridge by identifying the easiest points of clearance – a crucial need for relief efforts in disaster zones.

FINDER Senses Heartbeats Amid Rubble

By Colin Wood

Source: http://www.emergencymgmt.com/disaster/FINDER-Senses-Heartbeats-Rubble.html

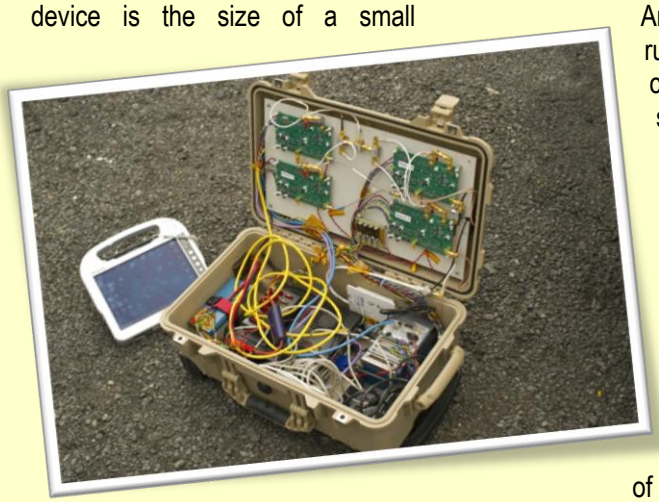
In the next large-scale disaster, a new people-finding device could save lives.

Disasters like the 2010 Haiti earthquake demonstrated a need for technology that would allow first responders to quickly answer a simple question when faced with hundreds of collapsed structures: Are there people in that rubble? *Flickr/U.S. Army Corps of Engineers*

Now under development by NASA's Jet Propulsion Laboratory (JPL) in Pasadena, Calif., the **Finding Individuals for Disaster and Emergency Response (FINDER) device** is ready for commercial deployment, said JPL Engineer Jim Lux. Research began following instruction from the U.S. Department of Homeland Security's Science and Technology Directorate in April 2012. Disasters like Hurricane Sandy

and the 2010 Haiti earthquake demonstrated a need for technology that would allow first responders to quickly answer a simple question when faced with hundreds of collapsed

structures: Are there people in that rubble?
FINDER can detect a human heartbeat buried beneath 30 feet of debris, or behind 20 feet of solid concrete and from distances of up to 100 feet in open space. The latest prototype of the device is the size of a small



suitcase and can fit into an overhead bin on a commercial airplane. Turning FINDER on and pointing it at a pile of rubble will tell workers within 30 seconds whether there's a person inside who needs saving or if the rescuers can move on.
FINDER detects humans by honing in on the one sound that can prove they're still alive.

"What we're looking for is the little tiny motions of your body when your heart beats — maybe 1/20th of an inch. Heartbeats are sort of unique," Lux said. "They happen about once a second. Things that are moving at a different rate we ignore. And that's how we ignore cats and dogs and rats is their heart rates tend to be a lot higher, and we don't detect cows because their heart rates are lower."
And ambient sounds, like flying birds or leaves rustling in the wind, typically are not consistent like a heartbeat, while mechanical sounds — that occur about once per second — can easily be filtered out because their timing is too consistent to be mistaken for a heartbeat, Lux said.
FINDER hasn't saved any lives yet, he added, because there haven't been any large-scale disasters for a while, but some licensees are going to begin manufacturing the devices soon so a product may be ready when the next disaster hits. Lux estimated a price point of about $10,000 per unit.
In September 2013, researchers began testing FINDER around the country by putting it in the hands of first responders, who helped guide user interface design, including putting a light on the outside that would allow workers to find it in the dark and integrating the data with a larger

operating picture, Lux said. As emergency responders begin using devices like tablets and embrace sensor technology, integrating all that data into one central location one would be immensely useful, Lux said, and he and his team are now looking at developing along those lines.

Their research will also continue to adapt the device to the needs of smaller, more common operations, like searching for missing children, searching from a moving platform, or searching in an area where people are walking around on the other side of the debris. Researchers are now updating the device to include an option to limit the range of the device to detect, for example, heartbeats that are farther than 10 feet away, but closer than 50 feet. Such adjustments will make FINDER more useful outside of large-scale disasters, Lux said, adding that FINDER could also be used to detect people inside burning buildings or trapped in storm shelters beneath rubble.

"The commander on the scene has to make that decision about, 'Do I send someone in, risking their life for somebody who may not be there?'" he said. "FINDER could potentially help with that problem, and that's something that does happen more often and could be more useful."

***Colin Wood** has been writing for* Government Technology *and* Emergency Management *since 2010.*

Smartphones can save life in health emergencies

Source: http://www.homelandsecuritynewswire.com/dr20140828-smartphones-can-save-life-in-health-emergencies

More Americans adopt smartphones for communicating, managing calendars, and storing contacts, but these all-in-one devices could also be used to save lives in health emergencies. Companies are developing apps that allow users to store health data which can then be accessed by emergency services personnel or physicians. "No one is immune to having an emergency," said Dr. Bettina Experton, president and CEO of Humetrix, which late in 2013 launched the **ICEBlueButton app.** "Kids playing sports or away from home at camp can have an accident and emergency personnel need to know if they have any medical conditions or life-threatening allergies."

Government Technology reports that the app was on display at the White House's Innovation for Disaster Response and Recovery

Demo Day on 29 July. The event brought together innovators in the disaster response community to showcase tools that may help save lives in large-scale emergencies.

The $2.99 per month or $19.99 per year app allows users to create an In Case of Emergency (ICE) record for themselves and family members. A QR code for each record can be saved onto the smartphone's lock screen, or printed on a sticker that can be placed on a car seat or a child's bicycle helmet. Upon arriving on the scene of an emergency, EMS personnel can use any QR scanner to scan the code and access the records created with the app. The app also offers an Auto-Alert feature that automatically sends an email to the designated emergency contact should the QR code be scanned by EMS or medical personnel responding to an emergency.

"We already have emergency medical professionals in the field advising people to download our app," Experton said. Cathy Chidester, director of the Los Angeles County Emergency Medical Services Agency, recommends apps such as ICEBlueButton to residents of Los Angeles County. She told the *Los Angeles Times*, "I would like to see people have their basic information available for the paramedics," she said. "That would go a long way toward helping them save lives."

Experton acknowledges that more emergency personnel would need to be aware of the app for it to become widely effective. She also noted that there is minimal training needed for medical personnel if they have a QR scanner. "Checking for a smartphone has really become part of the routine for the public health professional," she said. "Years ago they would look for a wallet for ID when responding to an emergency. Now they know to look for a smartphone."

In April, ICEBlueButton was awarded the Parent Tested Parent Approved (PTPA) Winner's Seal of Approval from PTPA Media, a volunteer parent testing community. Experton hopes the app will be recommended by disaster preparedness agencies such as the Federal Emergency Management Agency and the Centers for Disease Control and Prevention.

▶ **More about this application at:** http://www.icebluebutton.com/

New York City Tracks Firefighters to Scene with NRL Radio Tags, Automated Display

Source: http://www.nrl.navy.mil/media/news-releases/2014/new-york-city-tracks-firefighters-to-scene-with-nrl-radio-tags-automated-display#sthash.osLeHctk.dpuf

On 15 of its vehicles, Fire Department New York (FDNY) now can automatically see which firefighters are nearby from the onboard computer, and relay that information to the city's Operations Center. The system was invented by David DeRieux of the U.S. Naval Research Laboratory (NRL) Space Systems, along with Michael Manning of Manning RF, and in close partnership with FDNY.

Since the 9/11 terrorist attacks, New York City has been pursuing ways to better coordinate the 14,000 firefighters and emergency response it employs. (Prior to 9/11, the

FDNY used a paper/carbon-copy ride list—Battalion Form 4 (BF4)—to account for who's present.)
NRL's system is based on an active radio frequency identifier (RFID) tag carried by each firefighter, similar to E-ZPass or how retail tracks inventory. "It's in a little sealed plastic—it looks like a little key fob, actually," says George Arthur, an NRL engineer who contributed to the project. "They're positioned over the left breast, inside the bunker coat in a little Kevlar pocket that's sewn in there. And it just sends out a little ping every five seconds: here I am, here I am, here I am."
Fire Department New York uses a U.S. Naval Research Laboratory (NRL) system to automatically track firefighters. "That's the intention with this device, to make sure everyone's accounted for," says David DeRieux, one of the inventors.


Left: NRL worked with firefighters to determine where to add the RFID pocket. Right: The truck's onboard computer displays a table of who, based on their unique RFID tags, is nearby. *(Photo: U.S. Naval Research Laboratory)*

A radio receiver on the vehicle picks up the pings and builds a table of identifiers. "It just listens and says, 'Okay, 1234, that's Jessica Smith,' so we know Jessica Smith is nearby," says DeRieux. "Periodically, a program that's running on their MDT [mobile data terminal], their onboard computer, quizzes this reader and says, 'Let me have everything.'"
The table of every firefighter on or near the vehicle is displayed on the MDT screen. "As soon as [the driver] turns the ignition on," says DeRieux, "this thing comes up. When they get on the scene, everyone takes off, they all disappear. Then eventually they come back for a roll call situation, and the captain can tell instantly everyone is within so many feet of the truck."
The MDT also sends this accounting to the FDNY Operations Center in Brooklyn, using a commercial modem. "They actually have a massive display, twice the size of my wall," says DeRieux, "and on there this data gets projected. So they know what truck just showed up on scene, who was on the truck." To coordinate personnel during a city-wide disaster, this real-time information would be unimaginably valuable. "During 9/11 there were thousands of firefighters, it was a big problem," says DeRieux.
The data is also archived. "If there were a HAZMAT release," says Arthur, "they could go back and immediately see the firefighters that were on duty."
On April 23rd, the Federal Laboratory Consortium awarded NRL for Excellence in Technology Transfer. "Technology transfer is very important," says Arthur. "Doing things here [at NRL] that are beneficial, not just to the warfighter, but also to the average citizen."

Firefighters gave feedback to NRL throughout development

NRL worked closely with FDNY throughout the years of development. "They gave us very good feedback," says Arthur. "They'd say, 'That's kind of what I want, but can you do this

and can you change that?' They pretty much knew what they wanted and that was just all the difference in the world."

They also had the opportunity to spend time in New York getting to know the firefighters and their needs, and see them in action. "They're an impressive bunch to talk to, very big-hearted," says Arthur. "There's one guy, Chief [of Logistics Ronald] Spadafora, who's got this thick Brooklyn accent, rides a Harley to work. Well he's got two Masters degrees, he flies all over the world [giving] lectures on fire science. He's written a couple books."

The relationship started with a fortuitous meeting in 2002. "I recognized the guy next to me," says DeRieux. "Turns out, his name was [Battalion Chief] Joe Pfiefer." Pfiefer was the first chief to take command on 9/11. "[Pfiefer] brings me into his office and he says, 'We've got a problem. We need a way to keep track of our firefighters. Worse yet, some firefighters, who become dazed and confused during an operation, may not make it out of the building, or they end up in the wrong area for roll call.'"

NRL's system was needed so the other truck would be able to automatically relay through the Operations Center, "He's over at Engine number whatever so he's all right," says DeRieux. "That's the intention with this device, to make sure everyone's accounted for."

Working with FDNY led to an unexpected spin-off: the city liked the program's interface so much, they asked NRL to make a similar drag-and-drop program they could use to schedule personnel assignments. Says Arthur, "Now EBF4 is the standard scheduling tool New York City uses for their firefighters. NRL wrote it."

NRL got "easy to use, reliable, and cheap" hardware from industry

One of FDNY's primary requirements, says Arthur, was, "It has to be easy to use, reliable, and cheap."

So DeRieux turned to Michael Manning, who had a private company already working on RFID, to provide the hardware for NRL's program. Says Arthur, "All the hardware came off the shelf; the secret sauce is the software. Anybody can go out and buy the RFID components, but if they don't have our program it's just a bunch of dumb computer parts."

Using all off-the-shelf hardware kept costs low. "The readers cost around $1,100 a piece in the quantities we buy them, that might come down a bit," says Arthur. "The tags cost about $20 a piece."

The tags are active RFID; so, unlike passive RFID, the batteries will run out in three to four years, depending on how often they're programmed to transmit. But active gives greater range and the ability to transmit more data. Says Arthur, "If you used the same amount of equipment, you could conceivably load it with the oxygen the guy had left, the temperature in the area."

Is the future to track personnel moving inside a building?

"We have given them the piece that lets them track from the vehicle to the fireground or the event," says Arthur. "If we could drop in a complementary piece, where we could track firefighters while they're in the building, that would save so many lives."

"Indoor tracking," says DeRieux, "it's a very tough nut to crack."

NRL's system is simply, "I detect a signal or I don't"—but an indoor system would need to pin a precise point in three-dimensional space. "I've always said down to six inches," says Arthur, "because that's the approximate width of a wall. You don't want to track a firefighter only to find yourself on the wrong side of a wall."

The tracking systems Arthur's reviewed start at a known, fixed point, then uses sensors to estimate where you've gone. "Gyroscopes know which direction you're moving and there are movement sensors that estimate how fast you're moving. An altimeter tells whether you've gone up or down in the building." He adds, "But the problem is chaos." Say the system is accurate plus or minus an inch on each step. The firefighter's first step from the known point is accurate within an inch; but the second step is plus or minus an inch based on a guess that was also plus or minus an inch. "And the longer you're out walking around," says Arthur, "the more those inaccuracies compound."

Additionally, the firefighters may be behind metal walls, they may be 100 floors up from a data receiver, and an altimeter may not give reliable data "because in a building that's on fire you're going to have all kinds of changes in air pressure."

A separate avenue of research, particularly if NRL were to put a new system in another city or perhaps aboard a naval ship to track fire control teams, would focus on improving

the hardware. "We started implementing this system in 2007," says Arthur, "and everything's come a long ways since then." Today, there are passive RFID tags that, unlike FDNY's system, can last indefinitely. They're also ruggedized and wouldn't have to be removed before laundering.
Be it for U.S. Marines or firefighters, for talking to spacecraft or talking to Brooklyn, NRL is a place where engineers solve problems. Says Arthur, "I'm kind of a nuts and bolts guy. I'm an engineer who can change a tire. I like to fix things, take things apart."

The State of New York launches disaster preparedness initiatives

Source: http://www.homelandsecuritynewswire.com/dr20140916-the-state-of-new-york-launches-disaster-preparedness-initiatives

The state of New York is implementing a proactive strategy to deal with the threat of terrorism and natural disasters like Superstorm Sandy. Governor Andrew Cuomo is leading several initiatives that grant local municipalities state support for emergency preparedness projects. The state's Division of Homeland Security and Emergency Services (DHSES), led by commissioner Jerome Hauer, has expanded its regional footprint from five planning/response regions to ten, each led by a regional director, regional coordinator, and a lieutenant from the state police force. These representatives will work with members of other state agencies including the DHSES Office of Fire Prevention and Control to serve as the state's primary liaison with local emergency managers. With this structure, resources can be deployed quickly to help cities and counties during emergency situations.

New York Air National Guard members distribute disaster and emergency response starter kits and emergency information after a session of the state's Citizen Preparedness Corps Training Program on May 10. *(U.S. National Guard photo by Sgt. 1st Class Raymond Drumsta)*

New York has also developed a state-funded interoperable communications program to allow local and state public safety agencies and first responders to communicate during disasters. To date, $215 million has been awarded to all fifty-seven counties and New York City through thirteen regional partnerships. Counties must deploy proprietary communications technology to be eligible for state reimbursement for project expenses.

As part of its new preparedness plan, DHSES has improved its regional stockpile program which holds a variety of resources, including generators, large-scale pumps, cots, blankets, and water, along with specialty emergency items such as mass casualty equipment and other resources often needed during a disaster. *Emergency Management* reports that officials have developed a strategic fuel reserve and a program to issue backup generators to gas stations along evacuation routes.
New York State also offers an emergency management training program for elected officials so they are prepared to serve their communities during disasters.
The governor's office requires county chief executives and emergency managers to complete emergency training courses for

their counties to remain eligible for grants administered by DHSES. The State Preparedness Training Center (SPTC), housed in a former airport in Oriskany, New York with more than 700 acres, includes several courses to train emergency managers for all levels of disasters. **In 2013, more than 13,000 individuals were trained at the SPTC, including 4,500 teachers and school officials.** Officials plan to train at least 18,000 individuals this year in courses including active shooter events.

Often in large-scale emergencies, residents are asked to remain in safe zones until public safety officers arrive, but the state now wants the public to be readily available to respond to disasters, "as a member of (the) public will often be the first to the scene of an emergency." The newly launched Citizen Preparedness Corps will train residents to be ready for any type of disaster. Response kits that contain key items to assist in the aftermath of a disaster will be distributed to trainees. The training provided by the New York National Guard, and experts from DHSES aims to enroll 100,000 residents this year.

The state's proactive approach to emergency management is expected to adapt as new risks emerge**. "Mother Nature has become much more aggressive, so we too must adopt a similar posture to ensure we are ready to respond effectively when the next disaster strikes",** Hauer writes.

Sensors everywhere might mean privacy nowhere

Source: http://www.homelandsecuritynewswire.com/dr20140917-sensors-everywhere-might-mean-privacy-nowhere-expert

Just as we are coming to grips with having less privacy in our lives thanks to the Internet, a new use of the technology is poised to present new questions about security and privacy — and create a new threat to society.

Eugene Spafford, professor of computer science at Purdue University and executive director of the Center for Education and Research in Information Assurance and Security (CERIAS), says **the so-called "Internet of Things" will see small microprocessors and sensors placed seemingly everywhere, and these devices will collect much data about us — often without our knowledge.**

"Instead of a small number of scholars recording data, we will soon have millions and soon billions of tireless digital observers recording everything within reach, and storing it forever," Spafford says. "The benefit will be better decision making about many aspects of our lives, such as energy use, decisions about our health and financial decisions. The downside is that we give up a lot of our privacy, and, in fact, maybe all of it."

Ubiquitous Internet microprocessors will soon be in things we encounter every day. Spafford says examples are already appearing.

"We have the Nest thermostat, which does a better job of learning how we like to heat or cool our homes than previous thermostats, and we are beginning to see Internet-connected refrigerators, which can let us know when we need to buy groceries and pull together a shopping list for us," he says.

The problem is that consumers have little or no control about how the data collected will be used, or even knowledge about what data is being collected.

"We put ourselves in a position where we may be manipulated without our consent, and possibly without our knowledge, because connections may be drawn on this data that we don't understand or recognize even about ourselves," Spafford says. **"For example the company that makes the Nest thermostat was purchased by Google. Now Google will know when I'm home, can determine how many people are in the house, and that information will be provided to other companies and government agencies. Is that a trade I'm willing to make? To what extent can I control that?"**

A Purdue University release reports that Spafford will discuss security and privacy of "The Internet of Things" in a lecture titled "Faster Than Our Understanding" at a conference at Purdue called Dawn or Doom: The New Technology Explosion.

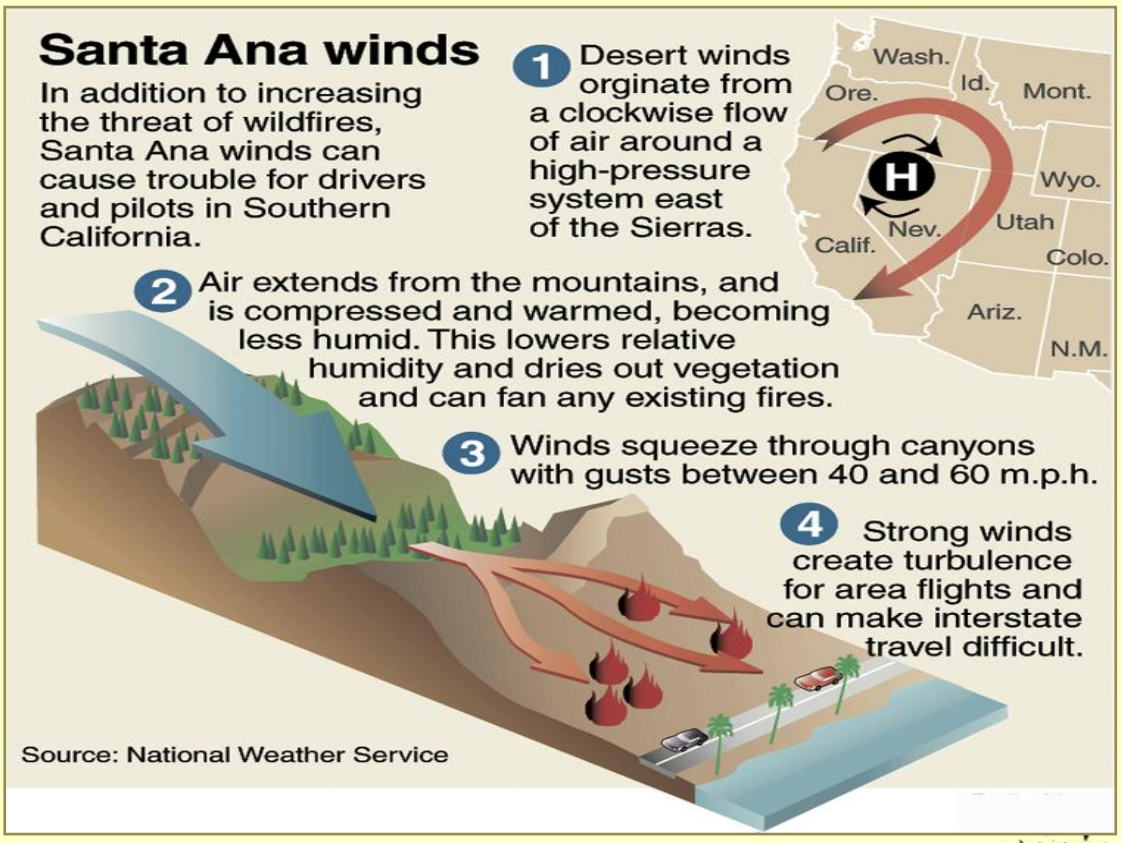
The Dawn or Doom conference is being held Thursday, 18

September, on the Purdue West Lafayette campus and is free and open to the public.
Spafford says what is needed is consumer information equivalent to the drug information that is packaged with each medication.
"We need a notice of the level of some of these observations, and which of these observations should we be allowed to opt out of. There needs to be greater transparency about what is done with the information that's collected, the accuracy of the data and where it's going," he says.
A second concern with the Internet of Everything is that we may have already crossed a threshold where a large event that would cripple these devices would mean that our current civilization would come to an immediate stop.
"Our telephones wouldn't work, hospitals would not be able to do medical tests, at the university we wouldn't be able to post grades," Spafford says.
An occurrence of a massive solar flare, like the 1859 Carrington Event, could disable all of these devices.
"If something like that were to happen, the Amish would become the only people without a major life upheaval," Spafford says.

A Santa Ana Wildfire Threat Index developed

Source: http://www.homelandsecuritynewswire.com/dr20140918-a-santa-ana-wildfire-threat-index-developed

UCLA atmospheric scientists were instrumental in the creation of the Santa Ana Wildfire Threat Index — a new tool to classify the fire threat potential of the powerful, hot, dry Santa Ana wind, which can turn a spark into an inferno. The index was introduced 17 September by the U.S. Forest Service, in collaboration with UCLA and San Diego Gas and Electric. The index includes four classification levels ranging from "marginal" to "extreme" that will be used to help fire agencies and other emergency responders, the media and the public determine the appropriate actions to take based on the likelihood of a catastrophic wildfire fueled by high winds.



A UCLA release reports that the UCLA research team was led by Robert Fovell, professor and chair of the department of atmospheric and oceanic sciences, and also comprised doctoral student Yang Cao and postdoctoral researcher Scott Capps. The three scientists performed high-resolution modeling for a large number of Santa Ana wind events, extending back decades.

"This effort has led to an enhanced understanding of the evolution of the Santa Ana winds, their potential for sparking and spreading fires, and their spatial and temporal variation," said Fovell, a faculty member in the UCLA College. "We not only have a new, deeper understanding of how the San Diego-area terrain influences weather, especially wind, which is crucial to SDG&E's operations, but we also have been able to make improvements in weather modeling that will benefit forecasters around the world."

The team undertook the difficult tasks of assessing "live fuel moisture" — essentially, the moisture content of chaparral —and ground cover conditions using meteorological data alone. Those data points are important components of the index.

"Given the current state of fuel conditions, we have the potential to see devastating fires this fall should significant Santa Ana winds occur," said Tom Rolinski, a Forest Service meteorologist. "This tool will directly benefit fire agencies by allowing us to better anticipate what kinds of resources may be needed, as well as where and when we could face the greatest challenges."

The threat index has four levels of increasingly severe fire potential:

- **Marginal: Upon ignition, fires may grow rapidly**
- **Moderate: Upon ignition, fires will grow rapidly and will be difficult to control**
- **High: Upon ignition, fires will grow very rapidly, will burn intensely and will be very difficult to control**
- **Extreme: Upon ignition, fires will have explosive growth, will burn very intensely and will be uncontrollable**

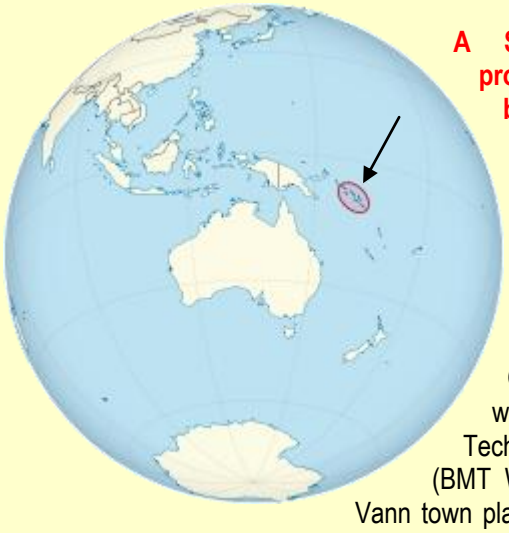
Each level includes recommended actions that escalate in accordance with the possible severity of the fire.

The Forest Service, a part of the U.S. Department of Agriculture, is the agency responsible for determining and issuing the alerts, which can be found on its Web site.

Tips for the public during fire season include closely monitoring fire conditions, registering phones to receive 911 warnings for the latest information about an emergency, making sure phones are charged, ensuring vehicles' gas tanks are full, and reviewing emergency evacuation plans at work and at home.

Rising sea levels force the Solomon Islands provincial capital to relocate

Source: http://www.homelandsecuritynewswire.com/dr20140825-rising-sea-levels-force-the-solomon-islands-provincial-capital-to-relocate



A Solomon Islands provincial capital will be relocated to the mainland due to coastal hazards and the risks of rising sea levels resulting from climate change.

The University of Queensland worked with British Maritime Technologies WBM (BMT WBM) and Buckley Vann town planners to develop a comprehensive climate change adaptation plan to move the town of Taro, with a population of 800, to the adjacent mainland.

UQ School of Civil Engineering's Professor Tom Baldock said the community of Taro was under significant risk from tsunamis and ocean storms.

"As the capital of the Choiseul Province, Taro is less than two meters above sea level, presenting a significant risk to the community, which will be compounded in the future with climate change and the resulting rise in sea levels," he said.

BMT WBM lead Project Manager Dr. Philip Haines said the plan, which was prepared on behalf of the Australian Government, marked the first time a Pacific Islands capital with all its services and facilities would be relocated due to coastal hazards and climate change.

"Relocation is the only option available that will keep the community safe and will allow for future growth and prosperity of the capital and the province," he said.

A UQ release reports that the relocation of the capital, including schools, hospitals, and businesses, will take many decades to complete, and the adaptation plan also aims to increase the community's resilience to coastal hazards, such as the preparation of a tsunami response plan.

A multi-disciplinary team of engineers, scientists, and town planners consulted extensively with the Choiseul Bay communities to develop a vision and future town layout that reflected the needs and values of the local Lauru people.

UQ's Dr. Simon Albert led the community

consultation and developed a management plan taking account of traditional practices and expertise.

Choiseul Province Premier Jackson Kiloe thanked the team for respecting tradition.

"The project followed the ways of our traditions — talking with people, listening to people, and reflecting the desires of the people," Kiloe said.

The project is now being hailed by the Solomon Islands National Government as a best-practice model for natural hazard resilience planning for other provinces across the Solomon Islands and more broadly across the Pacific region.

Climate change makes Europe hospitable to Dengue fever

Source: http://www.homelandsecuritynewswire.com/dr20140825-climate-change-makes-europe-hospitable-to-dengue-fever

Dengue fever could make headway in popular European holiday destinations if climate change continues on its predicted trajectory, according to University of East Anglia research published in *BMC Public Health*.

The study used current data from Mexico, where dengue fever is present, and information about EU countries to model the likelihood of the disease spreading in Europe. They found that coastal regions around the Mediterranean and Adriatic seas, the Po Valley, and North East Italy were most at risk.

Dengue fever is a tropical disease caused by a virus that is spread by mosquitoes, with symptoms including fever, headache, muscle and joint pain. **Each year, dengue infects fifty million people worldwide and causes approximately 12,000 deaths** — mostly in South-east Asia, and the Western Pacific.

A UEA release reports that because the mosquitoes that carry and transmit the virus thrive in warm and humid conditions, it is more commonly found in areas with these weather conditions. Dense populations and global travel are also associated with increasing the spread of the disease, which was observed in the last few decades.

Local cases such as those reported in France and Croatia in 2010 clearly show that dengue can be transmitted in Europe, in areas where the mosquito species that carries the virus has established.

For this study, the researchers wanted to estimate how likely the disease is to become established in Europe as its climate changes up to the end of the century.

The researchers analyzed data from Mexico on the occurrence of dengue fever and the effect of climate variables such as, temperature, humidity and rainfall, as well as socioeconomic factors that included population figures and GDP per capita. These data were then used to estimate dengue fever cases in the 27 EU member states over four time periods: baseline conditions (covering years 1961-90), short-term (2011-40), medium-term (2041-70), and long-term (2071-2100).

The results of the long-term projections found an increased risk of the disease when compared to baseline conditions. **The incidence rate is predicted to go from 2 per 100,000 inhabitants to 10 per 100,000 in some places.**

The areas anticipated to be at most risk were found to be along the Italian cost and Po Valley in Italy, the Spanish Mediterranean, and southern Spain in general.

Lead researcher Prof Paul Hunter, from UEA's Norwich Medical School, said: "Our study has shown that the risk of dengue fever is likely to increase in Europe under climate change, but that almost all of the excess risk will fall on the coastal areas of the Mediterranean and Adriatic seas and the North Eastern part of Italy, particularly the Po Valley."

The authors acknowledge that a limitation of their study is that it is based on clinical data from Mexico, which has much less summer-winter variation than Europe, thus affecting mosquitoes' survival and overwintering. They believe that future work can strengthen their model by modifying it to take into account the difference in seasonality between both areas and testing other climate change scenarios.

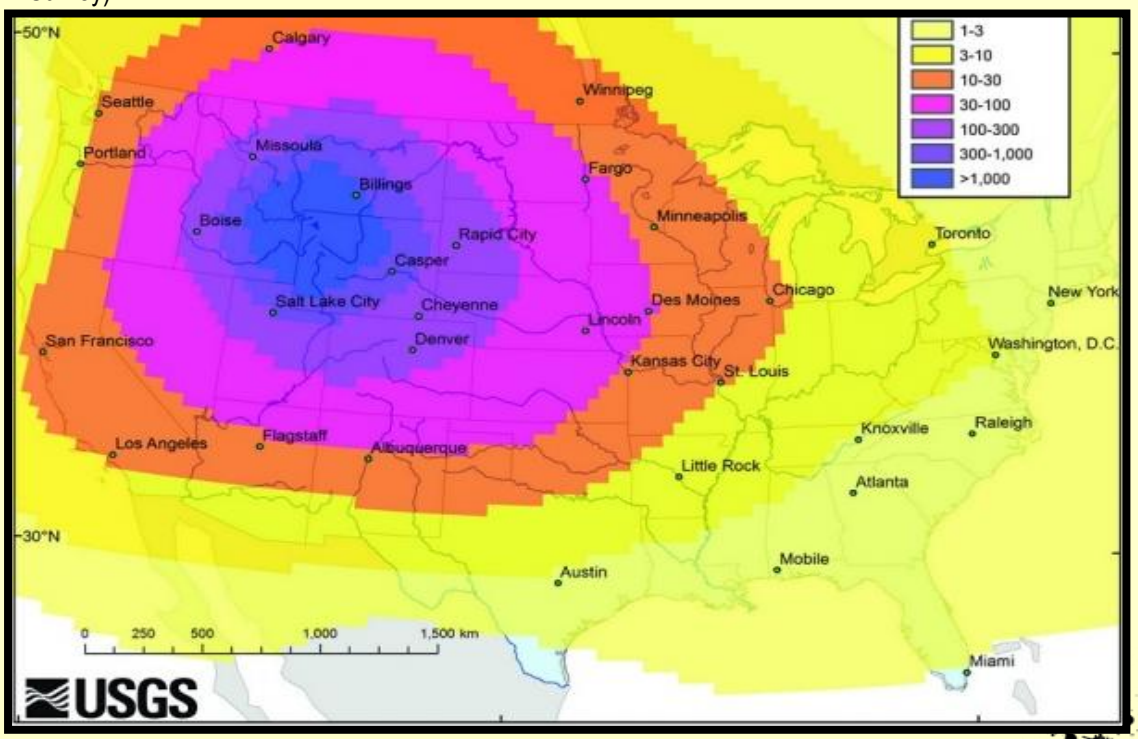
Prof Hunter said: "The exact incidence of dengue fever is dependent on several other factors, some of which we were unable to model at this stage. Nevertheless, public health agencies in high risk areas need to plan, implement and evaluate active reporting of mosquito populations and clinical surveillance by local doctors. Work should be carried out to improve awareness of the increased risk amongst health practitioners and the general public."

— Read more in Maha Bouzid etal., "Climate change and the emergence of vector-borne diseases in Europe: case study of dengue fever," *BMC Public Health* 14:781 (22 August 2014)

Yellowstone supervolcano eruption will be nightmarish but not catastrophic

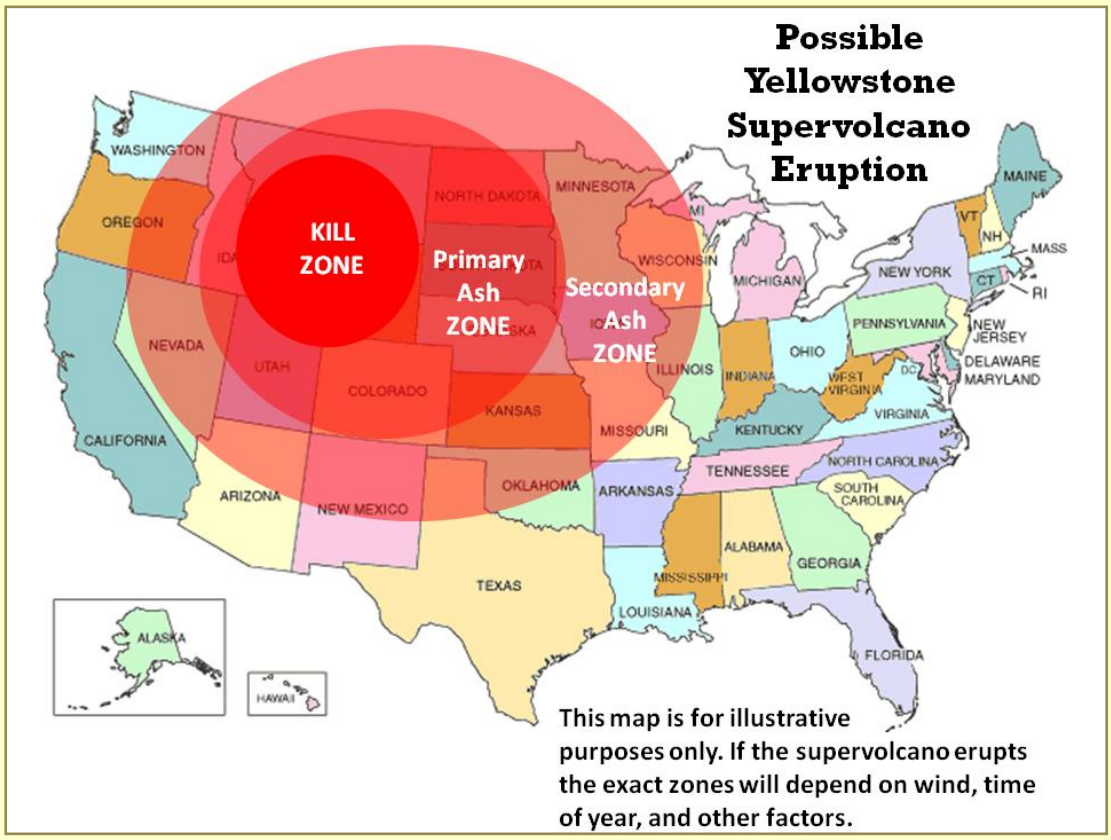
Source: http://www.techtimes.com/articles/14539/20140831/yellowstone-supervolcano-eruption-will-be-nightmarish-but-not-catastrophic-study.htm

August 31 – A Yellowstone eruption could blanket the whole of North America with ash and cause a winter during the summer months. It's unlikely to happen anytime soon, but a new computer model shows just how wide an area the eruption would impact. (Photo : Image courtesy of the US Geological Survey)



At least a meter of ash would blanket parts of the Rocky Mountain range and a few millimeters of the fallout would reach cities on both coasts of the U.S. if the Yellowstone supervolcano erupted, according to new computer simulation on the event, something that's unlikely to happen anytime soon.

There have been no supereruptions in recorded history that would size up with an explosion spewed by the Yellowstone supervolcano. Even eruptions by Chile's Quizapu volcano and the Valley of Ten Thousand Smokes in Alaska are magnitudes below a Yellowstone event, according to the simulation on a Yellowstone eruption and the model's accompanying study.



The Ash3D model simulated Yellowstone's eruption and the study, "Modeling ash fall distribution from a Yellowstone supereruption," was published in the Wiley Online Library.

There has been a rise in demand for models projecting the density of the ash driven by a ground-collapsing eruption from the Yellowstone volcano, according to Larry Mastin, lead author of the study. Mastin is also a U.S. Geological Survey hydrologist and he helped develop the Ash3D model.

"It's a crazy thing to think about because none of us have ever seen an eruption like Yellowstone," said Mastin. "It would be two or three orders of magnitude more ash than we've been able to observe."

Yellowstone's most recent caldera eruption, a crater-forming event, occurred roughly 640,000 years ago and, despite occurring in 600,000 to 800,000 intervals, geologists have indicated that there's no evidence the supervolcano is preparing for another cataclysmic explosion -- disregard the herds.

With evidence affected by hundreds and thousands of years of erosion and seemingly dormant volcanos awaking with little notice, the study using the Ash3D model is an act of prudence. After simulating a modern-day Yellowstone eruption, researchers determine that, unlike the fan-like plumes of smaller volcanoes, a Yellowstone caldera eruption would release an "umbrella" (PDF) **of ash that would spread from the center of the U.S. and reach to both shores.**

"In essence, the eruption makes its own winds that can overcome the prevailing westerlies, which normally dominate weather patterns in the United States," said Mastin. "This helps explain the distribution from large Yellowstone eruptions of the past, where considerable amounts of ash reached the West Coast."

The effects of the supervolcano's ash cloud would have a significant impact on every part of the U.S., even regions where only millimeter or two of the soot rained down. The whole continent would suffer drastic change.

Yellowstone National Park hot spring, powered by the super volcano that lurks beneath.

"Electronic communications and air transportation would likely be shut down throughout North America," stated the study (PDF). "There would also be major climate effects. Emission of sulfur aerosols during the 1991 Pinatubo eruption produced global cooling by an average of 1 degrees Celsius for a few years, while the 50-km 3 Tambora eruption of 1815 cooled the planet enough to produce the famed 'year without a summer' in 1816, during which snow fell in June in eastern North America and crop failures led to the worst famine of the 19th century."

Cities seek new ways to cope with sea level rise – and look to the Dutch for advice

Source: http://www.homelandsecuritynewswire.com/dr20140916-cities-seek-new-ways-to-cope-with-sea-level-rise-and-look-to-the-dutch-for-advice

Scientists predict a "tenfold increase" in the frequency of hurricanes and other storms, as well as sea-level rise of eleven to twenty-four inches within a little more than three decades – and planners and managers in U.S. coastal cities are looking at new ways to prepare their cities' infrastructure for these challenges. In New York and New Orleans, city planners are studying the experience of the Dutch, who have gained a lot of experience – and fame — for their water control methods.

Water control brought the Dutch well-deserved fame // Source: uh.edu

City planners and managers are looking at new ways to prepare their cities' infrastructure for rising sea levels and more frequent and intense natural disasters by 2050.

As *Emergency Management* reports, research from organizations such as the Niels Bohr Institute and others predicts a "tenfold increase" in the frequency of hurricanes and other storms, as well as sea-level rises of eleven to twenty-four inches within a little more than three decades.

New York City is examining potential projects to make it more resilient to flooding. One project, the Big U, would create a protective system around Manhattan, shielding it from storm water. *(The Big Team/Rebuild by Design)*

Many of the largest coastal U.S. cities are, therefore, looking to revolutionize the ways in which they can protect themselves, and New Orleans and and New York are just two that are leading the charge.

In New Orleans, where residents still live in the shadows of the devastation from Hurricane Katrina in 2005, state officials are looking into new ways to invest in the strengthening of the city. In 2012, they released a $50 billion measure to assess and repair the state's vulnerabilities to future disasters. Additionally, Greater New Orleans Inc., a regional economic development group, introduced the Urban Water Plan for the Orleans, Jefferson, and St. Bernard parishes.

"We need to address our water issues in a comprehensive way, recognizing that one solution alone is not going to work," said Robin Barnes, the chief operating officer for Greater New Orleans. Their goal is to develop unique ways to manage the water within the city, and not just try to pump it out when a disaster strikes.

Barnes said that the plan is to peer into "forward-looking, urban design elements," including "rain gardens and bio-swales" in addition to upgraded canals, ponds and higher levees. This more environmentally conscious approach would also include utilizing the region's flora and fauna that already exist to also control the tides and flows of water.

In 2013, New York mayor Michael Bloomberg announced a similar plan in the shape of the $20 billion Storm Protection Plan, which includes over 250 recommendations that take an honest look at the shape of infrastructure in the city. Some of these include the widening and elevating of beaches and sand dunes, lining shorelines with massive rocks, and placing special breakers within the wave zones to decrease their force. Further, many buildings will be assessed and updated, especially those erected before 1961. Many of these ideas form the basis of the "Big U," or the greater network of protective barriers that would ultimately encircle the perimeter of the city.

While each metropolis requires different approaches, both cities

share the common element of employing the research and experience of the Dutch, who have gained a lot of experience – and fame — for their water control methods.
"The Dutch have 800 years of water management experience, so when we were developing our plans we looked closely at what they have done. We also looked at plans in other parts of the world in an effort to bring a number of the best practices back to New York," said Dan Zarrilli, the director of the Mayor's Office of Recovery and Resiliency.
Zarelli sums up the strategy of many American communities in response to climate change when he stated, "One big challenge we've run into is the perception among some that there is a silver bullet solution out there. But we've learned that the risks are too varied. We need to advance a broad range of strategies, which is exactly what we're doing."

As Louisiana Sinks And Sea Levels Rise, The State Is Drowning. Fast

Source: http://www.huffingtonpost.com/2014/08/28/louisiana-sea-level-rise_n_5731916.html

At the source's URL check this animated picture showing landscape loss from 1956 until today

In just 80 years, some 2,000 square miles of its coastal landscape have turned to open water, wiping places off maps, bringing the Gulf of Mexico to the back door of New Orleans and posing a lethal threat to an energy and shipping corridor vital to the nation's economy.
And it's going to get worse, even quicker.
Scientists now say one of the greatest environmental and economic disasters in the nation's history is rushing toward a catastrophic conclusion over the next 50 years, so far unabated and largely unnoticed.
At the current rates that the sea is rising and land is sinking, National Oceanic and Atmospheric Administration scientists say by 2100 the Gulf of Mexico could rise as much as 4.3 feet across this landscape, which has an average elevation of about 3 feet. If that happens, everything outside the protective levees — most of Southeast Louisiana — would be underwater.
The effects would be felt far beyond bayou country. The region best known for its self-proclaimed motto "*laissez les bons temps rouler*" — let the good times roll — is one of the nation's economic linchpins.
This land being swallowed by the Gulf is home to half of the country's oil refineries, a matrix of pipelines that serve 90 percent of the nation's offshore energy

production and 30 percent of its total oil and gas supply, a port vital to 31 states, and 2 million people who would need to find other places to live.

The landscape on which all that is built is washing away at a rate of a football field every hour, 16 square miles per year.

For years, most residents didn't notice because they live inside the levees and seldom travel into the wetlands. But even those who work or play in the marshes were misled for decades by the gradual changes in the landscape. A point of land eroding here, a bayou widening there, a spoil levee sinking a foot over 10 years. In an ecosystem covering thousands of square miles, those losses seemed insignificant. There always seemed to be so much left.

Now locals are trying to deal with the shock of losing places they had known all their lives — fishing camps, cypress swamps, beachfronts, even cattle pastures and backyards — with more disappearing every day.

Fishing guide Ryan Lambert is one of them. When he started fishing the wetlands out of Buras 34 years ago, he had to travel through six miles of healthy marshes, swamps and small bays to reach the Gulf of Mexico.

"Now it's all open water," Lambert said. "You can stand on the dock and *see* the Gulf."

Two years ago, NOAA removed 31 bays and other features from the Buras charts. Some had been named by French explorers in the 1700s.

The people who knew this land when it was rich with wildlife and dotted with Spanish- and French-speaking villages are getting old. They say their grandchildren don't understand what has been lost.

"I see what was," said Lloyd "Wimpy" Serigne, who grew up in the fishing and trapping village of Delacroix, 20 miles southeast of New Orleans. It was once home to 700 people; now there are fewer than 15 permanent residents. "People today — like my nephew, he's pretty young — he sees what is."

If this trend is not reversed, a wetlands ecosystem that took nature 7,000 years to build will be destroyed in a human lifetime.

The story of how that happened is a tale of levees, oil wells and canals leading to destruction on a scale almost too big to comprehend — and perhaps too late to rebuild. It includes chapters on ignorance, unintended consequences and disregard for scientific warnings. It's a story that is still unfolding.

Speck by speck, land built over centuries

The coastal landscape Europeans found when they arrived at the mouth of the Mississippi River 500 years ago was the Amazon of North America, a wetlands ecosystem of more than 6,000 square miles built by one of the largest rivers in the world.

For thousands of years, runoff from the vast stretch of the continent between the Rockies and the Appalachians had flowed into the Mississippi valley. Meltwater from retreating glaciers, seasonal snowfall and rain carried topsoil and sand from as far away as the Canadian prairies. The river swelled as it rushed southward on the continent's downward slope, toward the depression in the planet that would become known as the Gulf of Mexico.

Down on the flat coastal plain, the giant river slowed. It lost the power to carry those countless tons of sediment, which drifted to the bottom. Over thousands of years, this rain of fine particles gradually built land that would rise above the Gulf.

It wasn't just the main stem of the Mississippi doing this work. When the river reached the coastal plain, side channels — smaller rivers and bayous — peeled off. They were called "distributaries," for the job they did spreading that land-building sediment ever farther afield.

The delta had two other means of staying above the Gulf. The plants and trees growing in its marshes and swamps shed tons of dead parts each year, adding to the soil base. Meanwhile, storms and high tides carried sediment that had been deposited offshore back into the wetlands.

As long as all this could continue unobstructed, the delta continued to expand. But with any interruption, such as a prolonged drought, the new land began to sink.

That's because the sheer weight of hundreds of feet of moist soil is always pushing downward against the bedrock below. Like a sponge pressed against a countertop, the soil

compresses as the moisture is squeezed out. Without new layers of sediment, the delta eventually sinks below sea level.
The best evidence of this dependable rhythm of land building and sinking over seven millennia is underground. Geologists estimate that the deposits were at least 400 feet deep at the mouth of the Mississippi when those first Europeans arrived.
By the time New Orleans was founded in 1718, the main channel of the river was the beating heart of a system pumping sediment and nutrients through a vast circulatory network that stretched from present-day Baton Rouge south to Grand Isle, west to Texas and east to Mississippi. As late as 1900, new land was pushing out into the Gulf of Mexico.
A scant 70 years later, that huge, vibrant wetlands ecosystem would be at death's door. The exquisite natural plumbing that made it all possible had been dismantled, piece by piece, to protect coastal communities and extract oil and gas.

Engineering the river

For communities along its banks, the Mississippi River has always been an indispensable asset and their gravest threat. The river connected their economies to the rest of the world, but its spring floods periodically breached locally built levees, quickly washing away years of profits and scores of lives. Some towns were so dependent on the river, they simply got used to rebuilding.
That all changed with the Great Flood of 1927.
Swollen by months of record rainfall across the watershed, the Mississippi broke through levees in 145 places, flooding the midsection of the country from Illinois to New Orleans. Some 27,000 square miles went under as much as 30 feet of water, destroying 130,000 homes, leaving 600,000 people homeless and killing 500.
Stunned by what was then the worst natural disaster in U.S. history, Congress passed the Flood Control Act of 1928, which ordered the U.S. Army Corps of Engineers to prevent such a flood from ever happening again. By the mid-1930s, the corps had done its job, putting the river in a straitjacket of levees.
But the project that made the river safe for the communities along the river would eventually squeeze the life out of the delta. The mud walls along the river sealed it off from the landscape sustained by its sediment. Without it, the sinking of land that only occurred during dry cycles would start, and never stop.
If that were all we had done to the delta, scientists have said, the wetlands that existed in the 1930s could largely be intact today. The natural pace of sinking — scientists call it subsidence — would have been mere millimeters per year.
But we didn't stop there. Just as those levees were built, a nascent oil and gas industry discovered plentiful reserves below the delta's marshes, swamps and ridges.
At the time, wetlands were widely considered worthless — places that produced only mosquitoes, snakes and alligators. The marsh was a wilderness where few people could live, or even wanted to.
There were no laws protecting wetlands. Besides, more than 80 percent of this land was in the hands of private landowners who were happy to earn a fortune from worthless property.
Free to choose the cheapest, most direct way to reach drilling sites, oil companies dredged canals off natural waterways to transport rigs and work crews. The canals averaged 13 to 16 feet deep and 140 to 150 feet wide — far larger than natural, twisting waterways.

Effects of canals ripple across the wetlands

Eventually, some 50,000 wells were permitted in the coastal zone. The state estimates that roughly 10,000 miles of canals were dredged to service them, although that only accounts for those covered by permitting systems. The state began to require some permits in the 1950s, but rigorous accounting didn't begin until the Clean Water Act brought federal agencies into play in 1972.
Researchers say the total number of miles dredged will never be known because many of those areas are now underwater. Gene Turner, a Louisiana State University professor who has spent years researching the impacts of the canals, said 10,000 miles "would be a conservative estimate."
Companies drilled and dredged all over the coast, perhaps nowhere more quickly than the area near Lafitte, which became known as the Texaco Canals.

This fishing village 15 miles south of New Orleans had been named for the pirate who used these bayous to ferry contraband to the city. For years, the seafood, waterfowl and furbearers in the surrounding wetlands sustained the community. As New Orleans grew, Lafitte also became a favorite destination for weekend hunters and anglers.

Today those scenes are only a memory.

"Once the oil companies come in and started dredging all the canals, everything just started falling apart," said Joseph Bourgeois, 84, who grew up and still lives in the area.

From 1930 to 1990, as much as 16 percent of the wetlands was turned to open water as those canals were dredged. But as the U.S. Department of the Interior and many others have reported, the indirect damages far exceeded that:

- **Saltwater creeped in**
  Canal systems leading to the Gulf allowed saltwater into the heart of freshwater marshes and swamps, killing plants and trees whose roots held the soils together. As a side effect, the annual supply of plant detritus — one way a delta disconnected from its river can maintain its elevation — was seriously reduced.
- **Shorelines crumbled**
  Without fresh sediment and dead plants, shorelines began to collapse, increasing the size of existing water bodies. Wind gained strength over ever-larger sections of open water, adding to land loss. Fishers and other boaters used canals as shortcuts across the wetlands; their wakes also sped shoreline erosion. In some areas, canals grew twice as wide within five years.
- **Spoil levees buried and trapped wetlands**
  When companies dredged canals, they dumped the soil they removed alongside, creating "spoil levees" that could rise higher than 10 feet and twice as wide.
- The weight of the spoil on the soft, moist delta caused the adjacent marshes to sink. In locations of intense dredging, spoil levees impounded acres of wetlands. The levees also impeded the flow of water — and sediments — over wetlands during storm tides.
- If there were 10,000 miles of canals, there were 20,000 miles of levees. Researchers estimate that canals and levees eliminated or covered 8 million acres of wetlands.

All this disrupted the delta's natural hydrology — its circulatory system — and led to the drowning of vast areas. Researchers have shown that land has sunk and wetlands have disappeared the most in areas where canals were concentrated.

In the 1970s, up to 50 square miles of wetlands were disappearing each year in the areas with heaviest oil and gas drilling and dredging, bringing the Gulf within sight of many communities.

As the water expanded, people lived and worked on narrower and narrower slivers of land.

"There's places where I had cattle pens, and built those pens … with a tractor that weighed 5,000 or 6,000 pounds," said Earl Armstrong, a cattle rancher who grew on the river nine miles south of the nearest road. "Right now we run through there with airboats."

There are other forces at work, including a series of geologic faults in the delta and the rock layers beneath, but a U.S. Department of Interior report says **oil and gas canals are ultimately responsible for 30 to 59 percent of coastal land loss.** In some areas of Barataria Bay, said Turner at LSU, it's close to 90 percent.

Canals created for navigation and oil and gas pipelines cut through the marsh off the coast of Louisiana, U.S., on Monday, July 26, 2010.

Even more damage was to come as the oil and gas industry shifted offshore in the late 1930s, eventually planting about 7,000 wells in the Gulf. To carry that harvest to onshore refineries, companies needed more underwater pipelines. So they dug wider, deeper

waterways to accommodate the large ships that served offshore platforms.
Congress authorized the Corps of Engineers to dredge about 550 miles of navigation channels through the wetlands. The Department of Interior has estimated that those canals, averaging 12 to 15 feet deep and 150 to 500 feet wide, resulted in the loss of an additional 369,000 acres of coastal land.
Researchers eventually would show that the damage wasn't due to surface activities alone. When all that oil and gas was removed from below some areas, the layers of earth far below compacted and sank. Studies have shown that coastal subsidence has been highest in some areas with the highest rates of extraction.

Push to hold industry accountable

The oil and gas industry, one of the state's most powerful political forces, has acknowledged some role in the damages, but so far has defeated efforts to force companies to pay for it.
The most aggressive effort to hold the industry accountable is now underway. In July 2013, the Southeast Louisiana Flood Protection Authority-East, which maintains levees around New Orleans, filed suit against more than 90 oil, gas and pipeline companies.
The lawsuit claims that the industry, by transforming so much of the wetlands to open water, has increased the size of storm surges. It argues this is making it harder to protect the New Orleans area against flooding and will force the levee authority to build bigger levees and floodwalls.
The lawsuit also claims that the companies did not return the work areas to their original condition, as required by state permits.
"The oil and gas industry has complied with each permit required by the State of Louisiana and the Corps of Engineers since the permits became law," said Ragan Dickens, spokesman for the Louisiana

Oil and Gas Association.
State leaders immediately rose to the industry's defense. Much of the public debate has not been about the merits of the suit; instead, opponents contested the authority's legal right to file the suit and its contingency fee arrangement with a private law firm.
"We're not going to allow a single levee board that has been hijacked by a group of trial lawyers to determine flood protection, coastal restoration and economic repercussions for the entire State of Louisiana," said Gov. Bobby Jindal in a news release demanding that the levee authority withdraw its suit.

"A better approach," he said in the statement, "to helping restore Louisiana's coast includes holding the Army Corps of Engineers accountable, pushing for more offshore revenue sharing and holding BP accountable for the damage their spill is doing to our coast."
The industry's political clout reflects its outsized role in the economy of one of the nation's poorest states. The industry directly employs 63,000 people in the state, according to the federal Department of Labor.
Many of those employees live in the coastal parishes that have suffered most from oil and gas activities and face the most severe consequences from the resulting land loss.
Legislators in those areas helped Jindal pass a law that retroactively sought to remove the levee authority's standing to file the suit. The constitutionality of that law is now before a federal judge.

Consequences now clear

Even as politicians fought the lawsuit, it was hard to deny what was happening on the ground.
By 2000, coastal roads that had flooded only during major hurricanes were going underwater when high tides coincided with strong southerly winds. Islands and beaches that had been landmarks for lifetimes were gone, lakes had turned into bays, and bays had eaten through their borders to join the Gulf.
"It happened so fast, I could actually see the difference day to day, month to month," said Lambert, the fishing guide in Buras.
Today, in some basins around New Orleans, land is sinking an inch every 30 months. At this pace, by the end of the century this land will sink almost 3 feet in an area that's barely above sea level today.
Meanwhile, global warming is causing seas to rise worldwide. Coastal landscapes everywhere are now facing a serious threat, but none more so than Southeast Louisiana.
The federal government projects that seas along the U.S. coastline will rise 1.5 to 4.5 feet by 2100. Southeast Louisiana would see "at least" 4 to 5 feet, said NOAA scientist Tim Osborn.
The difference: This sediment-starved delta is sinking at one of the fastest rates of any large coastal landscape on the planet at the same time the oceans are rising.
Maps used by researchers to illustrate what the state will look like in 2100 under current projections show the bottom of Louisiana's "boot" outline largely gone, replaced by a coast running practically straight east to west, starting just south of Baton Rouge. The southeast corner of the state is represented only by two fingers of land – the areas along the Mississippi River and Bayou Lafourche that currently are protected by levees.

Finally, a plan to rebuild — but not enough money

Similar predictions had been made for years. But Hurricane Katrina finally galvanized the state Legislature, which pushed through a far-reaching coastal restoration plan in 2007.
The 50-year, $50 billion Master Plan for the Coast (in 2012 dollars) includes projects to build levees, pump sediment into sinking areas, and build massive diversions on the river to reconnect it with the dying delta.
The state's computer projections show that by 2060 — if projects are completed on schedule — more land could be built annually than is lost to the Gulf.
But there are three large caveats.

- **The state is still searching for the full $50 billion**. Congress so far has been unwilling to help.
- If the plan is to work, sea-level rise can't be as bad as the worst-case scenario.
- Building controlled sediment diversions on the river, a key part of the land-building strategy, has never been done before. The predictions, then, are largely hypothetical, although advocates say the concept is being proven by an uncontrolled diversion at West Bay, near the mouth of the river.

Some of the money will come from an increased share of offshore oil and gas royalties, but many coastal advocates say the industry should pay a larger share.
In fact, leaders of the regional levee authority have said the purpose of the lawsuit was to make the industry pay for the rebuilding plan, suggesting that state could trade immunity from future suits for bankrolling it.
That idea is gaining momentum in official circles, despite the industry's latest win in the state Legislature.
Kyle Graham, executive director of the Louisiana Coastal Protection and Restoration Authority, said recently that the industry understands its liability for the crumbling coast

and is discussing some kind of settlement. “It's very difficult to see a future in which that [such an agreement] isn't there,” he said he said.
Graham has said current funding sources could keep the restoration plan on schedule only through 2019. He was blunt when talking about what would happen if more money doesn’t come through: There will be a smaller coast.
“There are various sizes of a sustainable coastal Louisiana,” he said. “And that could depend on how much our people are willing to put up for that.”

We used to see Louisiana on the map as a "BOOT". This "boot" does not exist anymore!

A vanishing culture

Trying to keep pace with the vanishing pieces of southeast Louisiana today is like chasing the sunset; it’s a race that never ends.
Lambert said when he’s leading fishing trips, he finds himself explaining to visitors what he means when he says, “This used to be Bay Pomme d’Or” and the growing list of other spots now only on maps.
Signs of the impending death of this delta are there to see for any visitor.
Falling tides carry patches of marsh grass that have fallen from the ever-crumbling shorelines.
Pelicans circle in confusion over nesting islands that have washed away since last spring.
Pilings that held weekend camps surrounded by thick marshes a decade ago stand in open water, hundreds of yards from the nearest land — mute testimony to a vanishing culture.
Shrimpers push their wing nets in lagoons that were land five years ago.
The bare trunks of long-dead oaks rise from the marsh, tombstones marking the drowning of high ridges that were built back when the river pumped life-giving sediment through its delta.
“If you’re a young person you think this is what it’s supposed to look like,” Lambert said. “Then when you’re old enough to know, it’s too late.”

*This story was written by **Bob Marshall** of The Lens.*

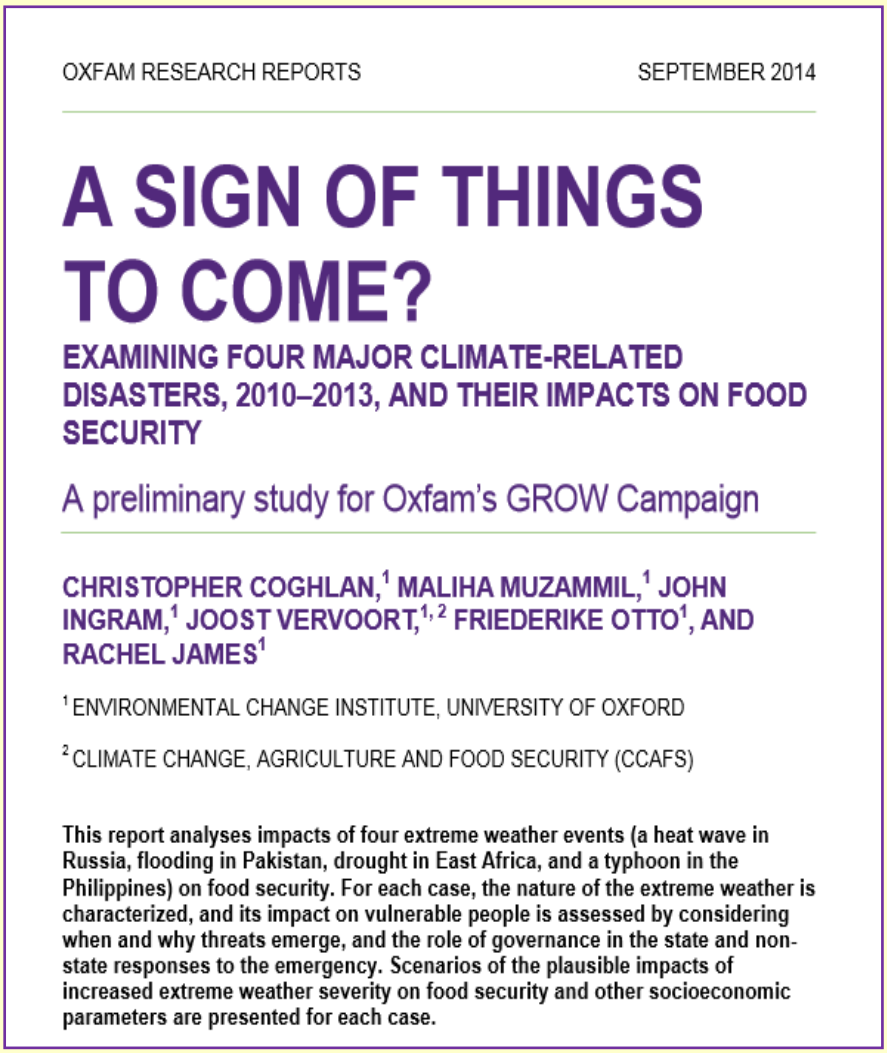
New report identifies populations most vulnerable to extreme weather events

Source: http://www.homelandsecuritynewswire.com/dr20140923-new-report-identifies-populations-most-vulnerable-to-extreme-weather-events

Extreme weather events leave populations with not enough food both in the short- and the long-term. A new report by the Environmental Change Institute (ECI) at the School of Geography and the Environment at the University of Oxford concludes that better governance could have lessened the impact on the poorest and most vulnerable, and affected populations have been

let down by the authorities in the past.

A University of Oxford release reports that the report, commissioned by the charity Oxfam, tracks the effects on four countries: Russia, which experienced a heatwave in 2010; flood-hit Pakistan the same year; East Africa during the drought of 2010-11; and the Philippines after Typhoon Haiyan in 2013. The researchers conclude that the authorities in each of the countries studied were unprepared for extreme weather events, and citizens suffered even more than they needed to.



OXFAM RESEARCH REPORTS SEPTEMBER 2014

A SIGN OF THINGS TO COME?

EXAMINING FOUR MAJOR CLIMATE-RELATED DISASTERS, 2010–2013, AND THEIR IMPACTS ON FOOD SECURITY

A preliminary study for Oxfam's GROW Campaign

CHRISTOPHER COGHLAN,[1] MALIHA MUZAMMIL,[1] JOHN INGRAM,[1] JOOST VERVOORT,[1,2] FRIEDERIKE OTTO[1], AND RACHEL JAMES[1]

[1] ENVIRONMENTAL CHANGE INSTITUTE, UNIVERSITY OF OXFORD

[2] CLIMATE CHANGE, AGRICULTURE AND FOOD SECURITY (CCAFS)

This report analyses impacts of four extreme weather events (a heat wave in Russia, flooding in Pakistan, drought in East Africa, and a typhoon in the Philippines) on food security. For each case, the nature of the extreme weather is characterized, and its impact on vulnerable people is assessed by considering when and why threats emerge, and the role of governance in the state and non-state responses to the emergency. Scenarios of the plausible impacts of increased extreme weather severity on food security and other socioeconomic parameters are presented for each case.

The report, *A Sign of Things to Come?,* says that the **Russian** heatwave led to a hoarding of food supplies and price-fixing by speculators, which compounded food shortages and led to global wheat prices rising dramatically. It also suggests this could possibly be linked with the political upheaval in the Middle East, with Egypt's hungry protestors suffering the most.

In **Pakistan**, "coercive landlords" took advantage of smallholders and others affected by the floods, says the report. Overall, the flooding is estimated to have led to an 80 percent rise in wheat and rice prices in 2010.

The drought-affected people of **East Africa** did not receive international or domestic aid for six months, partly due to the risks posed by armed groups. Food prices reached record levels in several markets including wheat in Ethiopia, maize in Kenya and red sorghum grain in Somalia, says the report. It notes that children under five accounted for over half of all deaths in Somalia.

Meanwhile in the **Philippines**, although storm surges were not a new problem, they were not properly understood by central and local governments, says the report. The exceptional storm surge associated with Typhoon Haiyan hit farmers and fishing communities particularly hard, with women, children and some ethnic minorities facing discrimination with aid distribution.

On a global level, the report warns that climate change is expected to increase the intensity and frequency of heatwaves and floods. It says although there is no scientific evidence to show a specific weather event would not have happened without climate change, scientists can estimate whether it increases the risk of an event. It finds that the **Russian heat wave and the East African drought were more likely because of climate change, but there is not yet the evidence to say that climate change played a part in the floods in Pakistan or Typhoon Haiyan.**

One of the lead authors Dr. John Ingram said: "Weather has always affected food security, particularly for many of the world's poorest people. Perhaps we think of farmers or fishermen first, but extreme weather will affect many more people in other ways too. While direct measures such as emergency preparedness and the strengthening of response-related institutions is helpful, this study has identified the need for a wider cultural shift to ensure the poorest and most vulnerable are properly protected.

This goes beyond mere technical improvements to equipment or redirected funding and gets to the very heart of what "climate justice" should be about."

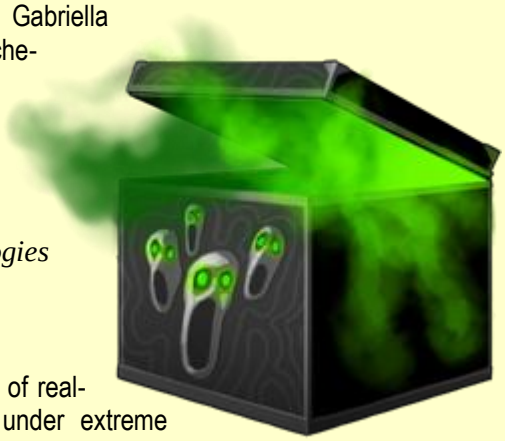
▶ **Read the full report at:** http://www.eci.ox.ac.uk/publications/downloads/2014-oxfam.pdf

Training Crisis Managers

Source: http://www.igi-global.com/article/using-emotional-intelligence-training-crisis/77841

Using Emotional Intelligence in Training Crisis Managers: The Pandora Approach

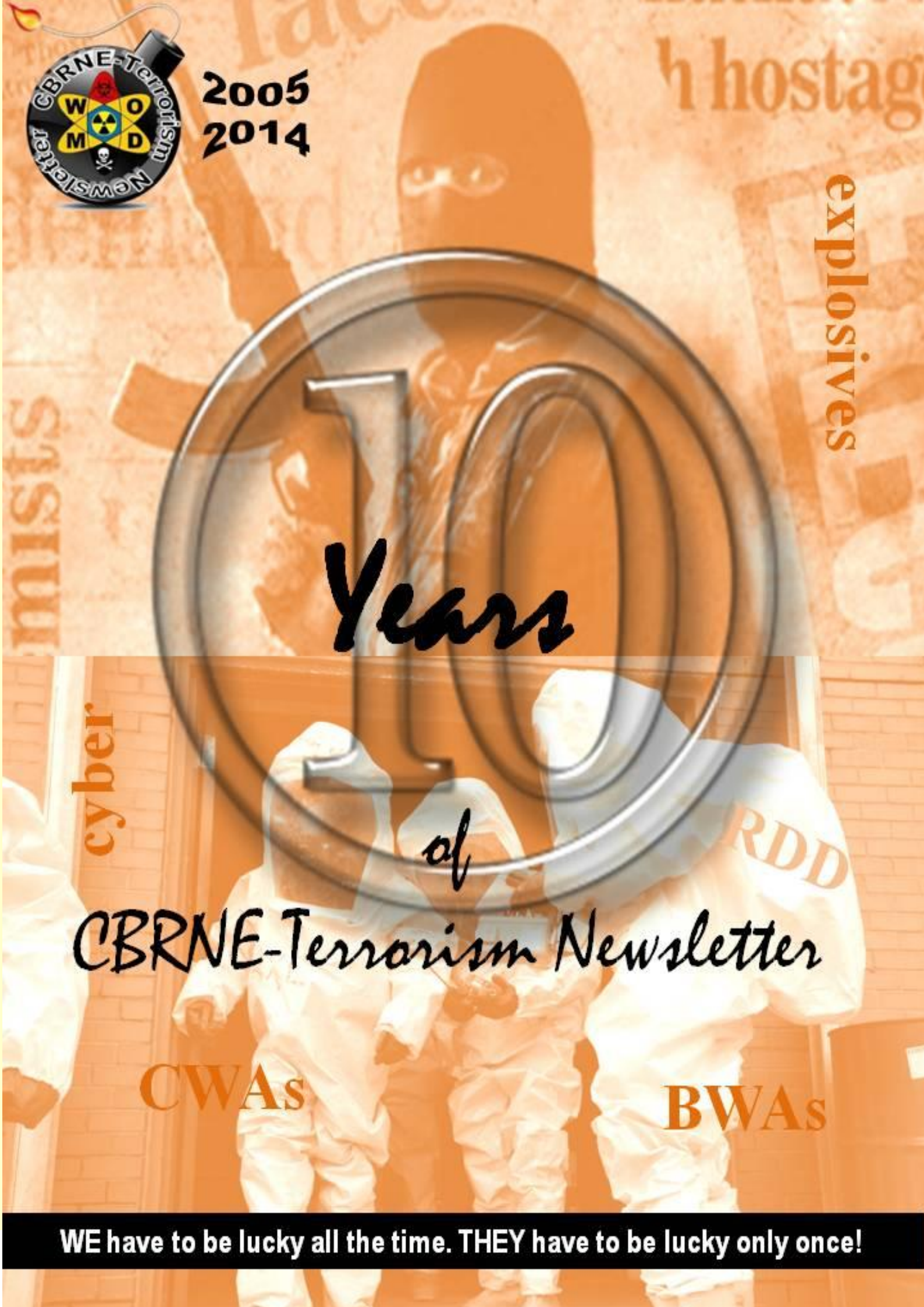
By Lachlan Mackinnon (School of Computing & Mathematical Sciences, Old Royal Naval College, University of Greenwich, London, UK), Liz Bacon (School of Computing & Mathematical Sciences, Old Royal Naval College, University of Greenwich, London, UK), Gabriella Cortellessa (Consiglio Nazionale delle Ricerche-Istituto di Scienze e Tecnologie della Cognizione, Rome, Italy) and Amedeo Cesta (Consiglio Nazionale delle Ricerche-Istituto di Scienze e Tecnologie della Cognizione, Rome, Italy)



International Journal of Distance Education Technologies (IJDET).Volume 11, Issue 2 (2013)

Abstract

Multi-agency crisis management represents one of the most complex of real-world situations, requiring rapid negotiation and decision-making under extreme pressure. However, the training offered to strategic planners, called Gold Commanders, does not place them under any such pressure. It takes the form of paper-based, table-top exercises, or expensive, real-world, limited-scope simulations. The Pandora project has developed a rich multimedia training environment for Gold Commanders, based on a crisis scenario, timeline-based, event network, with which the trainees and their trainer interact dynamically. Pandora uses the emotional intelligence of the trainees, through a behavioural modelling component, to support group dynamic and decision-making. It applies systemic emotional intelligence, based on inferred user state and rule-based affective inputs, to impact the stress levels of the trainees. Pandora can impose variable stress on trainees, to impact their decision-making, and model their behaviour and performance under stress, potentially resulting in more effective and realisable strategies.


CBRNE-Terrorism Newsletter
W
O
M
D
2005
2014
10
Years
of
CBRNE-Terrorism Newsletter
explosives
cyber
RDD
CWAs
BWAs
WE have to be lucky all the time. THEY have to be lucky only once!