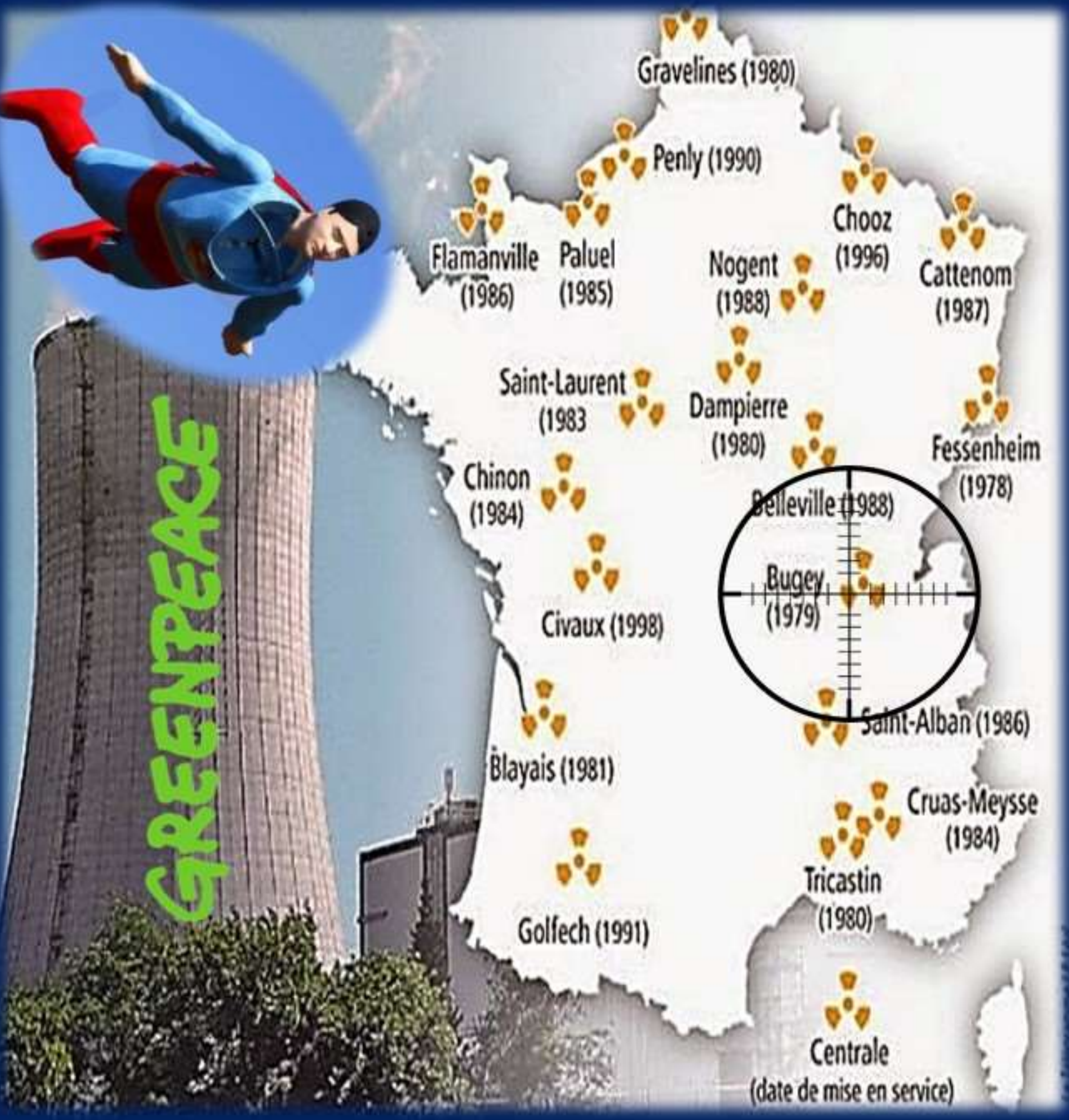
C2BRNE DIARY

Dedicated to Global First Responders

July 2018



www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

How to make radiation safety training easier and more effective

By Steven Pike

Source: http://www.argonelectronics.com/blog/how-to-make-radiation-safety-training-easier-and-more-effective

May 23 – A key objective for HazMat and CBRNe instructors is to be able to devise realistic radiation safety training opportunities that replicate the challenges and conditions of live incidents.

There are a variety of key skills that you may well want to be able to observe and assess in your radiation safety training exercises, including:

- Their understanding of critical search, reconnaissance, survey and location skills
- Their comprehension of inverse square law
- Their knowledge of isodoserate mapping, shielding and safe demarcation
- Their understanding of contamination, cross-contamination and decontamination

Hands-on training exercises can offer an invaluable opportunity to test your students' ability to read, interpret and accurately convey the information from their survey meters.

And wherever possible, these training exercises should enable you to mimic the complex physical and psychological challenges that your trainees are likely to face in real-life radiation events.

Training for live radiation incidents

Within the context of radiation safety, the Mirion RADOS RDS-200 Universal Survey Meter is an essential tool that is widely used by personnel across a diverse range of contexts, from military and civil defence to industrial and laboratory use.

A big selling point of the RDS-200 is that its interface has been designed around an easy-to-use menu structure. The question remains however - how you can create training scenarios that best replicate how that device will function in a real-life incident as it responds to an ionizing radiation source?

While training with actual radiological sources undoubtedly offers a high degree of realism, there is also a significant cost, administrative effort and health and safety consideration which can make these methods impractical except for in highly specialized situations.

Even very short term exposure to controlled quantities of radiation carries with it an element of risk. So if you can devise a scenario that removes the need for an ionizing radiation source, you instantly resolve a raft of regulatory, environmental and safety issues.

But what options exist for creating realistic, hands-on training scenarios that can accurately reflect the conditions of live radiation incidents for your students?

One solution is to use an intelligent, electronic simulator detector that can replicate all the functionality of a real detector.

The key point of difference with this training approach is that electronic simulator detectors have been designed to respond to a safe electronic source. So they can be used in any setting (including public buildings) and with zero risk to personnel, the environment or infrastructure.

For training in the use of the Mirion RADOS RDS-200 portable survey meter for example, there is the option to replace the actual device with a simulator version such as the RDS-200-SIM.

The RDS-200-SIM

The RDS-200-SIM works by receiving an encoded signal from a deployed electronic simulation source (or sources) which represents specific gamma emitting radionuclides.

The simulator is compatible with the GMP-11-SIM probe, which responds to fluorescent powder and liquid materials that simulate beta sources for training in contamination, cross-contamination and decontamination. It can also be used in conjunction with the PlumeSIM wide area exercise system for tactical field and nuclear emergency response exercises.

If it's required, multi-detector and multi-isotrope training can take place within the same scenario. And there is also the option to include hazardous substance releases (including chemical warfare agents) to drive HazMat / CW simulation detectors.

Safety, efficiency and enhanced learning outcomes

Electronic simulator detectors such as the RDS-200-SIM offer a realistic, hands-on training experience which enables radiological incident instructors to safely teach (and evaluate) every aspect of a trainee's response to a simulated radiation incident.

And crucially too, the use of simulator detectors enables you to quickly and easily set-up and break-down your exercises.

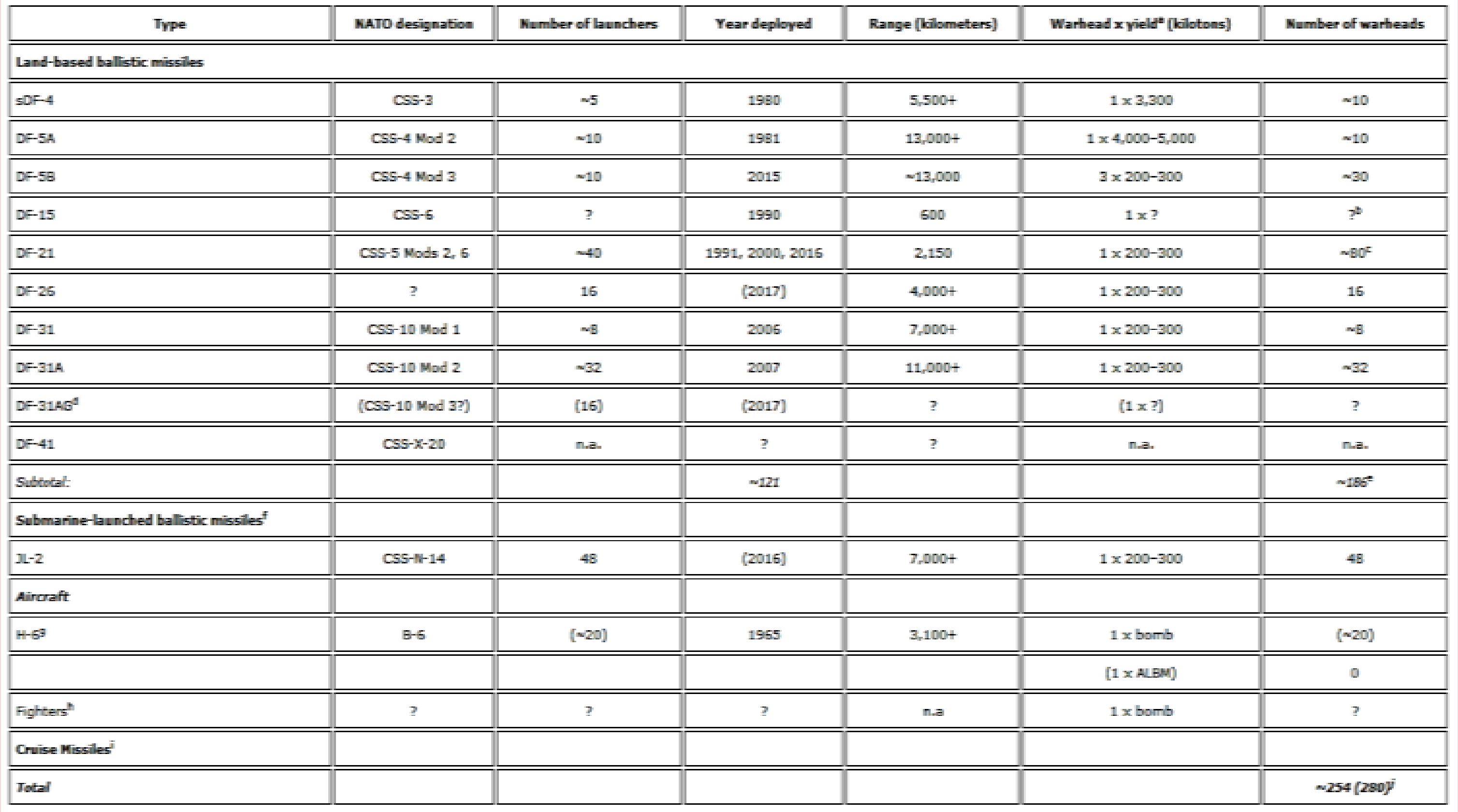
For HazMat and CBRNe instructors, there are many tangible benefits - with less time wasted on logistics and administration, and more opportunity to focus on delivering the best possible learning experience for your trainees.

Chinese nuclear forces, 2018

By Hans M. Kristensen and Robert S. Norris

Source: https://www.tandfonline.com/doi/full/10.1080/00963402.2018.1486620

June 25 – The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Robert S. Norris, a senior fellow with the FAS. The Nuclear Notebook column has been published in the *Bulletin of the Atomic Scientists* since 1987. This issue's column examines China's nuclear arsenal, which includes about 280 warheads for delivery by ballistic missiles and bombers. This stockpile is likely to grow further over the next decade.



Type	NATO designation	Number of launchers	Year deployed	Range (kilometers)	Warhead x yield[a] (kilotons)	Number of warheads
Land-based ballistic missiles						
sDF-4	CSS-3	~5	1980	5,500+	1 x 3,300	~10
DF-5A	CSS-4 Mod 2	~10	1981	13,000+	1 x 4,000–5,000	~10
DF-5B	CSS-4 Mod 3	~10	2015	~13,000	3 x 200–300	~30
DF-15	CSS-6	?	1990	600	1 x ?	?[b]
DF-21	CSS-5 Mods 2, 6	~40	1991, 2000, 2016	2,150	1 x 200–300	~80[c]
DF-26	?	16	(2017)	4,000+	1 x 200–300	16
DF-31	CSS-10 Mod 1	~8	2006	7,000+	1 x 200–300	~8
DF-31A	CSS-10 Mod 2	~32	2007	11,000+	1 x 200–300	~32
DF-31AG[d]	(CSS-10 Mod 3?)	(16)	(2017)	?	(1 x ?)	?
DF-41	CSS-X-20	n.a.	?	?	n.a.	n.a.
Subtotal:			*~121*			*~186[e]*
Submarine-launched ballistic missiles[f]						
JL-2	CSS-N-14	48	(2016)	7,000+	1 x 200–300	48
Aircraft						
H-6[g]	B-6	(~20)	1965	3,100+	1 x bomb	(~20)
					(1 x ALBM)	0
Fighters[h]	?	?	?	n.a	1 x bomb	?
Cruise Missiles[i]						
Total						***~254 (280)[j]***

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

Hans M. Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author of the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has coauthored Nuclear Notebook since 2001.

Robert S. Norris is a senior fellow with the Federation of American Scientists in Washington, DC. A former senior research associate with the Natural Resources Defense Council, his principal areas of expertise include writing and research on all aspects of the nuclear weapons programs of the United States, the Soviet Union and Russia, the United Kingdom, France, and China, as well as India, Pakistan, and Israel. He is the author of *Racing for the Bomb: General Leslie R. Groves, the Manhattan Project's Indispensible Man* (Steerforth) and co-author of *Making the Russian Bomb: From Stalin to Yeltsin* (Westview). He co-authored or contributed to the chapter on nuclear weapons in the 1985–2000 editions of the *SIPRI Yearbook* (Oxford University Press) and has co-authored Nuclear Notebook since 1987.

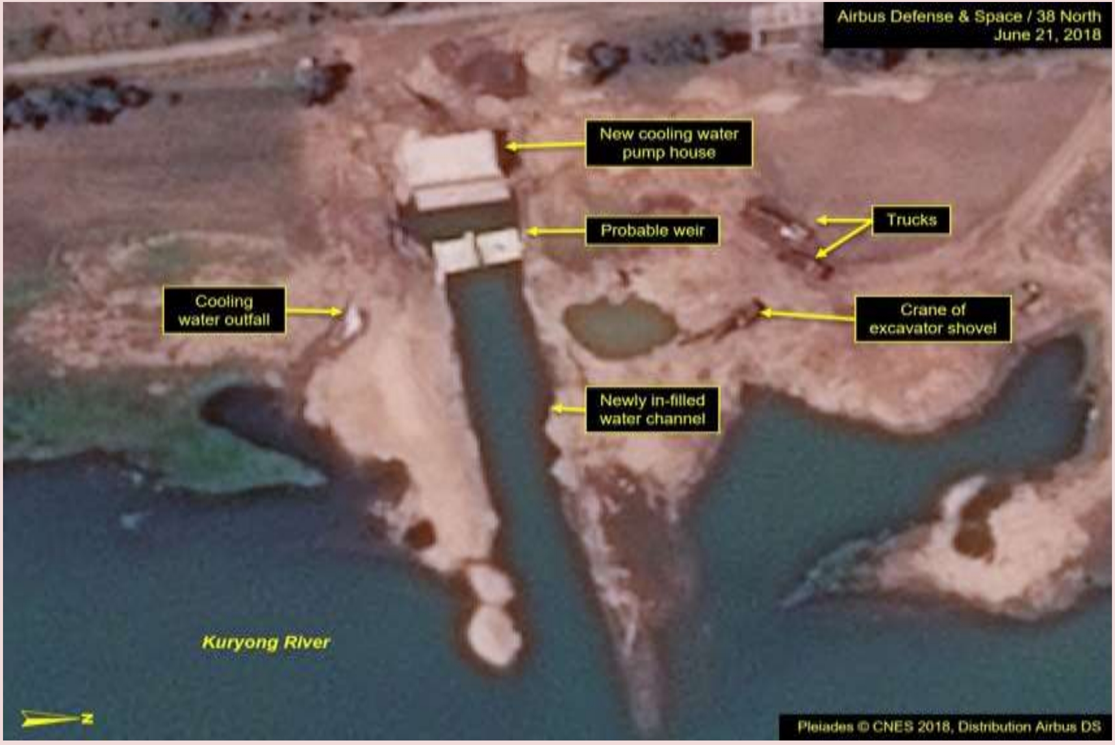
Satellite images show North Korea upgrading nuclear facility

By Zachary Cohen (CNN)

Source: https://edition.cnn.com/2018/06/27/politics/north-korea-infrastructure-improvements-nuclear-facility/index.html

June 27 – New satellite images show North Korea has made rapid improvements to the infrastructure at its Yongbyon Nuclear Scientific Research Center -- a facility used to produce weapons-grade fissile material, according to an analysis published by 38 North, a prominent North Korea monitoring group.

Captured on June 21, the photos reveal modifications to the site's plutonium production reactor and the construction of several support facilities -- long-planned upgrades that were already underway before North Korean leader Kim Jong Un and US President Donald Trump met in Singapore earlier this month.


Airbus Defense & Space / 38 North
June 21, 2018
New cooling water pump house
Probable weir
Trucks
Cooling water outfall
Crane of excavator shovel
Newly in-filled water channel
Kuryong River
N
Pleiades © CNES 2018, Distribution Airbus DS

When contacted by CNN about 38 North's analysis, the Unification Ministry said they "cannot confirm the report" and are "watching it closely."

The report states that "continued work at the Yongbyon facility should not be seen as having any relationship to North Korea's pledge to denuclearize," but the photos suggest that Pyongyang continues to proceed with business as usual when it comes to maintaining its nuclear sites following the summit.

"No change is actually a pretty significant story ... this is still an active site producing plutonium for North Korea," according to Jeffrey Lewis, a professor at the Middlebury Institute of International Studies.

The images stand in stark contrast to Trump's recent declaration that the North Korean regime no longer poses a nuclear threat, even though the meeting produced no verifiable proof that North Korea will discontinue its nuclear program.

Secretary of State Mike Pompeo said Wednesday that North Korea remains a nuclear threat, but defended Trump's previous comment.

"I'm confident what he intended there was we did reduce the threat," said Pompeo. "I don't think there's any doubt about that. We took the tension level down."

"I think his point was a fair one," he added. "For the moment, we have reduced risk."

But Trump has repeatedly mischaracterized the nature of his deal with Kim, insisting last week that the North Korean dictator had agreed to begin "total denuclearization" right away.

In reality, the document he signed with Kim at their June 12 summit in Singapore only reiterated North Korea's previous commitment to "work toward complete denuclearization of the Korean Peninsula," and the new images released Wednesday align with Defense Secretary James Mattis' assessment that Pyongyang remains in a holding pattern as negotiators discuss the next steps in talks.

"The summit pledge is important, but it was not a written agreement that laid out what the North Koreans have to do -- that doesn't exist right now, so I'm not surprised they are continuing to operate their facilities," said Joel Wit, a Senior Fellow at the Stimson Center and Director of 38 North.

Adam Mount, a senior fellow and director at the Federation of American Scientists, agreed that the images indicate that North Korea will continue to support the foundation of its nuclear program until the two sides are able to agree on specific terms.

"Because Kim Jong Un has so far avoided making a commitment to halt research and development activities, the changes are not a success or failure of the diplomatic process, but simply a signal that North Korea's nuclear infrastructure remains fully in use," Mount told CNN.

"That Yongbyon continues to receive scarce funds speaks to its continued value to the regime. There is little indication that North Korea has halted research, development, or production of nuclear systems even as talks continue," he added.

North Korea also maintains other nuclear facilities where they produce the bulk of their nuclear weapons materials and missiles. While these sites cannot be detected by monitoring groups, they are assumed to remain operational, according to Wit.

Trump has often pointed to the absence of North Korean missile and nuclear tests in recent months as a sign of progress toward denuclearization, but continued maintenance of facilities like Yongbyon show that talks with the US have not yet prompted Kim to take significant steps toward truly dismantling the foundation of his program.

"Both secret and Yongbyon facilities can continue operating and expand the fissile material stockpile," Vipin Narang, an associate professor of political science at the Massachusetts Institute of Technology who studies nuclear proliferation, told CNN.

"We have no way to stop this or verify any pledges to freeze," he said, noting that Kim has intentionally only agreed to freeze full blown testing, not production.

North Korea can also continue to improve its warhead and ballistic designs without conducting tests, Narang added.

"North Korea has had a decade-long nuclear testing sequence where they have presumably learned a lot about designs," he told CNN. "They probably do not need full blown tests to go into serial production of warheads. And they can improve components and perfect designs with subcritical and hydrodynamic tests which we wouldn't be able to monitor or detect."

Ultimately, 38 North's analysis of these images provides a realistic look at the current state of North Korea's nuclear program amid talks with the US and the challenges facing negotiators tasked with achieving denuclearization -- a process for which Pompeo has refused to offer a timeline.

"We should remain skeptical that North Korea's nuclear calculus has changed dramatically. Every indication since the beginning of the year is that Pyongyang is seeking to exploit diplomacy to its advantage, including by continuing to improve its arsenal," Mount told CNN. "Halting a clearly-defined list of weapons activities should be the first step in negotiations."

"What is needed now is sustained and direct negotiations between the two sides on a framework for phased steps on denuclearization, as well as concrete steps toward a peace regime on the Korean peninsula," according to Kingston Reif, director for disarmament and threat reduction policy at the Arms Control Association.

"So far, such a framework has not been established. In other words, there is no 'deal,'" he said.

US to send next-generation nuclear weapons to Turkey: Russian report

Source: http://www.hurriyetdailynews.com/us-to-send-next-generation-nuclear-weapons-to-turkey-russian-report-134073

July 02 – Russian state media claimed on July 2 that the United States is preparing to send the next generation of B61 guided nuclear gravity bombs to NATO bases in European countries, including Turkey.

The U.S. Department of Energy's National Nuclear Security Administration (DOE/NNSA) and the U.S. Air Force completed two non-nuclear system qualification flight tests of the B61-12 gravity bomb on June 9 at Tonopah Test Range in Nevada, according to a June 29 statement by DOE/NNSA.

The test, which was reportedly the first of its kind, was aimed at extending the B61 bomb's service life by adapting it to next generation aircraft, including B-2A Spirit Bomber.

"The B61-12 LEP will consolidate and replace the existing B61 bomb variants in the [U.S.] nuclear stockpile. The first production unit is on schedule for completion in fiscal year 2020," the statement said.

Russia's state-run RIA news agency claimed on July 2 that the nuclear bomb will also be adapted to the F-35 aircrafts.

"The United States continues to invest in weapons of mass destruction. The NATO bases in Turkey, Germany and Italy will receive the new bombs in 2020," Russian nuclear expert Alexandr Jilin was quoted as saying by the agency.

The United States has a total of 150 nuclear weapons in five NATO member countries, including Turkey, according to a report on worldwide nuclear arms prepared by the Turkish Parliament in October 2017.

Among those weapons, B61 type bombs are still in the İncirlik air base in the southern Turkish province of Adana.

According to data from the Federation of American Scientists (FAS), the number of B61s in Turkey is estimated to be nearly 50.

U.S. officials neither confirm nor deny reports about NATO's nuclear weapons in Turkey.

US has 150 nuclear weapons in five NATO countries: Turkish Parliament report

Source: http://www.hurriyetdailynews.com/us-has-150-nuclear-weapons-in-five-nato-countries-turkish-parliament-report-121667

October 2017 – The United States has a total of 150 nuclear weapons in five NATO member countries, including Turkey, according to a report on worldwide nuclear arms prepared by the Turkish Parliament.

The report, titled "Data on Nuclear Weapons," said there were around 15,000 nuclear weapons at 107 sites in 14 countries as of July this year, daily Milliyet reported on Oct. 31.

"Nearly 9,400 of these weapons are in arsenals for military use and the rest are standing idle to be destroyed," the report read.

It added that some 4,150 of the weapons in arsenals are ready to be used at any minute, while 1,800 are in "high alarm" status, which means they can be prepared for use in a short period of time.

According to the report, 93 percent of the world's nuclear weapons belong to Russia and the U.S.

The report also said that nuclear weapons belonging to the U.S. are present in five NATO countries that do not themselves have nuclear weapons.

Saying there are nuclear weapons belonging to the U.S. in five NATO countries that do not have nuclear weapons.

“There are nearly 150 U.S. nuclear weapons in six air bases in Belgium, Germany, Italy, the Netherlands and Turkey, which are NATO countries that don’t themselves own nuclear weapons,” it added.

The U.S., China, Russia, France and Britain are nuclear-armed state parties to the Treaty on the Prohibition of Nuclear Weapons, while India, Pakistan and Israel never became parties even though they own nuclear weapons.

According to the data in parliament’s report, Russia has 7,000 nuclear weapons, the U.S. has 6,800, France has 300, China has 260, Britain has 215, Pakistan has 130, India has 120, Israel has 80 and North Korea has 10 nuclear weapons.

During the Cold War, the U.S. placed nuclear weapons in NATO countries, including Turkey, as part of the organization’s nuclear sharing program. Some of the nuclear weapons placed in the 1960s are still in Turkey today.

At the time, negotiations were carried out between Ankara and Washington in the 1950s and they were concluded at the beginning of the 1960s.

Among those weapons, B61 type bombs are still in the İncirlik air base in the southern Turkish province of Adana. Nuclear warhead Jupiter missiles that were sent to the country during the same time period were only kept in the country between 1961 and 1963.

According to data from the Federation of American Scientists (FAS), the number of B61s in Turkey is estimated to be nearly 50.

Tsar Bomba

Source: https://en.wikipedia.org/wiki/Tsar_Bomba

Tsar Bomba (*Ivan bomb/King of Bombs*;) was the Western nickname for the Soviet RDS-220 hydrogen bomb (code name *Ivan* or *Vanya*), the most powerful nuclear weapon ever created. Its test on 30 October 1961 remains the most powerful explosive ever detonated. It was also referred to as *Kuzma's mother*, possibly referring to First secretary Nikita Khrushchev's promise to *show the United States a Kuzma's mother* (an idiom roughly translating to "We'll show you!") at a 1960 session of United Nations General Assembly.

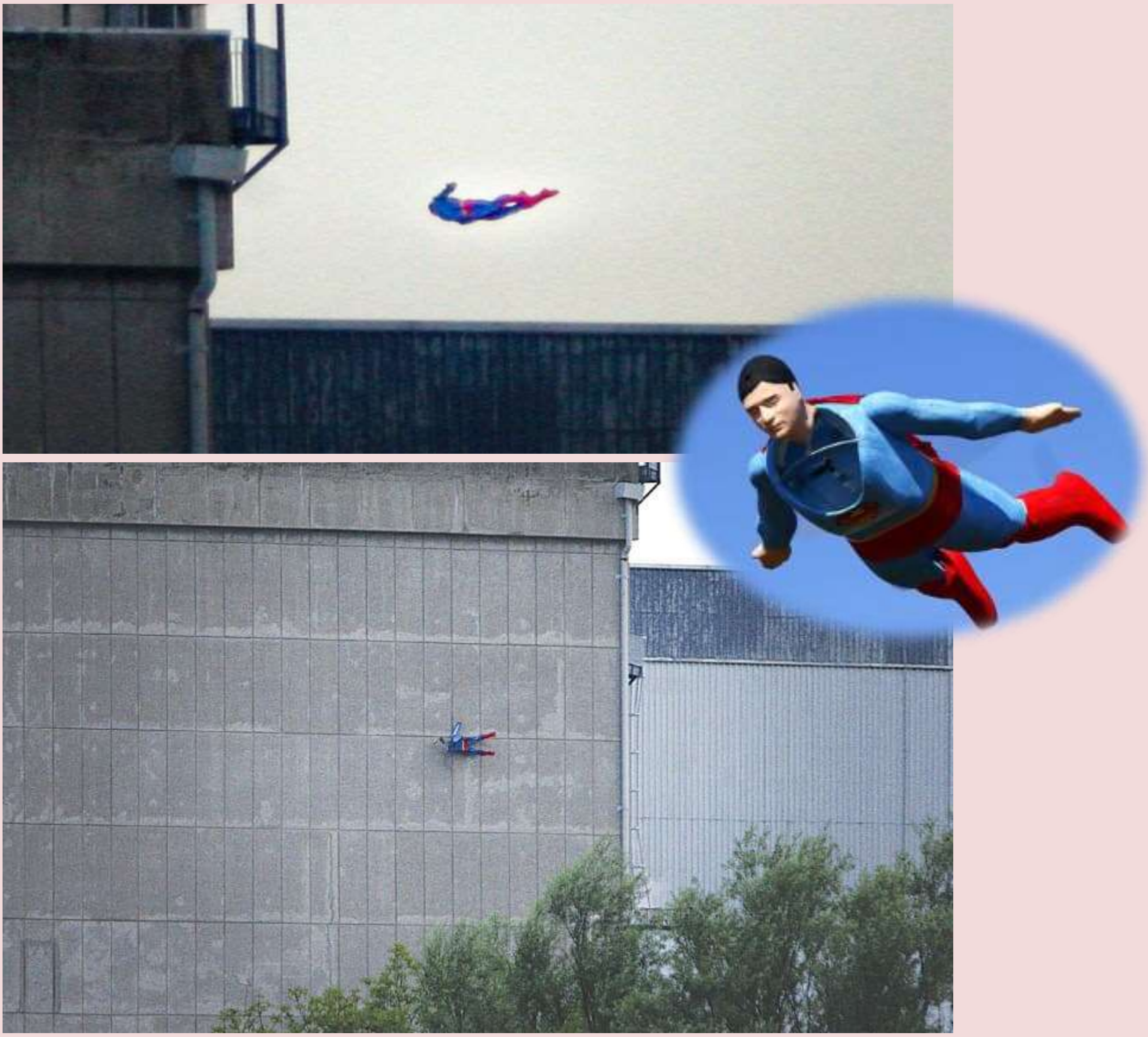
The bomb had a yield of 50 megatons of TNT (210 PJ). In theory, it would have had a maximum yield of 100 megatons if it had included a U-238 tamper, but because only one bomb was built, this was never demonstrated. The single bomb was detonated at the Sukhoy Nos Cape of Severny Island, part of Novaya Zemlya.

The remaining bomb casings are located at the Russian Atomic Weapon Museum in Sarov and the Museum of Nuclear Weapons, All-Russian Research Institute of Technical Physics, at Snezhinsk.

Greenpeace France crashes drone at French nuclear plant

Source: http://www.homelandsecuritynewswire.com/dr20180703-greenpeace-france-crashes-drone-at-french-nuclear-plant

July 03 – **Greenpeace France said Tuesday it had flown the drone – remotely piloted by one of its activists – over Bugey nuclear plant near Lyon, France. The pilot then crashed the Superman-shaped drone against the wall of the facility's spent-fuel pool building.**



"The action again highlights the extreme vulnerability of this type of buildings, which contain the highest amount of radioactivity in nuclear plants," Greenpeace said.

State-controlled EDF, which operates the plant, said that two drones had flown over the facility. French police intercepted one of them, it added.

"The presence of these drones had no impact on the security of the installations," EDF said in a statement, adding that it planned to file a police complaint against Greenpeace.

ABC News reports that the latest drone “attack” follows a series of similar stunts by Greenpeace. The group says it stages these stunts to expose the vulnerabilities of French nuclear plants.

In October last year, Greenpeace activists breached the perimeter security of EDF’s Cattenom nuclear plant, and then launched fireworks over the plant.

“Spent-fuel pools must be turned into bunkers in order to make nuclear plants safer,” said Yannick Rousselet, Greenpeace France’s chief anti-nuclear campaigner.

EDF insists the spent-fuel pool structures can withstand natural disasters and accidents.

Separately, a French parliamentary investigation into nuclear security is to due to be concluded this week, with a report presented to parliament on Thursday.

Several Greenpeace activities have been handed suspended jail sentences and fines since the beginning of the year for their anti-nuclear antics.

EDITOR’S COMMENT: Perhaps a small taste from a future aerial attack. They did it. Anybody can do it!

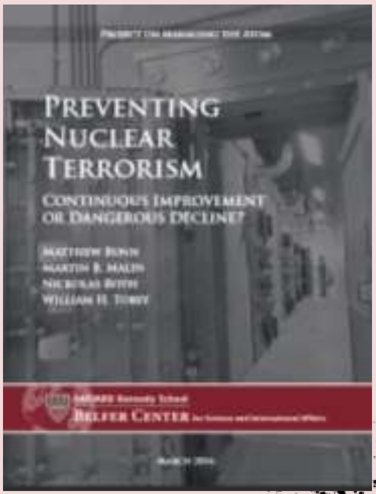
Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?

Authors: Matthew Bunn, William H. Tobey, Martin B. Malin, and Nickolas Roth

Source:https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf

March 2016 – World leaders face a stark choice at the final nuclear security summit later this month: Will they commit to continuous improvement, or will nuclear security efforts stall and potentially decline? Their answer will shape the chances that terrorist groups, including the Islamic State, could get their hands on the materials they need to build a crude nuclear bomb.

In this new report, *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?*, Matthew Bunn, Martin Malin, Nickolas Roth, and William Tobey provide a global reality check on nuclear security. They note that effective and sustainable nuclear security capable of addressing plausible threats is the single most effective chokepoint preventing terrorists from acquiring a nuclear weapon. In recent years, significant progress has been made securing vulnerable nuclear weapons-usable material—reducing



PROJECT ON MANAGING THE ATOM

PREVENTING NUCLEAR TERRORISM

CONTINUOUS IMPROVEMENT OR DANGEROUS DECLINE?

MATTHEW BUNN
MARTIN B. MALIN
NICKOLAS ROTH
WILLIAM H. TOBEY

HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

MARCH 2016

the number of countries with these materials by more than half, securing scores of sites around the world, and much more. But the work is not done.

Threats are constantly evolving, and there are new, worrying trends. Two years ago, the Islamic State was one of many small extremist groups. Today, it controls swaths of Iraq and Syria, is recruiting globally, has demonstrated a desire and capability to strike far beyond its borders, and espouses apocalyptic rhetoric.

Since the 2014 Nuclear Security Summit, there has only been modest progress securing vulnerable nuclear-weapons usable material around the globe, and some efforts have lost ground. At the end of 2014, Russia cut off most nuclear security cooperation with the United States. The Obama administration is proposing its lowest-ever budget for programs to improve nuclear security around the world. Fewer countries are announcing major security improvements at nuclear facilities, and some are hanging on to highly enriched uranium or plutonium stocks they clearly do not need. The nuclear security summit process is coming to an end—potentially decreasing international attention to this issue.

Matthew Bunn *is a Professor of Practice at Harvard University's John F. Kennedy School of Government. Before joining the Kennedy School, he served for three years as an adviser to the Office of Science and Technology Policy, where he played a major role in U.S. policies related to the control and disposition of weapons-usable nuclear materials in the United States and the former Soviet Union. He is the winner of the American Physical Society's Joseph A. Burton Forum Award for "outstanding contributions in helping to formulate policies to decrease the risks of theft of nuclear weapons and nuclear materials" and the Federation of American Scientists' Hans Bethe Award for "science in service to a more secure world," and is an elected Fellow of the American Association for the Advancement of Science. He is the author or co-author of over 20 books or major technical reports, and over a hundred articles in publications ranging from Science to The Washington Post.*

Martin B. Malin *is the Executive Director of the Project on Managing the Atom at Harvard's Belfer Center for Science and International Affairs. His research focuses on arms control and nonproliferation in the Middle East, U.S. nonproliferation and counter-proliferation strategies, and the security consequences of the growth and spread of nuclear energy. Prior to coming to the Kennedy School, Malin taught courses on international relations, American foreign policy, and Middle East politics at Columbia University and Rutgers University. He also served as Director of the Program on Science and Global Security at the American Academy of Arts and Sciences.*

Nickolas Roth *is a Research Associate at the Belfer Center's Project on Managing the Atom. Before coming to Harvard, he spent a decade working in Washington, D.C., where his work focused on improving government accountability and project management, arms control, and nonproliferation. Mr. Roth has written dozens of articles on nuclear security, nonproliferation, and arms control. His work has appeared in newspapers around the world. Roth is also a Research Fellow at the Center for International and Security Studies at the University of Maryland.*

William H. Tobey *is a Senior Fellow at the Belfer Center for Science and International Affairs at Harvard Kennedy School. He was most recently deputy administrator for Defense Nuclear Nonproliferation at the National Nuclear Security Administration. Mr. Tobey served on the National Security Council (NSC) staff in three administrations—Reagan, George H. W. Bush, and George W. Bush—working in defense policy, arms control, and counterproliferation positions. As director of counterproliferation strategy at the NSC, he oversaw development and implementation of U.S. policy on nuclear programs in Iran and North Korea, was a delegate to the Six Party Talks with North Korea, managed U.S. efforts to dismantle Libya's weapons of mass destruction programs, and authored the first draft of United Nations Security Council Resolution 1540. He has also served on the National Academies of Sciences, Engineering, and Medicine Committee on Improving the Assessment of Proliferation Risk of Nuclear Fuel Cycles.*

A management plan for hospitals and medical centers facing radiation incidents

By Fereshteh Davari and Arash Zahed

J Res Med Sci. 2015 Sep; 20(9): 871–878.

Source: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4696373/

Abstract

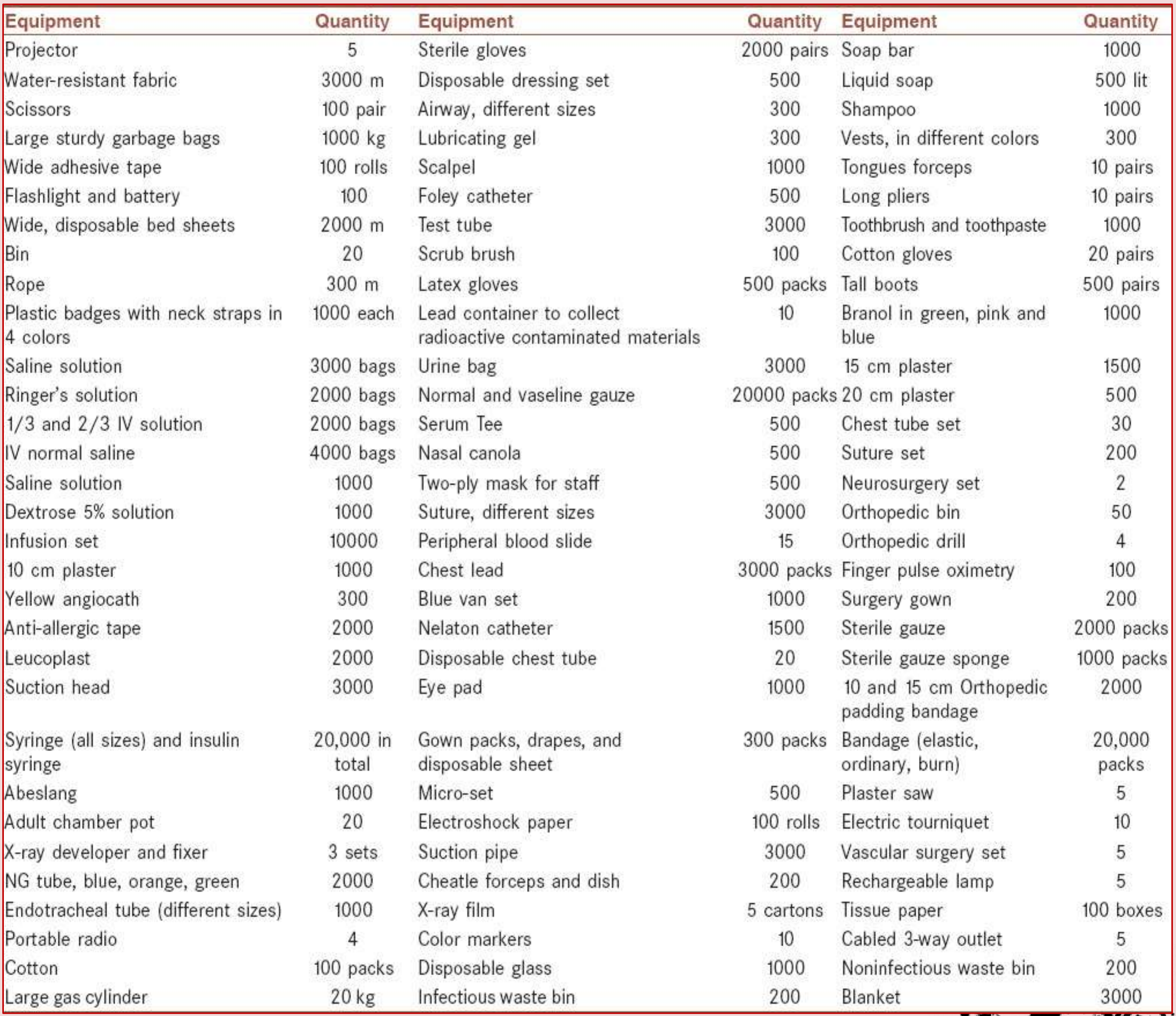
Background: Nowadays, application of nuclear technology in different industries has largely expanded worldwide. Proportionately, the risk of nuclear incidents and the resulting injuries have, therefore, increased in recent years. Preparedness is an important part of the crisis

management cycle; therefore efficient preplanning seems crucial to any crisis management plan. Equipped with facilities and experienced personnel, hospitals naturally engage with the response to disasters. The main purpose of our study was to present a practical management pattern for hospitals and medical centers in case they encounter a nuclear emergency.

Materials and Methods: In this descriptive qualitative study, data were collected through experimental observations, sources like Safety manuals released by the International Atomic Energy Agency and interviews with experts to gather their ideas along with Delphi method for polling, and brainstorming. In addition, the 45 experts were interviewed on three targeted using brainstorming and Delphi method.

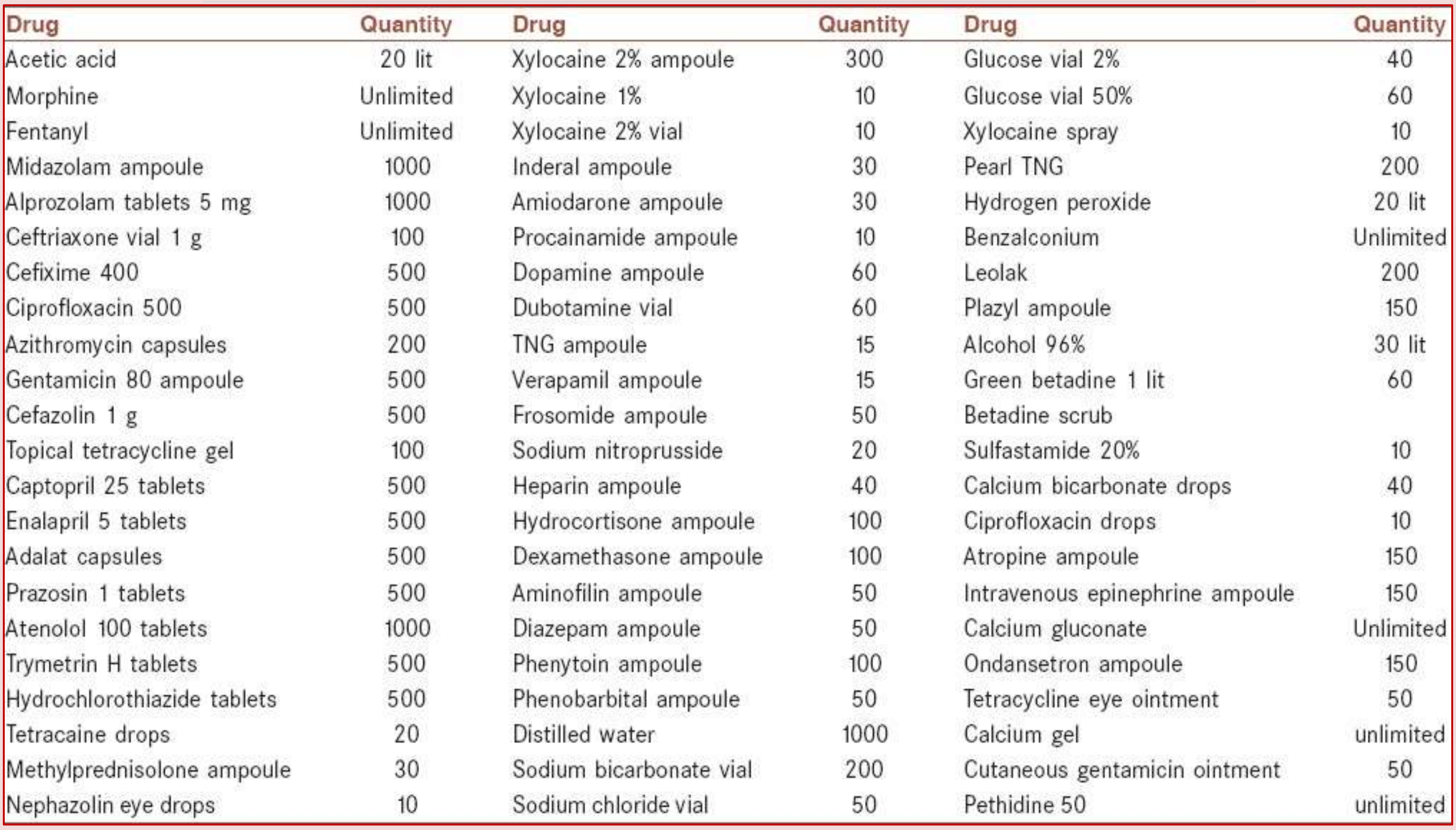
Results: We finally proposed a management plan along with a set of practicality standards for hospitals and medical centers to optimally respond to nuclear medical emergencies when a radiation incident happens nearby.

Conclusion: With respect to the great importance of preparedness against nuclear incidents adoption and regular practice of nuclear crisis management codes for hospitals and medical centers seems quite necessary.



Equipment	Quantity	Equipment	Quantity	Equipment	Quantity
Projector	5	Sterile gloves	2000 pairs	Soap bar	1000
Water-resistant fabric	3000 m	Disposable dressing set	500	Liquid soap	500 lit
Scissors	100 pair	Airway, different sizes	300	Shampoo	1000
Large sturdy garbage bags	1000 kg	Lubricating gel	300	Vests, in different colors	300
Wide adhesive tape	100 rolls	Scalpel	1000	Tongues forceps	10 pairs
Flashlight and battery	100	Foley catheter	500	Long pliers	10 pairs
Wide, disposable bed sheets	2000 m	Test tube	3000	Toothbrush and toothpaste	1000
Bin	20	Scrub brush	100	Cotton gloves	20 pairs
Rope	300 m	Latex gloves	500 packs	Tall boots	500 pairs
Plastic badges with neck straps in 4 colors	1000 each	Lead container to collect radioactive contaminated materials	10	Branol in green, pink and blue	1000
Saline solution	3000 bags	Urine bag	3000	15 cm plaster	1500
Ringer's solution	2000 bags	Normal and vaseline gauze	20000 packs	20 cm plaster	500
1/3 and 2/3 IV solution	2000 bags	Serum Tee	500	Chest tube set	30
IV normal saline	4000 bags	Nasal canola	500	Suture set	200
Saline solution	1000	Two-ply mask for staff	500	Neurosurgery set	2
Dextrose 5% solution	1000	Suture, different sizes	3000	Orthopedic bin	50
Infusion set	10000	Peripheral blood slide	15	Orthopedic drill	4
10 cm plaster	1000	Chest lead	3000 packs	Finger pulse oximetry	100
Yellow angiocath	300	Blue van set	1000	Surgery gown	200
Anti-allergic tape	2000	Nelaton catheter	1500	Sterile gauze	2000 packs
Leucoplast	2000	Disposable chest tube	20	Sterile gauze sponge	1000 packs
Suction head	3000	Eye pad	1000	10 and 15 cm Orthopedic padding bandage	2000
Syringe (all sizes) and insulin syringe	20,000 in total	Gown packs, drapes, and disposable sheet	300 packs	Bandage (elastic, ordinary, burn)	20,000 packs
Abeslang	1000	Micro-set	500	Plaster saw	5
Adult chamber pot	20	Electroshock paper	100 rolls	Electric tourniquet	10
X-ray developer and fixer	3 sets	Suction pipe	3000	Vascular surgery set	5
NG tube, blue, orange, green	2000	Cheatle forceps and dish	200	Rechargeable lamp	5
Endotracheal tube (different sizes)	1000	X-ray film	5 cartons	Tissue paper	100 boxes
Portable radio	4	Color markers	10	Cabled 3-way outlet	5
Cotton	100 packs	Disposable glass	1000	Noninfectious waste bin	200
Large gas cylinder	20 kg	Infectious waste bin	200	Blanket	3000

Required medical equipment for 1000 potential casualties



Drug	Quantity	Drug	Quantity	Drug	Quantity
Acetic acid	20 lit	Xylocaine 2% ampoule	300	Glucose vial 2%	40
Morphine	Unlimited	Xylocaine 1%	10	Glucose vial 50%	60
Fentanyl	Unlimited	Xylocaine 2% vial	10	Xylocaine spray	10
Midazolam ampoule	1000	Inderal ampoule	30	Pearl TNG	200
Alprozolam tablets 5 mg	1000	Amiodarone ampoule	30	Hydrogen peroxide	20 lit
Ceftriaxone vial 1 g	100	Procainamide ampoule	10	Benzalconium	Unlimited
Cefixime 400	500	Dopamine ampoule	60	Leolak	200
Ciprofloxacin 500	500	Dubotamine vial	60	Plazyl ampoule	150
Azithromycin capsules	200	TNG ampoule	15	Alcohol 96%	30 lit
Gentamicin 80 ampoule	500	Verapamil ampoule	15	Green betadine 1 lit	60
Cefazolin 1 g	500	Frosomide ampoule	50	Betadine scrub	
Topical tetracycline gel	100	Sodium nitroprusside	20	Sulfastamide 20%	10
Captopril 25 tablets	500	Heparin ampoule	40	Calcium bicarbonate drops	40
Enalapril 5 tablets	500	Hydrocortisone ampoule	100	Ciprofloxacin drops	10
Adalat capsules	500	Dexamethasone ampoule	100	Atropine ampoule	150
Prazosin 1 tablets	500	Aminofilin ampoule	50	Intravenous epinephrine ampoule	150
Atenolol 100 tablets	1000	Diazepam ampoule	50	Calcium gluconate	Unlimited
Trymetrin H tablets	500	Phenytoin ampoule	100	Ondansetron ampoule	150
Hydrochlorothiazide tablets	500	Phenobarbital ampoule	50	Tetracycline eye ointment	50
Tetracaine drops	20	Distilled water	1000	Calcium gel	unlimited
Methylprednisolone ampoule	30	Sodium bicarbonate vial	200	Cutaneous gentamicin ointment	50
Nephazolin eye drops	10	Sodium chloride vial	50	Pethidine 50	unlimited

Required medications in nuclear emergency center for 1000 potential casualties

Preparing for quick radiation diagnostic test in case of a nuclear disaster

Source: http://www.homelandsecuritynewswire.com/dr20180713-preparing-for-quick-radiation-diagnostic-test-in-case-of-a-nuclear-disaster

July 13 – Researchers at the University of Arizona College of Medicine – Phoenix are attempting to create a better diagnostic test for radiation exposure that potentially could save thousands of lives.
Jerome Lacombe, an assistant professor and researcher at the UA Center for Applied NanoBioscience and Medicine, recently published a study in *PLOS ONE*.
His study compiled a list of genes reported to be affected by external ionizing radiation (IR), and assessed their performance as possible biomarkers that could be used to calculate the amount of radiation absorbed by the human body.
"In the case of a nuclear event, a lot of people can be radiated," Dr. Lacombe said. "That is why it's so important that we can quickly and accurately assess the absorbed radiation so we can give patients the proper medical treatment as fast as possible."
Lacombe hopes to develop a radiation test that is less labor intensive and takes only two days for results. "If you have thousands of people and only two days to screen everyone, it would be almost impossible to do this with the current exposure test," Lacombe said. "With immediate care and the right diagnostics, people could have a better chance of survival."
Arizona says that Lacombe, who worked with researchers from Columbia University Medical Center and Texas A&M Engineering Experiment Station, analyzed published studies from 1978 through 2017 that identified **more than 10,000 unique responsive genes in human blood after external IR.**
Although many studies have tried to correlate gene expression after radiation exposure, their sample sizes have been small because of expense and the time it takes to test the genes.
By combining **24 studies**, Dr. Lacombe and his team investigated a large data set using a

standardized data extraction method and various statistical algorithms to find a list of robust candidate biomarkers.

This marks the first time a team has combined all these biomarkers and attempted to run a diagnostic assay to determine radiation exposure, Lacombe said.

“There is no validated signature for biodosimetry (the measurement of biological response for radiation dose),” Lacombe said. “There is no validated gene signature to assess the radiation

dose. We hope this paper can begin to identify these biomarkers and confirm genes that are radiation responsive.”

Arizona says that the UA Center for Applied NanoBioscience and Medicine is on the forefront of developing radiation treatment and diagnostics. In collaboration with Columbia University, the Translational Genomics Research Institute (TGen) and Georgetown University, the center has been co-sponsored by the National Institute of Allergy and Infectious Diseases for fourteen years. The partnerships have resulted in leading the development of gene expression-based biodosimetry technology platforms sponsored by several contracts with the Biomedical Advanced Research and Development Authority (BARDA).

The center has expanded its areas of research applications in radiation biology, including:

- ***Radio-sensitizing drugs:*** Oncologists may be able to prescribe a cancer patient a drug that could enhance the effect of radiation on their tumor. The lab investigates natural compounds found in plants that show promise in halting the growth of cancer cells.
- ***Radiotherapy treatments:*** The lab is looking into the effects of a high single radiation dose versus the same dose delivered in several fractions. Now, patients being treated for breast cancer usually receive about 30 fractions of two-grade doses. With improvements in technology, clinicians try to limit the number of fractions and therefore increase the radiation dose for each of them.
- ***Human organ-on-a-chip and microbiomes:*** Scientists are attempting to investigate radiation response through various novel devices, such as the “gut-on-a-chip.” This technology allows researchers to analyze the complex interactions between human cells and microbial ecosystems, predicting the effect of space radiation on the human gut during long missions beyond low Earth orbit.
- ***Engineered tissue models:*** The lab is developing a plant-based platform that provides cellulose scaffolds by treating leaves with detergents to remove all traces of plant cells, DNA and proteins. The resulting scaffold then is used as a 3D matrix and repopulated with various human cells to create a vascularized cancer tumor model so the role of the microenvironment in tumor radiation response can be investigated.

— Read more in Jerome Lacombe et al., “Candidate gene biodosimetry markers of exposure to external ionizing radiation in human blood: A systematic review,” PLOS ONE 13, no. 6 (7 June 2018).

Why Is Israel Simulating Attacks on Its Own Nuclear Reactors?

Source: https://nationalinterest.org/blog/buzz/why-israel-simulating-attacks-its-own-nuclear-reactors-25107

July 05 – Israel’s nuclear establishment has been conducting drills simulating attacks against the country’s two nuclear reactors.

“The Israel Atomic Energy Commission has been taking numerous steps to protect the nuclear reactors in Dimona and Nahal Sorek in light of assessments that Iran and Hezbollah see the reactors as preferred targets for missile attacks,” the left-leaning Israeli daily, Haaretz, reported on June 28 .

The **Nahal Sorek reactor** is a small research reactor America supplied to Israel as part of the Atoms of Peace program. The **Dimona reactor** is a much larger reactor that Israel used to produce plutonium for its nuclear weapons program. The Dimona reactor is still operating, although it’s unclear if it is making plutonium. It is **widely believed that Israel uses Dimona to produce tritium** for boosted atomic weapons .

According to the Haaretz article, members of the Israel Atomic Energy Commission (IAEC) believe that **a missile attack is the greatest danger to the reactors today.**

The report added that “recently the IAEC held a large training exercise that simulated a missile attack on one of the reactors, and included the evacuation of employees and actions to prevent a leak of radioactive materials.”

This threat is hardly imaginary, as Hezbollah leader Hassan Nasrallah has repeatedly threatened to attack Israel’s nuclear reactors as well as its chemical supplies.

“**I call on Israel not only to empty the ammonia tank in Haifa, but also to dismantle the nuclear reactor in Dimona.** Our military capabilities will strike Israel and its settlements,” Nasrallah said in February of last year.

He added: “In Israel, they know that Hezbollah has the possibility of reaching the nuclear reactor, which is antiquated, and it doesn’t require major force to hit.”

In 2016, Nasrallah called for targeting the ammonia stockpiles in Haifa Hezbollah’s “nuclear bomb” option.

IAEC members downplayed the actual dangers of an attack on one of Israel’s reactors. According to Haaretz, the IAEC believes that even if a missile hit one of the reactors the employees inside would be safe.

What the commission does fear is that the attack would be extremely useful for propaganda purposes. Indeed, Dimona has long served as a potent symbol of Israeli power ever since Israel’s founding father David Ben-Gurion purchased it from France.

The IAEC is also concerned that an attack against Israel’s reactors would spark panic among the Israeli public, similar to how some observers worry that the use of a dirty bomb in a crowded city would be a “weapon of mass disruption.”

The IAEC’s assessment might be overly optimistic, however. As Haartez’s notes, last year four Israeli scientists— including Irad Brandys, an engineer at the Dimona reactor— published an article estimating the damage caused by a Scud missile attack on a nuclear reactor similar to the ones that Israel operates. **They concluded that “the monitor and control equipment can resist the in-structure shock both in the horizontal and vertical directions when the missile explodes beyond 35 m.”**

However, missiles that landed closer to the reactor could cause various types of damage, including (in Haaretz’s description) “a breach of the reactor’s protective envelope, which could lead to a leak of radioactive gas, as well as a disruption to critical systems, most importantly the reactor’s cooling system.”

The loss of electricity powering the cooling systems of some of Japan’s reactors was at the heart of the Fukushima nuclear disaster in 2011.

Of course, most missiles are not anywhere near accurate enough to hit a target within 35 meters, at least with any sort of consistency.

Arguably Iran's most advanced missile is the Emad, which has a maneuverable re-entry vehicle (MaRV). MaRVs allow the missile's warhead to maneuver late in flight both to evade missile defenses and achieve pinpoint accuracy.

But Iran's Emad missile is believed to have an accuracy (technically a circular error probable) of **five hundred meters.** That means that fifty percent of the time it would land within five hundred meters of the target. Thus, even if Iran gave Emad missiles to Hezbollah, the Lebanese group would have to get extremely lucky to have one of them land within thirty-five meters of one of Israel's reactors.

Still, the IAEC's concerns highlight an underappreciated cost of nuclear reactors—the need to protect them, not just from terrorist groups but also from nation states. Of course, Israel itself has illustrated this challenge in the past when it bombed both an Iraqi and Syrian reactor before they were operational. This concern is especially warranted as more countries in the region begin building nuclear reactors.

Israel has also worried about the vulnerability of its Dimona reactor before. In fact, according to Avner Cohen—who has written extensively about the Israeli nuclear program—concerns that Egypt was preparing to attack Israel's nuclear reactor was one factor that prompted the Jewish state to launch a preemptive attack in the Six Day War.

"Dimona was on the minds of Israeli leaders, especially Prime Minister [Levi] Eshkol, almost from the beginning of the crisis," Cohen stated in his book Israel and the Bomb.

Egyptian President Gamal Abdul Nasser had threatened to attack Dimona a number of times during the 1960s. Then, Egyptian aircraft made a number of reconnaissance flights over Dimona in the days leading up to the war. And, as Cohen writes , "After the war it was discovered that the two Israeli nuclear research centers, at Dimona and Nachal Soreq, were high-priority targets in Egyptian war plans."

Fears about the vulnerability of Israel and other countries' nuclear reactors are likely to grow in the coming years and decades. Although Iran's missiles cannot realistically threaten Israel's nuclear reactors at the moment, the real question is how long will that continue to be the case? It wasn't long ago that a country like China didn't have guided missiles. Now, it is believed that Beijing has missiles that can threaten moving targets like U.S. aircraft carriers at long distances. And history has consistently shown that technology—including missiles—inevitably spreads.

Scavenger hunt for simulated nuclear materials

Source: http://www.homelandsecuritynewswire.com/dr20180716-scavenger-hunt-for-simulated-nuclear-materials

July 16 – Competing in a fictitious high-stakes scenario, a group of scientists at the Department of Energy's Lawrence Berkeley National Laboratory (Berkeley Lab) bested two dozen other teams in a months-long, data-driven scavenger hunt for simulated radioactive materials in a virtual urban environment.

The goal of this hackathon-styled event was both to improve the detection methods that could be applied to actual threats involving nuclear materials, and to create a platform to virtually vet out these methods. The computer-programming challenge ran from 22 January to 14 May and featured 66 researchers on 25 teams based at DOE national laboratories and other U.S. government research labs. The teams received data that simulated radiation sources scanned by a vehicle-mounted detector system traveling along urban streets.

Teams were scored on the success of the algorithm or algorithms they developed in sleuthing the time slots marking the detection of the simulated radioactive hotspots likely associated with potentially hazardous nuclear materials – and in ruling out common sources of radiation. Government agencies have previously conducted many field tests and performed comparisons to study how to find radioactive materials in different settings, but this was the first online competition.

LBL says that Tenzing Joshi, an applied nuclear physicist in Berkeley Lab's Nuclear Science Division, led the winning team in this Urban Radiological Search Competition created by the DOE's National Nuclear Security Administration. His teammates included Mark Bandstra, a senior scientific engineering associate, and UC Berkeley graduate student Kyle Bilton.

Berkeley Lab served as the host institution for the competition, which was also administered by Los Alamos National Laboratory and Oak Ridge National Laboratory. A group of researchers in Berkeley Lab's Computational Research, Nuclear Science, and Information

Technology divisions teamed with other researchers in the Nuclear Science Division to develop the competition platform.

Berkeley Lab organizers leveraged the Lab's capabilities in support of big data science to develop and roll out the competition platform, and they hope it can be used in other data analytics challenges. The Lab's Applied Nuclear Physics program has been developing a variety of mobile and portable detector systems to quickly identify radiation sources.

"We had a pretty healthy lead on the public scoreboard, but it turned out to be incredibly close," said Joshi. The Berkeley Lab team had submitted about 204 entries over the course of the competition, and their final submission – which they sent in the final 20 minutes of the competition – put them ahead of the second-place team by just 1.3 points.

"It was down to the wire," said Brian Quiter, an applied nuclear physicist in Berkeley Lab's Nuclear Science Division who managed the competition and led the development of the platform with Shreyas Cholia, who heads up a software systems group in Berkeley Lab's Computational Research Division.

Statistical sciences teams from Los Alamos and Lawrence Livermore national labs placed second and third in the competition, respectively.

The competition data was divided into public and private sets, and competitors did not know which was grouped into each category. For the public scoring, rankings were instantly updated for the public portion of the data sets. Meanwhile, participants' submissions covered by the private data set were scored only at the completion of the competition.

By separating the data into public and private sets and in limiting the number of algorithm submissions per team to 1,000, the competition was designed to prevent teams from "gaming" the competition. For example, if there was no cap on submissions one team might gain an advantage by submitting a huge volume of slightly varied algorithms until one of them, by chance, earns a top ranking. No team neared the submission limit, and by the end of the competition the teams had sent a total of 1,024 submissions.

"The teams were graded on false positives – whether they reported environmental 'background' radiation as human-made sources, for example – and also on the likelihood of detecting the sought-after radiation sources, the precision in time at which a particular source was reported, and on whether they could specifically identify a particular type of radioactive source based on a list of six possible sources, from weapons-grade plutonium to materials used for nuclear medicine," Quiter said.

To further complicate the challenge, there was no GPS or location-based information to inform participants about the layout of buildings, for example, and participants also had very limited information about the speed of the vehicle and the length of each of the paths traveled. The virtual streetscape used in the challenge was loosely based real streets, and the travel time of the detector along each path in the simulated data sets varied from 45 seconds to just over 12 minutes.

"We were told that the speeds were variable, from 1 to 13 meters per second," Joshi said. "We were also told that the radiation sources could be shielded in certain situations, which changes the energy spectrum that you can measure. How you handled that in the algorithm was an important part of doing well."

Joshi said that members of his team had already been working on similar algorithms prior to the challenge. "We have been building this capability up over the last year," he said. "We have collected a lot of data from radiological measurements in urban areas and have been investigating the relationships between these measurements and the radiological compositions of our surroundings."

While teams were not limited to using a single algorithm, Joshi said that ultimately the team developed one algorithm – they named it Berkeley Anomaly Detection – Factorized Matrices, or BAD-FM – to handle most of the data, with some refinements toward handling particular phenomena such as different speeds of the vehicle within the simulations.

The model was informed by data for naturally occurring radiation – which can vary based on local geography and building materials, for example, and can fluctuate over time even at the same location – as well as data from test sources of human-made nuclear materials.

Joshi said that the computing power of his desktop computer was adequate for initial prototyping of the algorithm; for the more advanced work, the team used a single node of a Lab supercomputer. They used visualization tools, which color-coded the simulated radiation sources based on the detector's energy readings, to help interpret and analyze the data.

The top three teams in the competition – with the second- and third-place teams composed of data scientists from Los Alamos and Lawrence Livermore national labs, respectively, will be recognized at a July 11 meeting and will receive follow-up funding, Quiter noted. There will also likely be a public competition.

“The next big plan is to repeat this challenge on an established open platform where we can ideally tap into a large community of data scientists,” Quiter said.

Reports detail Israeli raid on Iran's nuclear documents

Source: http://www.homelandsecuritynewswire.com/dr20180716-reports-detail-israeli-raid-on-irans-nuclear-documents

July 16 – Israel has revealed new details of how its spy agency smuggled out nuclear documents from Iran earlier this year, although the material does not appear to provide evidence that Iran failed to fulfill its commitments under the 2015 nuclear agreement with world powers.

The information reported by the *New York Times* and the *Washington Post* on 15 July shed more light on the Mossad operation in January but offered few other details beyond what Prime Minister Benjamin Netanyahu claimed in April when he announced the results of the raid.

Netanyahu claimed Israeli intelligence seized 55,000 pages of documents and 183 CDs on Iran’s disputed nuclear program dating back to 2003. Iran maintains the entire collection is fraudulent.

After his announcement in late April, the Israeli leader gave President Donald Trump a briefing at the White House and argued it was another reason Trump should abandon the 2015 nuclear deal.

In May, Trump withdrew from the deal.

Tehran has always claimed its nuclear program was only for peaceful purposes.

The *New York Times* reported on 15 July that Mossad agents had six hours and 29 minutes to break into a nuclear facility in the Iranian capital, Tehran, before the guards arrived in the morning.

In that time, they infiltrated the facility, disabled alarms, and unlocked safes to extract the secret documents before leaving undetected.

Better decisions during a radiological emergency

Source: http://www.homelandsecuritynewswire.com/dr20180720-better-decisions-during-a-radiological-emergency

July 20 – The Fukushima Daiichi nuclear power plant accident on 11 March 2011 resulted in public misconception that radioactive fallout would impact the west coast of the United States. State and local emergency managers did not have an effective way to communicate or project the effects, which led to disparate reporting and conflicting messages conveyed by the media.

The Federal Emergency Management Agency (FEMA) identified the need for a systematic platform where technically accurate and decision-making information could be easily shared across state, municipal and tribal jurisdictions. They contacted the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) – DHS’s research and development arm – for assistance.

S&T says that that partnership has grown beneficially for both organizations and generated numerous success stories. Since 2015, S&T’s National Urban Security Technology Laboratory (NUSTL), a testing and evaluation laboratory with a first responder focus located in New York City, has worked with RadResponder, a multi-function online network for emergency managers, first responders and radiation subject matter experts.

RadResponder is identified in the 2016 Nuclear Radiological Incident Annex as the national system for radiation data aggregation and is considered the standard resource for giving emergency managers a common operating picture, whether planning for the future or monitoring radiation in real time. Groups and individuals involved in radiation response can request to create an online account and become part of this network, which currently includes thousands of organizations and individual first responders.

“RadResponder builds capabilities for state and local response and connects them with federal assets from FEMA, the Environmental Protection Agency (EPA) and the Department of Energy (DOE),” said Ben Stevenson, an S&T Program Manager located at NUSTL.

While FEMA owns RadResponder, S&T, EPA and DOE have supported the development of some tools within the network. In January 2018, FEMA adopted the Radiation Decontamination tool (Rad Decon), developed by S&T and the EPA, into the system. Its developers refer to it as a "discussion support" tool meant to provide executive decision makers and subject matter experts a common information source to draw from in disaster preparation.

Even more recently, RadResponder added the Radiological Operations Support Specialist (ROSS) toolkit, an S&T-funded HTML tool that organizes important reference material for radiation specialists, to support subject matter experts in their analyses.

"RadResponder is constantly evolving," said James Blais, FEMA's RadResponder Program Manager, "S&T has been very active lately, helping with ROSS and Rad Decon, to spot needs and provide insight and perspective slightly different than what we had."

A thriving network

RadResponder consolidates information from all levels of government to benefit operations. In the past, local emergency response plans have been made independent of other agencies and governmental elements, with varying methods and effectiveness. Now, with radiation data federated on RadResponder, state and local governments are given a uniform, constantly updated set of tools to build their approach. The common platform allows several entities to communicate with each other where they might not otherwise.

"Some people use it to build relationships with other organizations," said Blais. "It's like [a social network] for the radiation community."

RadResponder is gradually becoming a more holistic radiological emergency network. It continues to grow rapidly as more response agencies join and new tools are added. Organizations have been eager to join—Michigan has adopted RadResponder state-wide, and Iowa and Kansas use it to track background radiation. These organizations benefit from the different tools in the network, which are updated constantly.

"We want to help communities at large become more resilient instead of reinventing the wheel at every turn," said Blais.

A "discussion support" tool

S&T says that whether a catastrophe is natural or man-made, emergency managers need to respond quickly with the optimal solution. Making decisions on the fly can be difficult, which is why significant planning must go into a disaster response strategy. Many conversations need to happen, and they need to cover a range of possible scenarios. The Rad Decon tool was developed to facilitate those very discussions.

While some executive decisions can be supported by a straightforward decision tree, there are other problems—in this case, large scale radiological incidents—for which the solution depends on more nuanced factors. This is where the "discussion support" (as opposed to "decision support") distinction comes into play. Radiological emergencies could require a different response depending on the type of radiation, the landscape or the time of year. The Rad Decon tool guides users through a continuum of parameters and priorities they can set based on the conditions of a specific radiological event to prioritize decontamination strategies. The tool uses this data to provide a list of possible solutions that gives a common point of reference to guide the emergency management conversation. The application even allows for printable results to aid the discussion.

"The Rad Decon tool is designed to take you from all your options to a couple key options," said Stevenson, "We want responders to have the ability to collect data and make decisions quickly and more efficiently."

The tool was inspired in 2013 by a decision-making model used in the United Kingdom. S&T and the EPA worked together to establish the needs the tool should fulfill, and they were then able to put together the pieces to fully transition it to the FEMA-hosted network.

The ROSS toolkit was implemented in May 2018, providing an infrastructure to better integrate subject matter experts from the ROSS program, a position in the emergency management structure that can provide radiological expertise to incident commanders and emergency managers. The toolkit provides a ROSS with a streamlined analysis capability, aiming to further improve the quality of information provided to first responders around the country—in this sense, the entirety of RadResponder serves as "discussion support," promoting dialogue between organizations, leveraging the strengths of their experts and executives.

More than a toolbox

The RadResponder network provides a host of other tools for emergency managers to keep informed. There are videos, repositories of past drills and exercises, training information, factsheets, manuals and more.

Exercises are catalogued in several different ways, using dashboards with charts, graphs and even interactive maps to provide insight for the future. Users can search for past events and view this information in any one of these interactive forms. They can also filter activity down to their own organization to stay updated on their own events, equipment, facilities and personnel.

Radiological response teams around the country have joined RadResponder, able to connect their radiological detection hardware—computers, meters, samplers, etc.—to the network to perform experiments and store data in real time. The network can connect to detectors through Bluetooth equipment, a mobile app or, simply, a radio. State and local governments have used the network to test, plan and train their radiological response teams. RadResponder is also integrated into the Radiological Dispersal Device (RDD) Guidance, providing a science-based tool for responding in the First 100 minutes of an RDD detonation, recently released by DHS S&T, FEMA and DOE NNSA.

Another recent addition to the network was the ability to merge data from different events together—an example of how RadResponder helps give experts a unified picture of radiological response across agencies. The network also recently made the mobile app accessible to a wider range of smartphones, which will allow more robust communication, more data shared between and within organizations in their planning and research.

National impact

S&T says that the teams behind RadResponder want to consolidate information as much as possible to allow emergency managers easy access to a shared radiation emergency response resource. Future capabilities will include a two-way chat function (accessible through the RadResponder site and the mobile app), an alert system for teams to immediately have awareness when radiation has reached a certain threshold, and the ability to receive data from drones connected to the network.

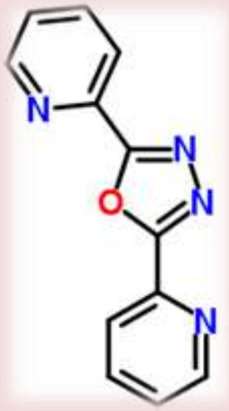
More operational tools will promote a faster, more informed radiological response nationwide, as Ben Stevenson said: “A radiological emergency is an event of national significance.” Certainly, local preparedness is an excellent first step to reducing the long-term impact of an incident by preparing responders to manage information and make data driven protective action decisions.

EXPLOSIVE NEWS

Replacing TNT with less toxic explosive

Source: http://www.homelandsecuritynewswire.com/dr20180626-replacing-tnt-with-less-toxic-explosive

June 26 – Scientists at Los Alamos National Laboratory and the U.S. Army Research Laboratory in Aberdeen, Maryland have developed a novel "melt-cast" explosive material that could be a suitable replacement for Trinitrotoluene, more commonly known as TNT.



"The Army and the Laboratory, through the Joint Munitions Program, have been looking for a TNT replacement," said David Chavez, an explosives chemist at Los Alamos. "Something with non- or low-toxicity that has the right melting point so it can be liquified and cast, for use in a variety of munitions."

The new molecule is a nitrogen-containing compound called **bis-oxadiazole**.

Chavez has been developing high-nitrogen explosive compounds for decades at Los Alamos, with particular emphasis on low explosive sensitivity and good environmental properties.

"One major challenge was coming up with a formula that would significantly surpass the explosive energy of TNT, but still have melt-casting capability" said Chavez. "When designing a molecule to be melt-castable, yet high performing, you typically encounter many challenges due to numerous obstacles."

LANL notes that one of the biggest challenges was getting a high enough yield of the material out of the synthesis process. An early procedure produced only a 4 percent yield, far too low to be practical and affordable. After several iterations of the process the scientists boosted the yield to 44 percent.

Working with Jesse Sabatini and colleagues at Aberdeen, they developed a 24-atom molecule that's packed with nitrogen, and has increased performance 1.5 times greater than TNT. The full chemical name is bis(1,2,4-oxadiazole)bis(methylene)dinitrate.

Research will continue with production of the material on a kilogram scale, a battery of explosive testing as well as future toxicity studies.

The Environmental Protection Agency has listed **TNT as a possible carcinogen**, and exposure to the material has been linked to disorders of the blood, such as anemia, and abnormal liver function, according to the Centers for Disease Control. TNT was first prepared in 1863 by German chemist Julius Wilbrand but its full potential as an explosive wasn't discovered until 1891. **TNT has been in use as a munitions explosive since 1902.**

— Read more in Eric C. Johnson et al., "Bis(1,2,4-oxadiazole)bis(methylene) Dinitrate: A High-Energy Melt-Castable Explosive and Energetic Propellant Plasticizing Ingredient," Organic Process Research & Development 22, no. 6 (25 May 2018).

The past, present and future of bomb disposal robots

Source: https://www.governmenteuropa.eu/bomb-disposal-robots/88618/

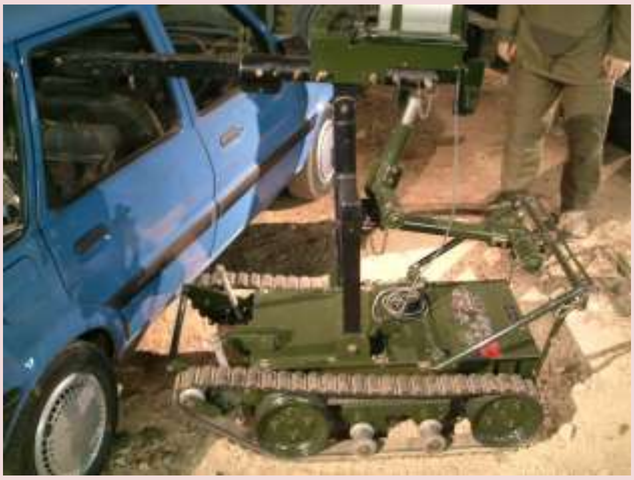
June 20 – Bomb disposal robots have come a long way since the introduction of the Wheelbarrow in 1972, as *Government Europa* explores.

An REME corporal repairing a Dragon Runner EOD variant © Crown 2012

Of all the roles in the British Army, one of the most dangerous is that of the ammunition technical officer, who has the daunting task of dismantling, defusing and disposing bombs and other explosive ordnance, often in the most hostile and c hallenging of environments. Making this job safer (if far from risk-free) are bomb disposal robots, unmanned vehicles capable of disabling explosive devices without endangering human lives. In this article, *Government Europa* chronicles the past, present and future use of this innovative, life-saving technology in the British Army.

The Wheelbarrow

Bomb disposal robots were first invented by Peter Miller, a retired lieutenant-colonel of the British Army who conceived the idea after eight ammunition technical officers of the Royal Army Ordnance Corps lost their lives to improvised explosive devices (IEDs) during the conflict in Northern Ireland in 1971-2.

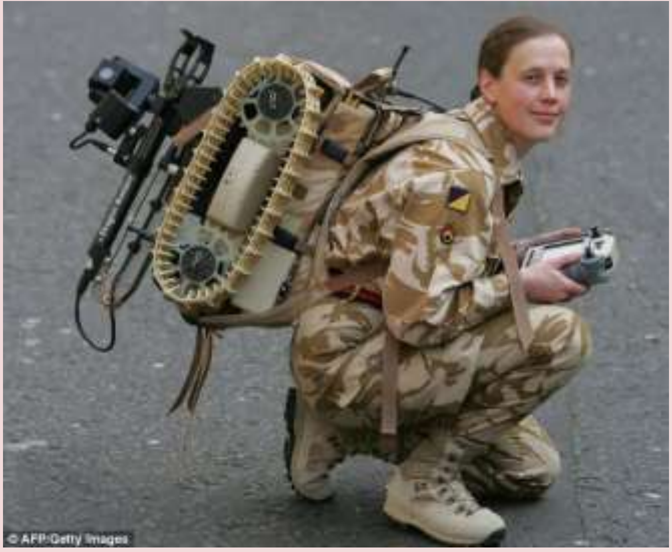


Based on a modification Miller had made to his lawnmower, the 'Wheelbarrow' was assembled out of the chassis of an electrically powered wheelbarrow, a remote-control device, and a spring-loaded hook that could be attached to and used to tow a car. This allowed suspect devices to be safely removed from a scene and bombs or explosives to be detonated where they would not endanger any civilians or military personnel. The later addition of Major Robert John Wilson Patterson's so-called 'Pigstick', a water jet disruptor, enabled it to successfully defuse bombs rather than just transport them.

Since its introduction in 1972, the Wheelbarrow has been through countless revisions, saved hundreds of military and civilian lives, and been destroyed more than 400 times while in operation. But, as technology progresses and the threats facing the armed forces evolve, new, more advanced bomb disposal robots have come forward, offering even greater protection to service personnel on the front line.

Dragon Runner

One such example is Dragon Runner, a lightweight reconnaissance robot developed by scientists at the Robotics Institute of Carnegie Melon University (CMU), USA. Originally weighing in at just 20lb, Dragon Runner was developed, according to CMU, as a 'low-cost rugged alternative to overly heavy, bulky, slow and costly robotic scouts already on the market' and is light enough that it can be carried around in a specially designed backpack and even thrown out of windows, over fences or from moving vehicles. Later upgrades boast an even lighter design and enable Dragon Runner to open doors and climb stairs.



The innovative multi-terrain robot also features high-speed capabilities, is easy to manoeuvre, and can dig around, pick up and even move objects thanks to its manipulator arm. The easy-to-use system requires little formal operator training and can be deployed in under three seconds. Dragon Runner is also able to place small charges in order to disrupt suspect items and can operate in the dark with the aid of onboard infrared capabilities.

Dragon Runner was acquired by the British Army as part of its urgent operational requirements in support of explosive ordnance disposal (EOD) activity in Afghanistan in 2009 and is used to help identify and deactivate IEDs.

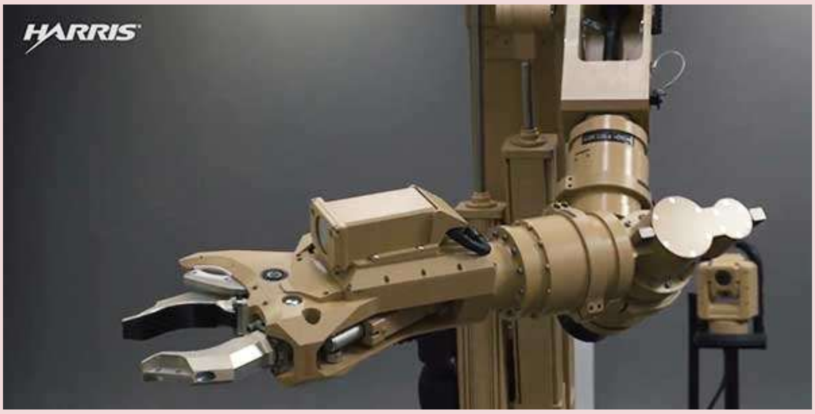
The Harris T7

More recently, in September, then defence secretary Sir Michael Fallon announced a £55m (~€63m) contract for 56 innovative bomb disposal robots for use by the British Army. The T7 robots, which will be purchased from US robotics manufacturer Harris under the Ministry of Defence's Project Starter, will be used to support UK EOD missions across the globe, and will also assist with hazardous materials (HAZMAT) clean-up, intelligence, surveillance and reconnaissance (ISR), and special weapons and tactics missions.

"With our rising defence budget, we are investing in the latest equipment for our Armed Forces to tackle the growing threats we face," Sir Michael said. "These state-of-the-art bomb disposal robots will be powerful and reliable companions to our troops on the battlefield, keeping them safe so they can help keep us safe."

The T7 robots' many features include:

- High-definition cameras;
- High-speed datalinks;
- An adjustable manipulation arm; and
- A track system specially designed to cope with rough terrain.



A haptic feedback function provides operators with human-like dexterity, while an intuitive control interface ensures ease of use as well as offering a high degree of command and control. Operators will even be able to disable and defeat IEDs planted in vehicles thanks to various attachments that allow for the use of standard-issue sensors, disruptors and tools.

Together, these features are expected to help improve mission effectiveness and shorten the time it takes to complete a task.

"This award will bring life-saving technology to UK forces in the field and reaffirms the importance of highly reliable, precise and easy-to-use robotic systems for EOD operators," said Harris Electronic Systems president Ed Zoiss. "During Project Starter's assessment trials in 2016, T7 successfully demonstrated to the UK MoD the manoeuvrability, reliability, and capability required for the toughest EOD missions."

All 56 of the bomb disposal robots are expected to be delivered to the UK and in service by December 2020. They will replace the current Wheelbarrow Mk8b robots, which have been in service since 1995, and will be supported by engineers at Harris EDO MBM Technology in Brighton, where the contract is anticipated to sustain ten highly skilled jobs.

EOD is a complex and demanding task, but thanks to ever-more advanced technologies like the Wheelbarrow, Dragon Runner and T7 Harris bomb disposal robots, it has also become a far safer one, too.

The swimming pool clue: how Islamic State's worst bloodshed in Europe could have been avoided

Source: https://emmejihad.wordpress.com/tag/tatp/

June 11 – A car theft in the Netherlands, a seemingly insignificant note that was found in Molenbeek, and a shop for swimming pool equipment in the North of France. These are the three ingredients of the best clue there ever has been to thwart the Paris and Brussels attacks — a new investigation by the Belgian newspaper Het Laatste Nieuws **reveals**.

Bayroshock, a product against algae used in swimming pools

A lot has been written already about the clues that security services missed in the run-up to the Paris and Brussels attacks — clues that could have prevented the bloodshed by Islamic State. Could have. In hindsight, it is easy to list the mistakes. Yes, it was known to the police that Salah Abdeslam had started to radicalize. But at that time, it was the case with tens, if not hundreds of Belgian Muslims like him. And yes, only 22 days before the Paris attacks, a search took place in the house of Khalid El Bakraoui because he tried to obtain kalashnikov chargers. But he was known as a gangster and in the end no weapons were found.

Bayroshock without chlorine

About one clue, however, nothing has been published yet — and that clue is likely the very best chance authorities missed to detect the terrorist cell. It started with the theft of a car in a small village between the Dutch rivers Maas and Waal. It was a silver colored Audi S4 built in 2003 that disappeared in the night from August 10 to 11, 2015 at a parking lot in Rijswijk — part of the municipality of Woudrichem and not to be confused with the much bigger town of Rijswijk near The Hague. "Klerelijers", a friend of the owner reacted at a notice on Facebook, using an equivalent for "assholes" that is endemic for the Netherlands — while another one hurled: "Your country will be proud of you", easily assuming that the thief was of foreign origin.

The rightful owner got his car back after it was found in the Brussels municipality of Molenbeek, and during a subsequent house search a handwritten note was found. It seemed of little importance: "Bayroshock without chlorine", it mentioned, followed by the addresses of two shops for swimming pool equipment in the North of France. Bayroshock is a product against algae that consists of hydrogen peroxide at a concentration of 34%. Apart from being recommended for the treatment of pools, that same substance is also a main ingredient of TATP. Triacetone triperoxide is the explosive often called 'the Mother of Satan' and known as a terrorist's favorite since the failed attempt by 'shoe bomber' Richard Reid to blow up a plane between Paris and Miami in December 2001.

The man in whose house the note was found, is Ahmed Dahmani — a naturalized Belgian citizen of Moroccan descent. He was born in 1989 in Al Hoceima, a town between the Rif mountains and the Mediterranean Sea. In 2015, he was living in a fourteen-storied building in the Molenbeek ‘Zone du Canal’ — not the kind of address where a swimming pool owner can be expected. He was mainly known to the judiciary as a multi-recidivist criminal, who was caught for theft already at the age of twelve. The latest of the 51 cases in which his name appeared, was about a massive traffic in hard drugs between Belgium, France and Luxembourg. But there were signs of radicalization too, much stronger signs in fact than those present at that time with his childhood friend Salah Abdeslam.

Blessing the expansion of Shariah4Belgium

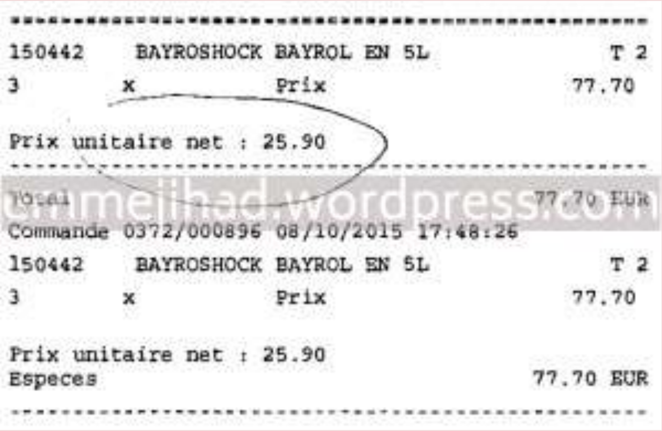
With Abdeslam, he underwent an identity check on board of a ferry between Patras in Greece and Bari in Italy only a week before the car theft in the Netherlands. Now, we know that they conducted one of many travels along the refugee route that was used by the Islamic State to smuggle terrorists to the West, but then it understandingly did not raise a particular suspicion yet. Ten days after the search that uncovered the note, however, Dahmani was named in a report about radicalism. Written by a motorized patrol of the Brussels police that had apprehended a suspected candidate for the Syrian jihad. Friends of the suspect had tried rather brutally to prevent that arrest, and Dahmani was one of them.

At Facebook, Dahmani did not hide his beliefs. There, he complained in 2014 already that the word extremism was “invented by enemies of the Islam”, while posting a quote that the Islamic State often uses to recruit criminals like him for the jihad — the one in which the second caliph Omar ibn al-Khattab declared: “Sometimes the people with the worst past create the best future”. Dahmani also posted Islamic State videos, and three days before a terrorist attack was foiled in Verviers — in January 2015 — he threatened: “One day everything will be paid.” He did all of that under the cover of a pseudonym, but his contacts with a suspect in the Verviers case could have lead to his identification back then already.

In Dahmani’s family tree, radicalism became obvious almost a decade ago. His older brother Mohamed — who basically raised him instead of their always absent father and their chronically ill mother — was named in a terrorist case as early as 2009. He was investigated for his contacts with the suspects of a bomb attack in Cairo that killed a French teenager — the same suspects behind the earliest plot against the Bataclan in Paris. Mohamed Dahmani was never charged, but by the time his brother Ahmed entered the scene, at least three of Mohamed’s friends had left for Syria. One of them departed from Brussels in the company of the later terrorist commander Abdelhamid Abaaoud. And in 2012 already, Mohamed himself was known as a patron of Shariah4Belgium, asked explicitly for his blessings when leader Fouad Belkacem wanted to expand his recruitment from Antwerp to Brussels.

“Talking like youngsters, but not impolite”

Altogether, there were plenty reasons to raise the alarm when Ahmed Dahmani showed his interest in an ingredient for bombs. But that did not happen, and at the 8th of October 2015 — a month after the note of Dahmani was found — a BMW left Molenbeek towards the North of France. At 4h04 that afternoon, the car was caught by a speed camera at the A2 highway in Neuville-sur-Escaut. The license plate would later learn that the vehice was rented by Salah Abdeslam, and the GPS revealed two stops: at 5h02 in the rue Maurice Thorez in Saint-Sauveur, and at 5h44 in the rue Ferdinand de Lesseps in Beauvais — the two shops mentioned on Dahmani’s note.



```
150442     BAYROSHOCK BAYROL EN 5L               T 2
3          x           Prix                    77.70

Prix unitaire net : 25.90
----------------------------------------------------
Total                                      77.70 EUR
Commande 0372/000896 08/10/2015 17:48:26
150442     BAYROSHOCK BAYROL EN 5L               T 2
3          x           Prix                    77.70

Prix unitaire net : 25.90
Especes                                    77.70 EUR
----------------------------------------------------
```

Receipt for 15 liters Bayroshock purchased in Beauvais on October 8, 2015 – sufficient to make about 10 kg of TATP.

Both are branches of Irri Jardin, a chain “for your swimming pool, irrigation and spa”. The shop in Saint-Sauveur had ran out of Bayroshock, it seems. But the Beauvais manager recounted to the police how he sold his entire stock that day. “I had three jerrycans of five liters each, and they asked for more. When I told that half a jerrycan is sufficient for one pool, they claimed that they did the maintenance of several pools in the Paris area. Then they asked for a similar product, which I couldn’t offer. ‘Let’s buy these three then, we have to leave’, one of them said. They paid with cash and didn’t look tense, only a bit in a hurry.”

The manager described the two men as North-Africans between 25 and 30 years old. Both were of average build, had short hair and a short shaved beard. One of them was wearing a jacket over his sweater, the other one a bodywarmer. They spoke French — also when they talked to each other — without a particular accent. "They expressed themselves like youngsters do, but they weren't impolite", the manager said. Confronted with the pictures of known suspects, he thought to recognize Salah Abdeslam. But he wasn't sure. Altogether, the two men spent no more than seven minutes in his shop, after which they made a fuel stop at the Total station of Hardivillers and returned to Molenbeek.

Forbidden in Belgium now, but not in France

French investigators are fairly confident that their purchase has served to fabricate the bombs that were used for the attacks in Paris on the night of 13 November 2015. There were eight explosive belts, of which two have failed to detonate. Each of them contained between one and two kilograms of TATP, and according to explosives experts of the French police, the terrorists could make ten kilograms with fifteen liters Bayroshock. In Belgium, the EU directive banning the sale of hydrogen peroxide in concentrations above 12% to private customers was passed into law in July 2016. But in France, a softened version entered into force last year, just requiring registration for private purchases.

Ahmed Dahmani is in Turkish custody now. He took a flight in Amsterdam on the morning after the Paris attacks, with a ticket that was bought a few hours prior to the bloodbath — indicating that he knew what was going to happen. When he was arrested near Antalya on the 16th of November 2015, he was still in the possession of his Belgian documents, including membership cards of the Christian trade union CSC and the Grand Casino in Brussels. In the meantime, however, he had also bought a false Syrian passport with the name Mazen Mohamad Ali, and the WhatsApp Islamic State. In December 2016, a Turkish court convicted him to ten years and nine months in jail for membership of a terrorist organization. After he has served that sentence, Belgian and French extradition requests are awaiting him.

I Made Over 500 IEDs For Suicide Missions – Boko Haram Teenager

Source: https://thewillnigeria.com/news/i-made-over-500-ieds-for-suicide-missions-boko-haram-teenager/

July 03 – A 15 year-old former Boko Haram bomb maker, Ali Goni, has made a chilling confession about how he made over 500 underwear Improvised Explosive Devices(IEDs) used by insurgents for suicide missions on soft targets in the last five years.

The military authorities described the teenager as the most deadly Boko Haram member, who had mastered various techniques that can cause maximum destruction of lives.

Army intelligence sources told NAN that Goni, who was only ten years old and in primary six when he was kidnapped in Bama, is the most innovative bomb maker to emerge in recent years.

Goni, who is undergoing rehabilitation at a military detention camp in Maiduguri, told NAN recently that he assembled IEDs with fragmented materials and configure them for suicide missions.

He said he introduced the use of padlock to IEDs strapped on bombers that can hardly be demobilised or detected by bomb detectors.

"I was kidnapped along with my mother in Bama's Kawuri Street by Baba Kaka, a dreaded Boko Haram commander. They took us to Sambisa and kept us in a camp called "Kwalfata".

"We underwent various training in the camp. During the course of our induction training, I was selected to be trained on bomb making technique, bomb detection as well as identifying and demobilising explosives.

“I refused initially, but they said they would kill my mother just like the way they killed my father when they stormed Bama. So I eventually agreed. During the training, many of my colleagues died while trying to make bombs. At the end I emerged the best among all.

“My job was to make many bombs that would be used for suicide missions. I was working under the supervision of Baba Musa, a 70 year-old. Musa also thought me the new technique of making underwear IED with padlock.

“At some point, I was the only bomb maker when all those I was trained with were killed by the military during several attacks. So they took me from camp to camps to make IEDs for suicide missions.

“I was in Kangarwa, Pulka, Banki and other camps. I managed to escape when the military bombed our camp in Baga. I ran to Cameroon where I surrendered to the Cameroonian forces. I was later handed over to the Nigeria military.

Goni hoped to be a soldier in the future to help the military in identifying IEDs.

Powders to be banned from hand luggage at UK airports

Source: https://www.telegraph.co.uk/travel/news/powders-banned-hand-luggage-uk-flights/

July 09 – **Powders such as make-up, coffee, and spices are to be banned from hand luggage on flights leaving the UK in a new effort to improve airport security.**

The move, which raises the prospect of more queues and disruption for travellers, would follow in the footsteps of Australia, New Zealand and the US, where passengers were told last month to treat powders in the same way they would liquids, removing them into ziplock bags for separate scanning.

Government plans for UK airports could see travellers restricted to 12 ounces (340 grams) of powder on flights, before being subjected to extra screening, according to The Times.

The measures have been introduced in response to a foiled Isis plot to carry an explosive on board an Etihad flight from Sydney to Abu Dhabi last July. The would-be terrorists were stopped at check-in.

A spokesperson for the Department of Transport, which says it keeps airport security under constant review, would not confirm the plans but told the newspaper: “It is for each country to determine its own security measures based on its own assessments. We work closely with all our international partners to keep aviation security under constant review.”

EDITOR’S COMMENT: Perhaps this is the perfect (secure) way to travel in the future – Oh! Forgot the IED inplants!

There are concerns the new rules will cause confusion and delays at airports. In the US, there have been reports of passengers missing flights after being held up at security over the restrictions.

Mils Hills, associate professor in risk, resilience and corporate security at the University of Northampton, said it was luck that the Isis plot was disrupted, adding: “In itself, these extra restrictions are not going to create lots of disruption at airport security but it has the potential to feed into general public concerns about the safety of flying.”

The Transport Security Administration (TSA) in the US has also been screening food purchased by passengers to eat on flights. The TSA's official line is that it is regularly changing security methods to tackle what it describes as an evolving terrorist threat.

"Terrorists are constantly trying to pack explosives into small everyday items," a TSA spokesman told Telegraph Travel.

The powder restrictions follow in the same vein as rules governing flying with liquids in hand luggage, introduced in 2006 in response to a foiled terror plot to blow up flights between the UK and North America. Three British men were convicted for conspiring to assemble improvised explosive devices on board transatlantic jets – devices containing a liquid derived from hydrogen peroxide – and detonate them above the Atlantic.

The new rules caused chaos at airports, with British Airways alone forced to cancel more than 1,500 flights.

Experts have since said the restrictions - which remain in place forbidding liquids, aerosols or gels in containers of more than 100ml - were a knee-jerk reaction.

"It's not relevant and it should never have been introduced 10 years ago," said Philip Baum, editor of Aviation Security International, in an interview with Telegraph Travel in 2016.

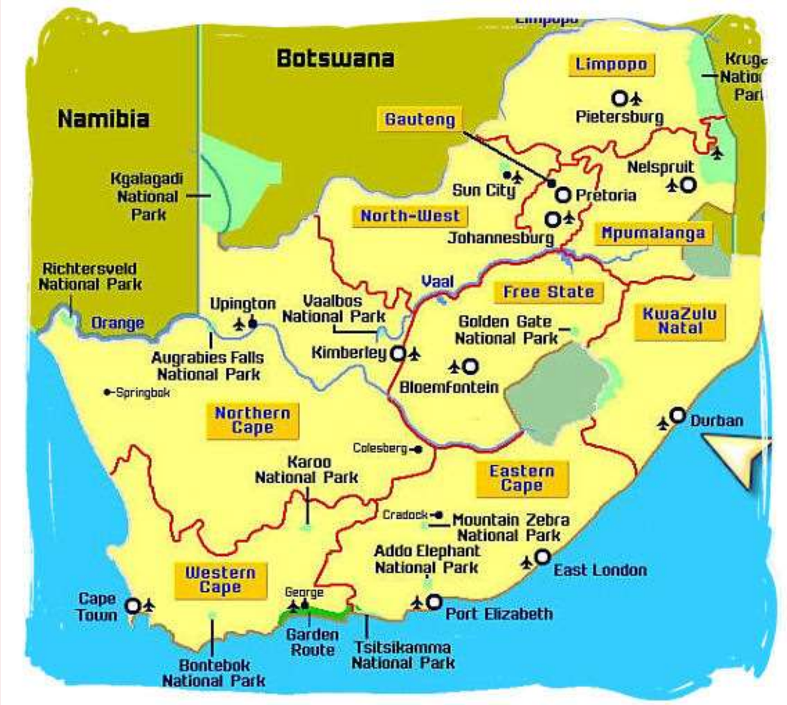
"All they have succeeded in doing is creating longer queues at checkpoints where screeners are spending all of their time looking for restricted items rather than looking for genuine threats."

Explosive devices a sign of what's to come?

Source: https://www.iol.co.za/sunday-tribune/news/explosive-devices-a-sign-of-whats-to-come-16033591

July 15 – The recent spate of explosive devices found around Durban (the largest city in the South African province of KwaZulu-Natal and the third most populous in South Africa after Johannesburg and Cape Town), could be the start of what's to come.

This was the view of two intelligence experts, who said the incidents were being viewed as "trials" to see how police and the public respond - the perpetrators were sending out a discreet message.



Several suspicious incendiary devices were found around Durban in the past two weeks.

Police are expected to make arrests soon. Suspects have been identified, allegedly staying at houses in Verulam and on the Bluff.

A national team from the Hawks Crimes Against the State unit have been in Durban over the past few days, investigating.

Hawks national spokesperson Brigadier Hangwani Mulaudzi called for calm, but said the public should remain vigilant at all times.

"We are working around the clock to arrest suspects and these incidents are receiving serious attention," said Mulaudzi.

Explosive devices were found in Woolworths stores at Gateway and Pavilion malls last week. While Durban July festivities were taking place, pipe bombs were detonated near cars parked on Gladys Mazibuko and Avondale roads.

This week, a suspicious device was reported in a parking lot at the Pavilion, but it turned out to be a hoax. On Monday night another explosive device was found at a Spar store in Wentworth. There were also hoax reports of bombs at the Cornubia Mall and Phoenix police station on Thursday.

Willem Els, an expert in crime scene handling and bomb disposal at the Institute of Security Studies, said the improvised explosive devices were designed to detonate and were not made in a factory.

Extremists

“This is the preferred choice for extremist groups such as al-Shabaab and Islamic State, so we cannot root out the possibility of extremism,” said Els.

Another possibility was that a group of people or an individual could be holding the event or business affected to ransom, he said.

“We have heard of threats being made against certain businesses or organisations where those making the threats would claim they planned to use an explosive device if money was not handed to them.”

He said the string of devices that were found also raised questions about why authorities had not acted sooner when an explosive device was found at the Imam Hussain Mosque more than two months ago.

State Security spokesperson Brian Dube said the series of explosive threats was receiving attention and a multidisciplinary task team had been appointed to look into the problem.

“Law enforcement agencies have noted the incidents with concern. The motive and intent behind this, as well as the identification of those responsible for the acts, form part of our ongoing investigations,” said Dube.

He also called on the public to remain calm but vigilant.

“I am confident we will make a breakthrough soon. The case is at a sensitive stage.”

Former spy reveals why al Qaeda called off NYC subway attack

By Aimen Dean

Source: https://edition.cnn.com/2018/07/12/world/al-qaeda-spy-nine-lives-aimen-dean-book-excerpt/index.html

July 12 – The device itself was not particularly impressive to look at.

Taped together from parts you might find in a tool shed, it had holes that would allow the 'violent spewing' out of cyanogen chloride, as a detailed description of the device later posted by American authorities said.

The detonator could be triggered by a timer or cell phone so that the attacker could deploy the weapon without sharing the choking, excruciating death it caused.

'The 2000s' on CNN

On a gloomy afternoon in Afghanistan, before the events of September 11, 2001, al Qaeda jihadis and I rigged up a prototype and inserted a timed fuse to set off the detonator. The fuse set off the weapon as planned, and from a safe distance we heard a crack and a rush of air.

I felt sick to my stomach. Whether I liked it or not, the 'unique invention' -- the al-mubtakkar-al farid, as it quickly became known -- was born.

A new class of terrorist weapon had been created.

Something called a 'mubtakkar'

After 9/11, MI6 was enthusiastic about my moving to the Gulf. Bahrain was regarded as an important conduit between Saudi Arabia and Iran, where some in al Qaeda's upper echelons had taken refuge.

I did not advertise my presence there, but waited for opportunity to come my way. Within just a few weeks, it did. And it was no accident.

His name was Akhil, and he was a chemistry teacher.

A Saudi in his mid-30s, Akhil was working in Bahrain. He was balding and slightly overweight, with a forgettable face but intense, excitable eyes. He had fought in Afghanistan in the early 1990s.

"You must have dinner with me. I know a great place on Exhibition Road," he told me.

Days later we were sharing grilled lamb and Bukhari rice. But I sensed this was not just a social event; Akhil had something to ask me. As the plates were cleared away he leaned forward, his eyes searching me.

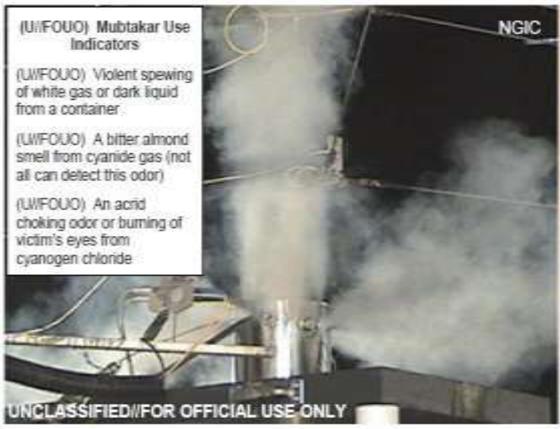
"Are you by any chance also known as Abu Abbas al-Bahraini?" he asked quietly.

"Yes," I answered, "that was the name I took in Afghanistan." I had to tread carefully. I hardly knew this man.

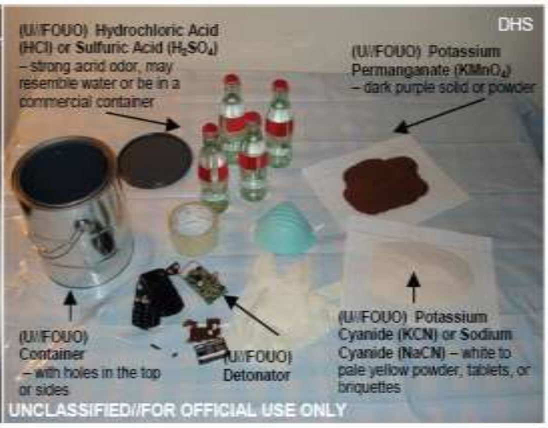
"So you are aware of something called a mubtakkar?"

He now had my full attention.

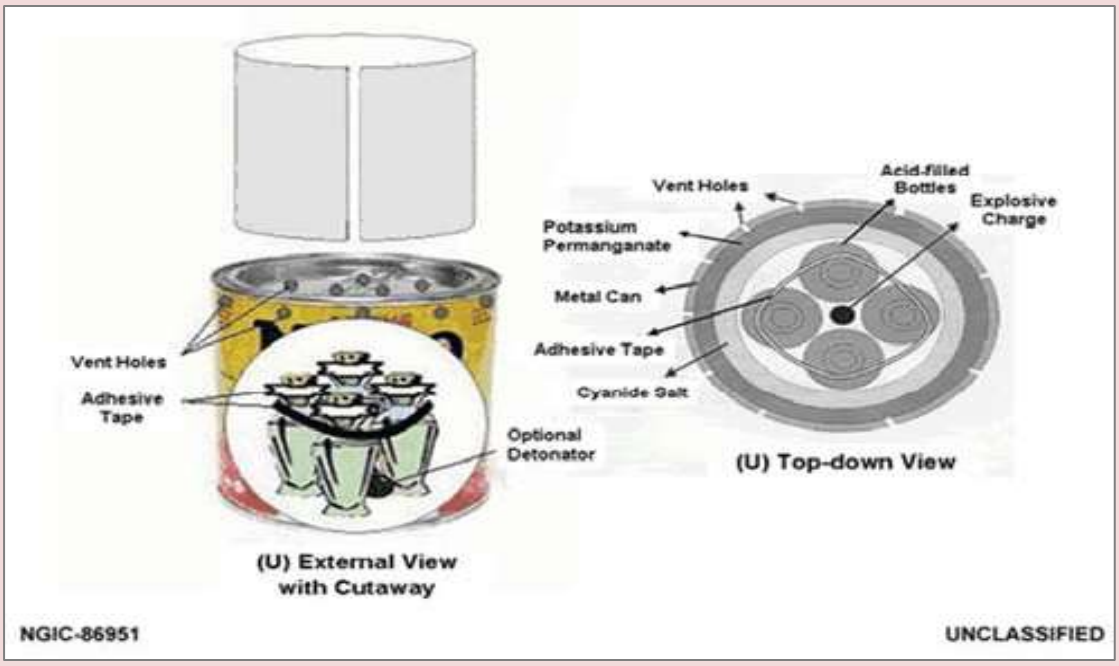
"Yes, I am," I responded, and as casually as I could gave him the barest details about the device.


(U//FOUO) Mubtakar Use Indicators
(U//FOUO) Violent spewing of white gas or dark liquid from a container
(U//FOUO) A bitter almond smell from cyanide gas (not all can detect this odor)
(U//FOUO) An acrid choking odor or burning of victim's eyes from cyanogen chloride
NGIC
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Demonstration of a mubtakar release.


(U//FOUO) Hydrochloric Acid (HCl) or Sulfuric Acid (H_2SO_4) – strong acid odor, may resemble water or be in a commercial container
DHS
(U//FOUO) Potassium Permanganate ($KMnO_4$) – dark purple solid or powder
(U//FOUO) Container – with holes in the top or sides
(U//FOUO) Detonator
(U//FOUO) Potassium Cyanide (KCN) or Sodium Cyanide (NaCN) – white to pale yellow powder, tablets, or briquettes
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Mubtakar production indicators (mock-up).



"I have an urgent message from your friends in Saudi Arabia who are looking for you. We have your notes from the mubtakkar. But we can't understand your handwriting."

Akhil slid a stack of papers with diagrams and formulae across the table. "Have we got it right?" he asked. They had. Akhil knew his chemistry, and I could not lie to him for that very reason.

'Which is more deadly?'

A week later we met again at the same restaurant.

"I have great news," he went on, his eyes glowing. "Our brothers built the mubtakkar in the desert. There was a successful test."

How he loved being the go-between, at the center of the web.

"When you guys were developing the device, did you ever talk about the sarin attack in Tokyo?" he asked.

"Yes."

His eyes flitted conspiratorially. For a moment he looked like a squirrel.

"Remember I asked you to confirm that cyanogen chloride was 2.47 times heavier than air?" Now he was into his chemistry teacher mode. "How will that affect how quickly it spreads in the ventilation of a subway system? Should we use it or hydrogen cyanide?" he asked. "Which is more deadly?"

He had used the English word "subway." He hadn't said metro or underground.

For a moment I forgot my training. "Subway, as in New York?"

He smiled but said nothing.

I had to cooperate, to sound as if I, too, wanted to maximize casualties. The best approach, I quickly decided, was to provide him a mix of information and disinformation. It was perturbing to be discussing the relative merits of gassing New Yorkers with what was in effect Zyklon B or the equally nasty cyanogen chloride.

"What can happen with both gases," I continued, "is that the lungs are flooded with fluid. Your last moments can include cardiac arrest, choking and violent seizures. It's a ghastly way to die."

The rapt attention on Akhil's face is an image I still remember. It was time to request an urgent meeting with British intelligence.

Al Qaeda's surprise

There followed more dinner meetings with Akhil, as I needed to find out more about their plans.

"We have four Saudi brothers already in Morocco and someone there who will teach them how to build the mubtakkar," he said. "They all have 10-year visas for the United States and can go anytime."

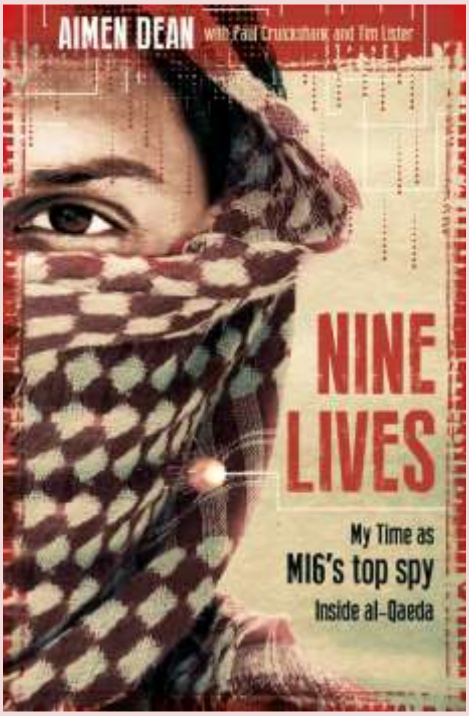
The operation had clearly moved beyond the planning stage. The enormity of what I was hearing was slowly sinking in.

MI6 shared my intelligence with the Americans. My information was fed quickly up the chain to the White House. President George W. Bush was briefed in the Oval Office; according to one account there was stunned silence when the implications of the mubtakkar were absorbed.

Despite the fact that the invasion of Iraq was weeks away, the plot was discussed at length, with CIA Director George Tenet stressing the need to "chase down" the threat. The mood among some officials was later described as "just shy of panic." Might the cell already have been dispatched to the United States? Was there a plan to attack the New York subway the moment the invasion began? When the NYPD police chief Ray Kelly was eventually briefed he worried "the damage could be catastrophic."

But al Qaeda had another surprise in store.

Al Qaeda's deputy leader, Ayman al-Zawahiri, had consulted al Qaeda's Shura Council. He was concerned that an attack in New York would be used to claim that Saddam Hussein had given al Qaeda weapons of mass destruction so that the Americans could legitimize the invasion of Iraq, however ridiculous the link.


AIMEN DEAN with Paul Cruickshank and Tim Lister
NINE LIVES
My Time as MI6's top spy Inside al-Qaeda

"It's not going to happen," Akhil told me when we next met. "Zawahiri has cancelled the operation."

I tried to appear desperately disappointed despite the relief coursing through my veins. "So what are Zawahiri's instructions?" I asked.

"To keep knowledge about the mubtakkar under tight control," Akhil replied.

When my intelligence reached the White House, Vice President Dick Cheney was perplexed and worried that something bigger was in the works. For British intelligence, the priority was to prevent the mubtakkar blueprint from finding a wider audience.

On February 13, 2003, as a result of intelligence I provided to the British, Bahraini police stopped a group of men as they drove across the King Fahd Causeway. One of those detained was Bassam Bokhowa, an IT technician in his mid-30s. On his laptop they found blueprints for the mubtakkar.

Within hours of Bokhowa's arrest, MI6 and the CIA were poring over the blueprints. Any remaining skepticism that a real plot had been in the works was banished. The CIA arranged for a prototype of the device to be built and estimated that a coordinated attack involving multiple mubtakkars would undoubtedly be lethal. The agency was so disturbed by the outcome that they took the device to the Oval Office.

President Bush is said to have picked it up, saying quietly: "Thing's a nightmare."

Aimen Dean was arguably the most important spy inside al Qaeda for the UK's secret service agencies leading up to and following the September 11, 2001 terror attacks. After 9/11, al Qaeda plotted to release a poison gas inside New York City's subway system. In this edited excerpt from his book "Nine Lives," Dean reveals how the plot came to be and why it never happened.

International CBRNE Institute

CBRNE-Terrorism Newsletter

CYBER NEWS

Technology as Enabler of Fake News and a Potential Tool to Combat It

By Dr. Žiga TURK, University of Ljubljana, Slovenia
Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Source:http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018)619008

May 15 – This paper investigates the role of technology in the circulation of the so-called fake news. Technology is a major tool for the dissemination of fake news but also offers methods to analyse their real impacts and tools with which fake news can be argued against and even, more or less democratically, stopped. This document was prepared for Policy Department A at the request of the Internal Market and Consumer Protection Committee.

ISPI and Leonardo present a new Observatory on cyber security

Source: https://www.marketforecast.com/industrynews/ispi-and-leonardo-present-a-new-observatory-on-cyber-security-45622#.Wzyu13amWRE.linkedin

July 06 – A new Observatory on cyber security has been created by ISPI, the Italian study centre specialised in global geopolitical and political-economical analysis and Leonardo, a global player in Aerospace, Defence and Security and Italy's main industrial company. **The new project is aimed at analysing the dynamics taking place in the cybernetic space through debates and publications, with a focus on foreign and security policies and the role of national stakeholders, including those in the private sector.**

The first conference, "Living with cyber risk", will take place on Friday 29th June at ISPI's Milan office. Giampiero Massolo, ISPI Chairman, Giorgio Mosca, Director of Competitive Analysis, Strategy and Technologies, Security and Information systems division, at Leonardo, Merle Maigre, Director of NATO Center of Excellence on Cooperative Cyber Defence, John Allen, Chairman of Brookings In-stitution, Marina Kaljurand, Chairman of the Global Commission on Cyberspace Stability will take part in the event. The analysis will start from the observation that modern companies rely more and more on a secure, resilient and - at least in the Western side of the World - free internet. At the same time, the cybernetic space is not completely governed, it does not have clear lines of authority, criminals often use it, and it is a place where the strongest often win. The introduction of new technologies such as Artificial Intelligence, lethal autonomous weapons and robotics will lead to further transformation in this direction. It is therefore necessary to reflect on whether and how to accept a permanent state of conflict within the networks, coexisting with these existential threats to our security.

Leonardo has already worked together with ISPI on a study regarding "Armed conflicts in the cyber age". The next dossier the two organisations will produce together, which will cover cyber-crime and national security, will be published soon.

Hacking The Bomb, Cyber Threats & Nuclear Weapons, reviewed

By Simon Cocking
Source: https://irishtechnews.ie/hacking-the-bomb-cyber-threats-nuclear-weapons-reviewed/

July 13 – *Are nuclear weapons safe from cyber-attack? Could terrorists actually launch a nuclear attack through hacking? Are we standing at the edge of a major technological challenge to global nuclear order? These are among the many vital security questions addressed in* Dr *Andrew Futter's ground-breaking study of this worrying and little-understood development.*

Hacking the Bomb provides the first comprehensive analysis of the cyber threat to nuclear weapon systems around the world. Dr *Andrew Futter, associate professor at The University of Leicester, makes the case for caution when it comes to the way we manage the ultimate weapon. Many of the considerable* number *of nuclear weapons that remain in the world today are now held on quick alert and are increasingly reliant on complex lines of digital code. When you combine this with the growing spread of both cyber and nuclear weapons* *technology, the risks are evident – mixing weapons of mass disruption with weapons of mass destruction could be devasting and Andrew argues against establishing a dangerous norm of "hacking the bomb."*

This is potentially the sort of book you don't want to read. If you cast your mind back over the last 50 years and beyond, and the number of times we, as the human race have nearly managed to completely blow ourselves up, due to physical mess ups and massive human incompetence, then the last thing we need is to now have IT related options for our own destruction. Stories of loaded, but not primed weapons of massive destruction rolling out of in-flight cargo bays are not uncommon. Nor are error messages informing us of a massive incoming Soviet nuclear strike, before realising it was just a flock of pigeons, and etc etc. You get the idea.

So then the question of our nuclear safety, now that we are in the digital age, should not leave us with any confidence that things are going to be any better. This book calmly and effectively illustrates that your worst fears are more than confirmed. If something can be hacked, why on earth would it not be hacked. We're too big, and too diverse a global population now to not have someone do something that could wipe us all out, simply because they can…

This book is necessary, it is useful, it illustrates where the errors and the loop holes are. Will it actually save us from our selves? Who knows, but hopefully some of the more basic ways of doing so could perhaps be tightened up?

Cybersecurity operations: Don't wait for the alert

By Robert C. Covington

Source: https://www.csoonline.com/article/3290397/network-security/cybersecurity-operations-dont-wait-for-the-alert.html

July 15 – One of the reasons that we in the cybersecurity industry continue to lose to bad actors is our lack of pro-activity. While many organizations have made big investments in their security functions, they tend focus largely on reacting to alerts and responding to known situations. This is a bit like arming your burglar alarm after the robbery.

For the typical enterprise, the key aspect of the cybersecurity function involves a security operations center (SOC), typically a large room with big monitors lining the walls. The SOC Analysts watch the monitors for alerts, and when they find one, they follow a playbook that defines the corporate standard for responding to that type of alert. Such a system is well designed as a reactive approach to security. They are popular, in part, because of their scalability. They are staffed by folks that in most cases have limited experience and undeveloped investigatory skills. These Analysts are often comparably inexpensive, and if activity warrants, these operations can be easily enlarged. The SOC would seem to be the ideal solution keeping up with our abundant cybersecurity activities. Unfortunately, a SOC is usually only good at responding to alerts, with the damage often being done before the first alert sounds.

A recent published report in Crowdstrike indicated that the average dwell time for a network intrusion, from entry to discovery, was 229 days. As such, a bad actor has plenty of time to steal data or damage systems before the first alert is ever sounded. A SOC responding to alerts will provide little benefit in responding to such an attack and can only serve to minimize and quantify the exposure.

The SOC does have its place. My organization uses a commercial SOC service from a well know company. They generate many alerts, each of which is investigated by my in-house team. Their alerts are often for conditions my team would not have the time to find. Unfortunately, we generally do not get such an alert until well after the problem has occurred, and they are often for lower priority issues. These alerts do provide value, because they allow us to clean up infections, and tighten our preventive measures. They would not, however, prevent damage from a significant incident. Thus, if we try to rely on the SOC as our primary means of enforcing cybersecurity, we are doomed to failure.

So, if the SOC is not the best answer, what is? I would suggest that the best approach is a team of folks with strong investigative skills, who spend their days finding issues before the first alert sounds. These individuals are far different in skill and mindsets from the typical SOC occupant. They have an instinct to follow their noses, and a strong drive to find an explanation for every anomaly they identify. They usually possess the tenacity to not give up on an issue until they have an answer.

True, these individuals are more expensive, and much harder to find. When you do find them however and empower them to dig for issues rather than waiting on them to surface via an alert, they quickly pay for themselves.

Here are some tips for achieving a true investigative function:

Hire the right folks

This almost goes without saying, but having a team with investigative skills and mindset is critical to achieving an effective organization. I prioritize investigative abilities over actual experience in most cases, to find the people I need. Selection requires a careful interview process, because these special skills will often not jump out at the reader from a resume page.

Provide the needed tools

Although you don't need to spend a fortune on tools for a good team, certain fundamental systems are essential for a good investigative function. The cornerstone for this is the Security Incident Event Management system (SIEM), which collects log records from various systems into a single repository. This requirement does not stop at the purchase of the system, however. It is critical that key servers, network devices, and even workstations be setup to send their log records to the SIEM. A SIEM with the necessary data allows an investigator to correlate events from various logs to look for behavioral patterns. Without an SIEM, the Analyst would need to look at too many individual logs, hampering the process.

Provide good training

Ongoing training is critical to a good investigative function. Sadly, I have seen few good training opportunities specific to this need. In my experience, training designed for red teams, which many companies use to test security from the outside of a company in, works best for investigators, given that it allows the Analysts to put themselves in the position of an attacker, so they have a better idea what to look for.

Give them time

A good investigator must have time to follow their gut. If they see something that bothers them, they must be allowed to dig into the issue until they find a problem or satisfy themselves that all is well. In the process, they will go down many rabbit holes and find nothing of note, but each one is an educational experience. Rather than scheduling them for too many routine activities, free them to do what they do best—dig.

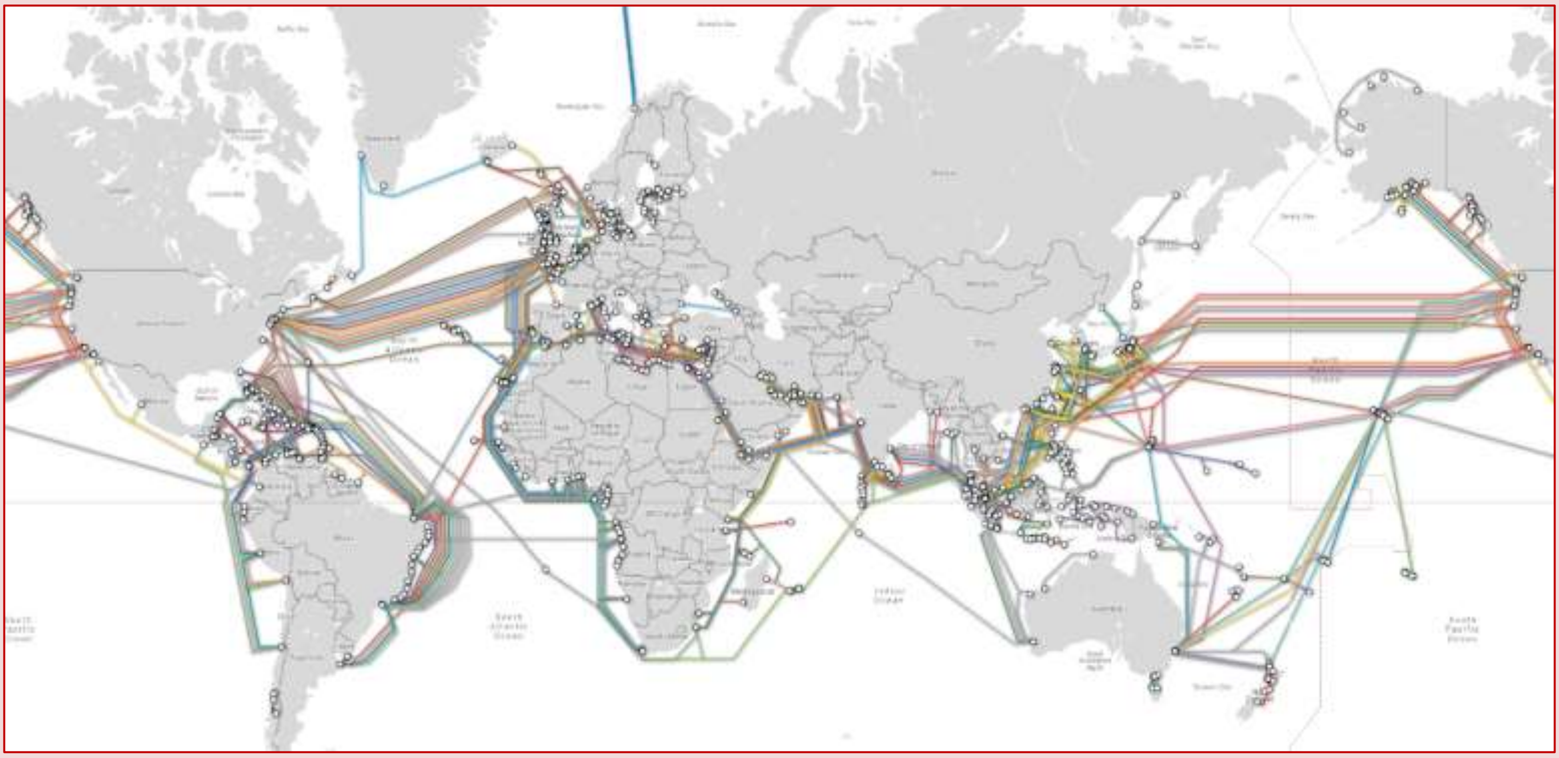
Bottom line: An SOC is a useful part of our cybersecurity arsenal, but its main benefit will be in helping to minimize damage from an issue that has already happened. A strong investigative team, on the other hand, can help to identify and resolve issues before they cause major damage, which is always our preference.

Robert C. Covington, *the "Go To Guy" for small and medium business security and compliance, is the founder and president of togoCIO.com. Mr. Covington has B.S. in Computer Science from the University of Miami, with over 30 years of experience in the technology sector, much of it at the senior management level. His functional experience includes major technology implementations, small and large-scale telecom implementation and support, and operations management, with emphasis on high-volume, mission critical environments. His expertise includes compliance, risk management, disaster recovery, information security and IT governance.*

Buried internet infrastructure at risk as sea levels rise

Source: http://www.homelandsecuritynewswire.com/dr20180717-buried-internet-infrastructure-at-risk-as-sea-levels-rise

July 17 – Thousands of miles of buried fiber optic cable in densely populated coastal regions of the United States may soon be inundated by rising seas, according to a new study by researchers at the University of Wisconsin–Madison and the University of Oregon.



The study, presented yesterday (16 July 2018) at a meeting of internet network researchers, portrays critical communications infrastructure that could be submerged by rising seas in as soon as fifteen years, according to the study's senior author, Paul Barford, a UW–Madison professor of computer science.

"Most of the damage that's going to be done in the next 100 years will be done sooner than later," says Barford, an authority on the "physical internet" — the buried fiber optic cables, data centers, traffic exchanges and termination points that are the nerve centers, arteries and hubs of the vast global information network. "That surprised us. The expectation was that we'd have 50 years to plan for it. We don't have 50 years."

Wisconsin says that the study, conducted with Barford's former student Ramakrishnan Durairajan, now of the University of Oregon, and Carol Barford, who directs UW–Madison's Center for Sustainability and the Global Environment, is the first assessment of risk of climate change to the internet. It suggests that by the year 2033 more than 4,000 miles of buried fiber optic conduit will be underwater, and more than 1,100 traffic hubs will be surrounded by water. The most susceptible U.S. cities, according to the report, are New York, Miami and Seattle, but the effects would not be confined to those areas and would ripple across the internet, says Barford, potentially disrupting global communications.

The study combined data from the Internet Atlas, a comprehensive global map of the internet's physical structure, and projections of sea level incursion from the National Oceanic and Atmospheric Administration (NOAA). The study, which only evaluated risk to infrastructure in the United States, was shared today with academic and industry researchers at the Applied Networking Research Workshop, a meeting of the Association for Computing Machinery, the Internet Society and the Institute of Electrical and Electronics Engineers.

Much of this infrastructure is buried and follows long-established rights of way, typically paralleling highways and coastlines, says Barford. "When it was built 20–25 years ago, no thought was given to climate change."

Many of the conduits at risk are already close to sea level and only a slight rise in ocean levels due to melting polar ice and thermal expansion as climate warms will be needed to expose buried fiber optic cables to sea water. Hints of the problems to come, says Barford, can be seen in the catastrophic storm surges and flooding that accompanied hurricanes Sandy and Katrina.

Buried fiber optic cables are designed to be water-resistant, but unlike the marine cables that ferry data from continent to continent under the ocean, they are not waterproof.

Risk to the physical internet, says Barford, is coupled to the large population centers that exist on the coasts, which also tend to be the same places where the transoceanic marine cables that underpin global communication networks come ashore. “The landing points are all going to be underwater in a short period of time,” he notes.

Moreover, much of the data that transits the internet tends to converge on a small number of fiber optic strands that lead to large population centers like New York, one of the more vulnerable cities identified in the study.

The impact of mitigation such as sea walls, according to the study, are difficult to predict. “The first instinct will be to harden the infrastructure,” Barford says. “But keeping the sea at bay is hard. We can probably buy a little time, but in the long run it’s just not going to be effective.”

In addition to looking at the risk to local and long-haul infrastructure in the nation’s coastal areas, the study examined the risk to the buried assets of individual internet service providers. It found the networks of CenturyLink, Inteliquent and AT&T to be at highest risk.

The findings of the study, argues the Wisconsin computer scientist, serve notice to industry and government. “This is a wake-up call. We need to be thinking about how to address this issue.”

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

Source: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

July 20 – In Singapore’s worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. **Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.**

The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

At a multi-ministry press conference on Friday (July 20), the authorities said PM Lee's information was "specifically and repeatedly targeted".

The 1.5 million patients had visited SingHealth's specialist outpatient clinics and polyclinics from May 1, 2015, to July 4, 2018.

Their non-medical personal data that was illegally accessed and copied included their names, IC numbers, addresses, gender, race and dates of birth. No record was tampered with and no other patient records such as diagnosis, test results and doctors' notes were breached. There was no evidence of a similar breach in the other public healthcare IT systems.

Health Minister Gan Kim Yong and Minister for Communications and Information S. Iswaran both described the leak as the most serious, unprecedented breach of personal data in Singapore.

Mr Gan apologised to the affected patients, saying: “We are deeply sorry this has happened.”

Mr David Koh, chief executive of the Cyber Security Agency of Singapore, said that “this was a deliberate, targeted and well-planned cyber attack”.

“It was not the work of casual hackers or criminal gangs,” he added.

In the light of the attack, all of Singapore's Smart Nation plans, including the mandatory contribution to the National Electronic Health Record (NEHR) project - which enables the sharing of patients' treatment and medical data among hospitals here - have been paused.

Specifically, mandatory contribution to NEHR is now on hold until further notice.

Mr Iswaran, who is also Minister-in-Charge of Cyber Security, will convene a Committee of Inquiry (COI) to conduct an independent external review of the incident. Retired district judge Richard Magnus will chair the committee.

Initial investigations showed that one SingHealth front-end workstation was infected with malware through which the hackers gained access to the data base. The data theft happened between June 27, 2018, and July 4, 2018.

SingHealth has imposed a temporary Internet surfing separation on all of its 28,000 staff's work computers. Other public healthcare institutions will do the same.

Unusual activity was first detected on July 4 on one of SingHealth's IT databases. Security measures, including the blocking of dubious connections and changing of passwords, were taken to thwart the hackers.

On July 10, the Health Ministry, SingHealth and the Cyber Security Agency of Singapore were informed after forensic investigations confirmed that it was a cyber attack. A police report was made on July 12.

No further data has been stolen since July 4.

All patient records in SingHealth's IT system remain intact and there has been no disruption of healthcare services.

SingHealth will be contacting all patients who visited its specialist outpatient clinics and polyclinics from May 1, 2015, to July 4, 2018, to notify them if their data has been stolen. An SMS message will be sent to all patients over the next five days.

Patients can also access the Health Buddy mobile app and SingHealth website to check if they are affected by the breach. They can also check using this link.

Mr Iswaran said that “we must get to the bottom of this breach”.

“We must not let this derail our Smart Nation services... it is the way of the future,” he said, taking a longer-term view of the projects.

Even though a thorough review of Smart Nation projects will be conducted, he stressed that Singapore has paused but not halted these projects.

The Ministry of Health has directed a thorough review of the public healthcare system to improve cyber security, and all public and private healthcare institutions have been advised to take cyber-security precautions.

FBI wish list: An app that can recognize the meaning of your tattoos

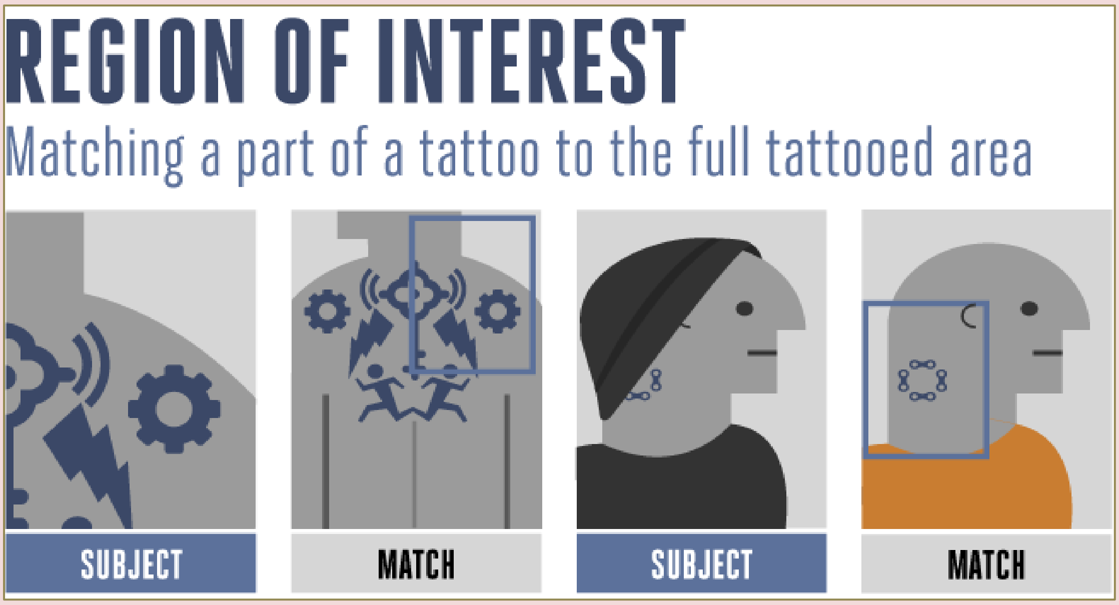
By Dave Maass

Source: http://www.homelandsecuritynewswire.com/dr20180720-fbi-wish-list-an-app-that-can-recognize-the-meaning-of-your-tattoos

July 20 – We’ve long known that the FBI is heavily invested in developing face recognition technology as a key component in its criminal investigations. But new records, obtained by EFF through a Freedom of Information Act (FOIA) lawsuit, show that’s not the only biometric marker the agency has its eyes on. The FBI’s wish list also includes image recognition technology and mobile devices to attempt to use tattoos to map out people's relationships and identify their beliefs.

EFF began looking at tattoo recognition technology in 2015, after discovering that the National Institute for Standards & Technology (NIST), in collaboration with the FBI, was promoting experiments using tattoo images gathered involuntarily from prison inmates and arrestees. The agencies had provided a dataset of thousands of prisoner tattoos to some 19 outside groups, including companies and academic institutions, that are developing image recognition and biometric technology. Government officials instructed the groups to demonstrate how the technology could be used to identify people by their tattoos and match tattoos with similar imagery.

Our investigation found that NIST was targeting people who shared common beliefs, with a heavy emphasis on religious imagery. NIST researchers, we discovered, had also bypassed basic oversight measures. Despite rigid requirements designed to protect prisoners who might be used as subjects in government research, the researchers failed to seek sign-off from the in-house watchdog before embarking on the project.



Following our report, NIST stopped responding to EFF's FOIA requests. The agency also rushed to retroactively alter its documents to downplay the nature of the research. In a statement issued to the press, NIST denied our findings, claiming that its goal was simply to evaluate the effectiveness of tattoo recognition algorithms and "not about the many complex law enforcement policies or approaches that may be related to images of tattoos."

This claim rings especially hollow now that the FBI has released email communications and slide presentations with NIST in response to our FOIA suit.

Among the records were two previously withheld presentations from FBI divisions focused on deciphering tattoos that were delivered at a special event organized by NIST for participants in the research project.

What the FBI "wants" and "needs"

While the FBI has long used a rudimentary system called TAG-IMAGE to use tattoos to identify people, according to the presentation, "It does NOT [sic] attempt to answer the question 'What does it mean?'" Officials told the roomful of government, academic, and corporate researchers assembled by NIST that the FBI is seeking to establish "affiliation" using tattoo images. This means identifying "gang membership, terrorist relevance, location, [and] symbols description/meaning."

One particularly alarming presentation by the chief of the FBI's Cryptanalysis & Racketeering Records Unit was titled, "Tattoo, Graffiti, and Symbol Recognition: A Codebreakers Perspective." It began with a graphic of exclusively religious symbols, including Christian, Jewish, Hindu, and Taoist iconography.

A subsequent slide was even more ominous. The headline read: "We want a one stop database to tell us what a symbol means."

The presentation went onto explain that the FBI currently uses open-source resources to decipher the meanings of symbols and tattoos. These include the Anti-Defamation League's Hate on Display database, the University of Michigan's Science Fiction and Fantasy "Dictionary of Symbolism," and the U.S. Patent and Trademark Office's website.

The heavily redacted presentation included blacked-out slides that would have shown the extent of the FBI's current efforts as well as several individual examples that posed the question, "What does this tattoo mean?"

Further in the presentation, the FBI further elaborated on its goals: "The Technology We Need: web accessible user populated database with instant i2i matching" (i2i stands for "image to image"). The slide included a photograph of a New York Police Department officer tinkering with a smartphone.

This technology is not science fiction: several years ago the Department of Homeland Security promoted a controversial program at Purdue University to crowdsource gang graffiti and tattoo images for a mobile recognition app. A prototype technology was deployed in Indiana and Illinois and introduced to the FBI in 2014. However, very little information is available about this pilot program after 2016.

Tattoos and meaning

Most biometric technology, such as face, iris, or finger print recognition, is designed to establish the identity of otherwise unknown suspects or victims. Tattoo recognition is different in that not only can tattoos be used for identification, they can also reveal further information about the individual. For example a tattoo could say a lot about a person's politics, religious beliefs, who their family members are, or even their favorite recording artist.

It's this utility that raises civil liberties concerns, particularly in an age where law enforcement may be using tattoos to add individuals to gang databases or prioritize immigrants for deportation proceedings. For example, while the FBI says that the database could link members of a particular gang, it is also true that it could be used to compile a list of individuals who subscribe to a particular religion.

It's also important to note the risk of erroneous interpretations of tattoos, whether by human or technology. A swastika tattoo, for example, could refer to the Neo-Nazi movement, but it's also a symbol used by Native Americans. A six-pointed star is often associated with Judaism, but it can also signify a particular street gang.

In one high profile case, federal officials attempted to deport a Mexican man after accusing him of having a gang-affiliated tattoo. A judge found that claim to be unfounded [PDF] after prosecutors were unable to counter a well-respected gang expert's testimony that he had "never seen a gang member with a similar tattoo nor would [he] attribute this tattoo to have any gang-related meaning."

Even if a person has a gang tattoo, it does not mean they are part of that gang: often people who leave gangs cannot afford to have tattoos removed. In some cases, gang members have forcibly tattooed women against their will.

NIST's research itself also illustrates how dangerous this technology can be: none of the third parties were able to produce better than 15% accuracy in matching tattoos based on imagery.

More records on the way

The new documents from the FBI begin to bare the truth about the agency's tattoo recognition plans, however we are still waiting on the government to fully provide the records we requested. For example, EFF has demanded NIST and the FBI provide a list of the 19 companies and research institutions that received copies of the images collected from inmates.

Tattoo recognition technology is still in its early stages, but as we see an increased interest from federal agencies to use tattoos as an excuse to persecute immigrants, it's more important than ever to expose this technology before it reaches maturation.

— Read the FBI records provided in response to EFF's FOIA litigation

Dave Maass is Senior Investigative Researcher at EFF. This article is published courtesy of the Electronic Frontier Foundation (EFF)

New method detects malicious emails

Source: http://www.homelandsecuritynewswire.com/dr20180720-new-method-detects-malicious-emails

July 20 – Researchers at the Ben-Gurion University of the Negev (BGU) Malware Lab have developed a new method for detecting malicious e-mails that is more effective than the top 60 antivirus engines on the market.

"Current e-mail solutions use rule-based methods and don't analyze other elements of the message," says Dr. Nir Nissim, head of the David and Janet Polak Family Malware Lab at Cyber@BGU, and a member of the Department of Industrial Engineering and Management. "Existing antivirus engines primarily use signature-based detection methods and therefore are insufficient for detecting new, unknown malicious emails."

Email-Sec-360, the new method from BGU, leverages 100 general descriptive features extracted from all e-mail components, including header, body and attachments, to detect a malicious message. The research was published in the exclusive scientific journal *Expert Systems with Applications*.

AABGU notes that the method, developed by Ph.D. student and researcher Aviad Cohen, is built on machine learning principles and operates without internet access, making it a useful solution for both individuals and businesses.

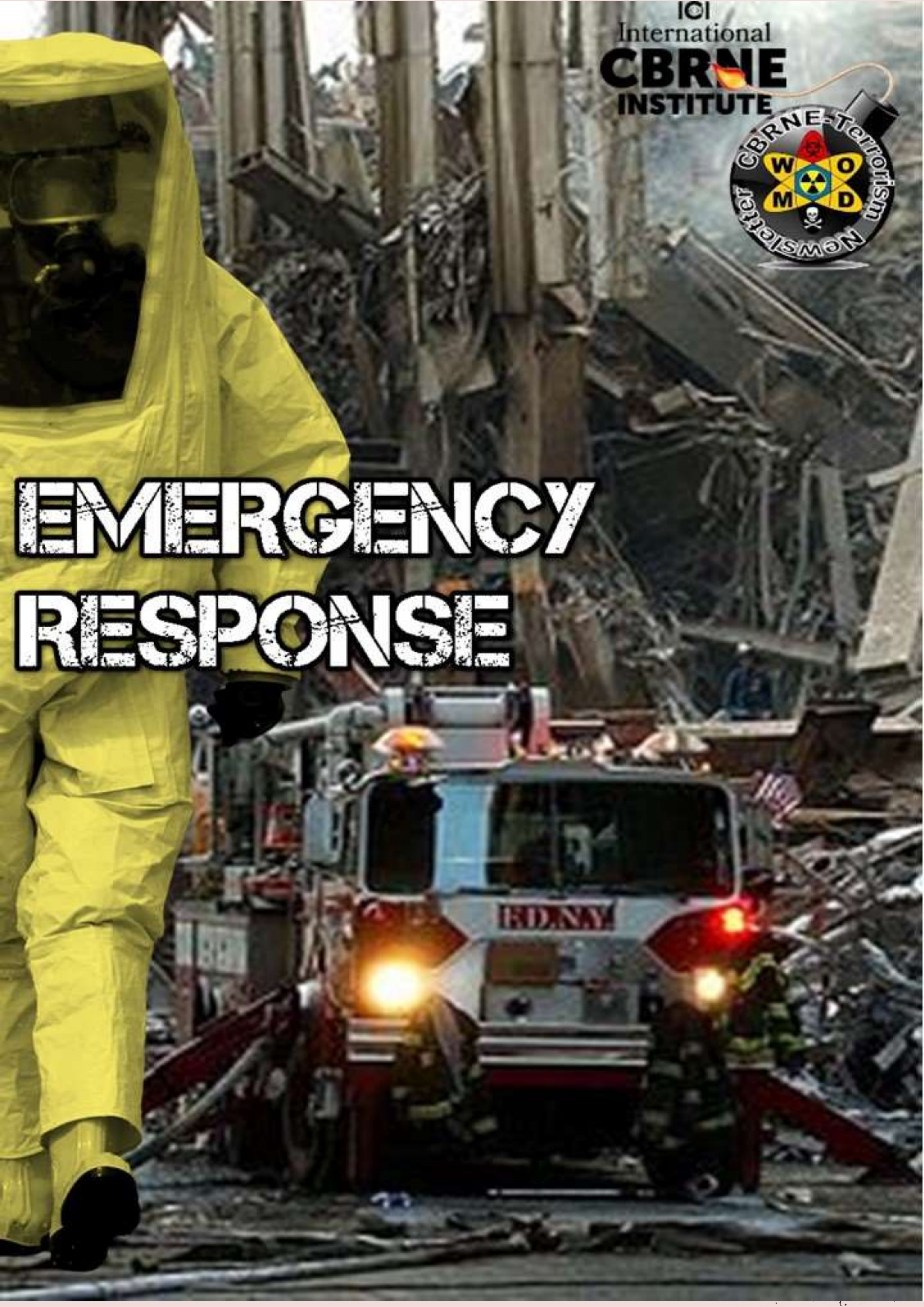
To build out their detection model, the researchers used 33,142 emails (12,835 malicious and 20,307 benign), which they collected between 2013 and 2016, the release noted. Upon testing, researchers found that their method outperformed the next best antivirus engine by 13 percent.

"In future work, we are interested in extending our research and integrating analysis of attachments, such as PDFs and Microsoft Office documents within Email-Sec-360°, since these are often used by hackers to get users to open and propagate viruses and malware," says Dr. Nissim. He also noted that these methods have already been developed at the BGU Malware Lab.

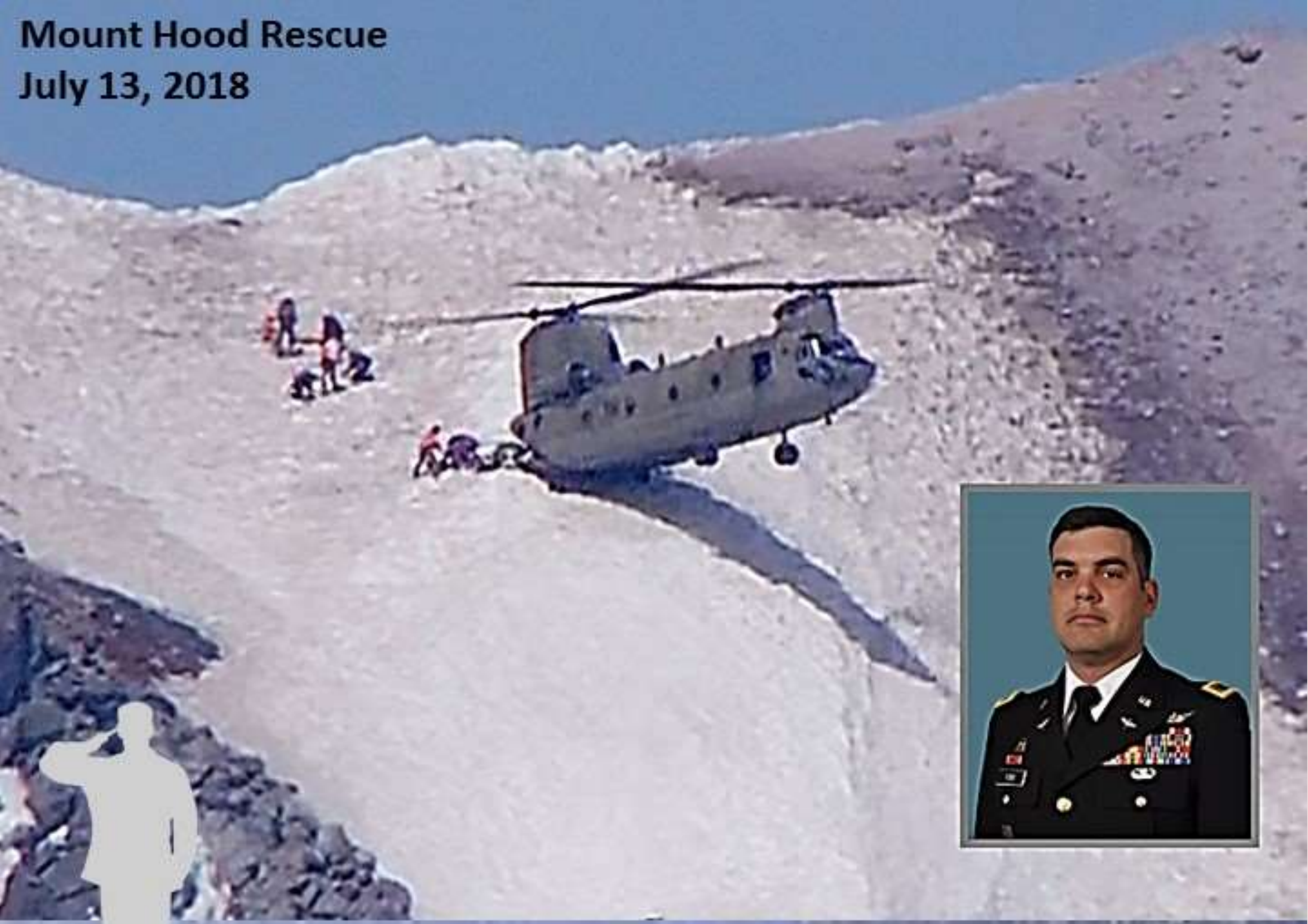
Researchers at BGU's Malware Lab are also working on an online portal where users could submit e-mails they think may be malicious and get a score on their potential maliciousness. The system would use machine learning to do so, and offer the user recommendations on what they should do with the message in question.

"In addition, the system would assist in collecting benign and malicious e-mails for research purposes which, due to privacy issues, is currently a very difficult task for researchers in this arena," says Dr. Nissim.

— Read more in Conner Forrest, "New email malware detection can outperform the top 60 antivirus engines," TechRepublic (18 July 2018).



EMERGENCY RESPONSE



Mount Hood Rescue
July 13, 2018

Afghanistan rooftop evacuation

Lessons from extreme weather events: What disasters teach us about resilience

Source: http://www.homelandsecuritynewswire.com/dr20180628-lessons-from-extreme-weather-events-what-disasters-teach-us-about-resilience

June 28 – Extreme weather events are among the most likely causes of disasters. Every dollar spent on disaster resilience saves five dollars in future losses. Post-Event Review Capability analysis helps to identify opportunities to reduce risk and build long-term resilience.

With that in mind, Zurich Insurance Group (Zurich) says it is sharing what it has learned about how individuals, businesses and communities can increase resilience to disasters. As one of the world's leading insurers, the Group believes it is appropriate to think about a holistic approach to risk, and also ways to address it prior to a disaster. This is appropriate especially now as the Atlantic hurricane season gets underway, and many countries may also face heightened risks of destructive seasonal floods.

According to the Global Risks Report 2018, **extreme weather events are at the top of the list in terms of global risks most likely to occur, and when they occur, they can be devastating.** Instances of extreme weather events might also be increasing, with September 2017 the most intense month for Atlantic storms on record.

It is important to address the risks before a disaster strikes. Alison Martin, Zurich Group Chief Risk Officer and member of the Executive Committee, notes: "We know that every dollar spent on reducing risks and their impacts before a disaster saves five dollars in future losses. That means **it's five times more expensive to be unprepared.** Building resilience is money well spent, and more importantly – it saves lives."

Zurich's says that its experience and extensive research can provide valuable insights to help mitigate risks from weather-related catastrophes. Using Zurich's Post-Event Review Capability (PERC) methodology, the Group has found there are often striking similarities among different types of hazards no matter where they occur. And nearly all disasters – floods, fires, windstorms or other events – share common traits in the impact they have on lives, property and communities. They can thus teach valuable lessons no matter what type of risks they might bring.

Zurich has led twelve PERC studies. Each one analyzes the response to natural events that turned into a disaster. The countries where the PERCs were conducted included Austria, Bosnia and Herzegovina, Croatia, the Czech Republic, Germany, Morocco, Nepal, Peru, Serbia, Switzerland, the U.K. and the U.S. These investigations identify critical gaps and promising opportunities, particularly around actions aimed at reducing risk and building long-term resilience.

Businesses can take actions based on these insights. For example, in 2010 a serious flood caused $155 million of losses to a plant of Bombardier in Bautzen, Germany. Situated near the Spree River, such flooding could easily affect the plant once again. Bombardier, with help from Zurich's risk engineering experts, began making changes to protect the site. When the Spree flooded again in 2013, the flooding caused extensive damage in the region. But Bombardier's plant was unscathed, protected by integral flood risk solutions.

"Of course, proper insurance coverage will speed recovery by providing funds quickly to aid in rebuilding. However, one of the central lessons from the PERC studies is that **businesses play a key role in building communities' resilience to large natural events so they do not turn into a social disaster.** Providing equipment, access to food and water, assisting with cleanup and offering paid time off for employees to help rebuilding can go a long way toward supporting a community and creating a culture of assistance," Martin said.

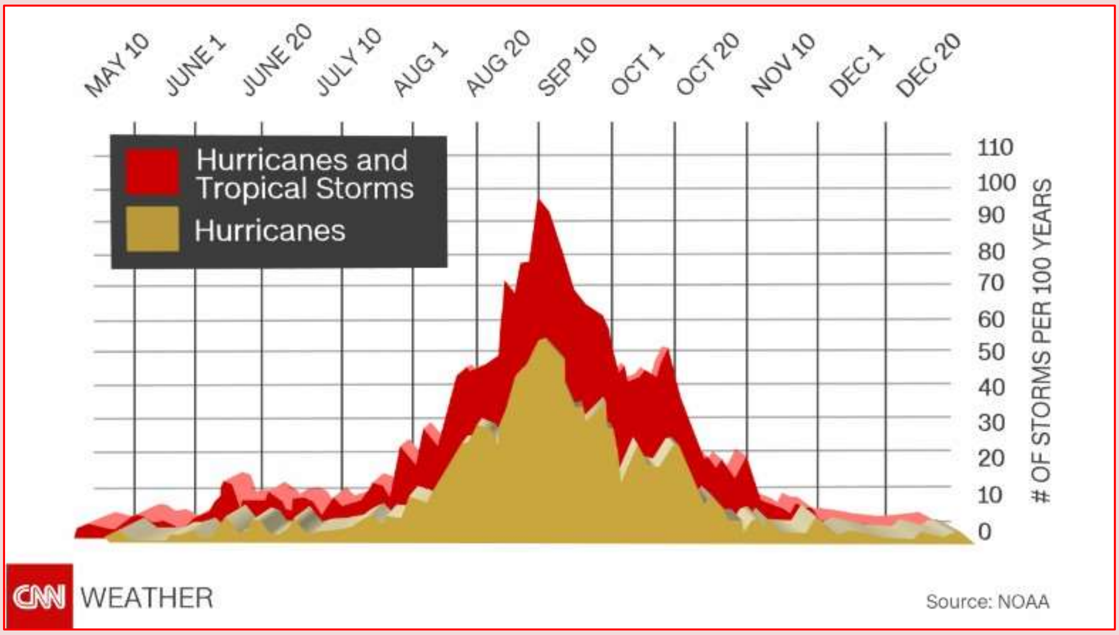
— Read more in Extreme weather events: How hard lessons strengthen resilience against the next big event. PERC studies and a manual that serves as a guide for conducting PERCs are available here.

3 reasons why the U.S. is vulnerable to big disasters

By Morten Wendelbo

Source: https://www.scientificamerican.com/article/3-reasons-why-the-u-s-is-vulnerable-to-big-disaster/

July 03 – During the 2017 disaster season, three severe hurricanes devastated large parts of the U.S. The quick succession of major disasters made it obvious that such large-scale emergencies can be a strain, even in one of the world's richest countries.



Source: NOAA

As a complex emergency researcher, I investigate why some countries can better withstand and respond to disasters. The factors are many and diverse, but three major ones stand out because they are within the grasp of the federal and local governments: where and how cities grow; how easily households can access critical services during disaster; and the reliability of the supply chains for critical goods.

For all three of these factors, the U.S. is heading in the wrong direction. In many ways, Americans are becoming more vulnerable by the day.

Where Americans live

Large shares of the U.S. population live in the parts of the country most vulnerable to major disasters, mainly coastal areas prone to hurricane damage. Hurricanes Katrina, Sandy, Harvey and Irma all hit heavily populated coasts.

Seven of the 10 largest metropolitan areas in the U.S. are on or near the coast, accounting for more than 60 million people. In fact, the vast majority of counties with more than 500,000 inhabitants are concentrated on the coast.

More than 5 million Americans also live on islands like Puerto Rico and Hawaii, where a hurricane, volcanic eruption or tsunami can be devastating.

California has been spared landfall of a major tropical cyclone, but torrential rainfall still causes severe damage along the coast. On top of this, most of California's coastal cities are adjacent to the San Andreas Fault, which caused the death of around 3,000 people in 1906. Geologists agree that another large earthquake is bound to occur.

Large concentrations of people pose problems, too. To support large populations in small spaces, cities need advanced large-scale infrastructure – not only to house people, but to deliver utilities like electricity and gas, as well as to tame water with dams, levies and spillways.

While such infrastructure is impressive, its occasional failure can have grave consequences. In several of the most severe American disasters, infrastructure collapse caused substantial damage. In New Orleans, the Lower Ninth Ward was violently flooded when levies collapsed. In the 1906 San Francisco earthquake disaster, gas mains ruptured, fueling a deadly fire that tore through the city for days.

The large cities on the coasts are consistently growing larger. The 10 largest metropolitan areas on the coast alone have grown by almost 5 million people since 2010, an increase of nearly 7 percent.

Experts project that by 2040, these 10 metropolitan areas will add a whopping 16.7 million more people, making the total population around 92.5 million people – most of whom will be particularly vulnerable to disaster.

Access to emergency funds

In a disaster, people often need money to cover medical care, food, water and other crucial needs. In a frustrating catch-22, however, access to funds can be severely limited if power outages take out ATMs and credit card terminals. That was the case in Puerto Rico after Hurricane Maria.

A 2015 Federal Reserve survey found that even with access to bank accounts and ATMs, almost half of Americans would be unable to find US$400 for an emergency without borrowing or using a credit card.

Today, there's almost three times the amount of U.S. currency in circulation as there was in 1997. But a large share of U.S. dollar bills are actually used abroad. U.S. dollars are the legal or de facto currency in many countries, as well as a preferred currency for savings around the world. Consequently, the amount of cash in circulation that is actually available to make transactions in disasters is relatively low.

The problem with access to cash to cover emergency expenses is especially acute for minority Americans. The same Federal Reserve survey showed that even for Americans with the same income, blacks and Hispanics are far less likely to have access to the $400 emergency funds than whites.

Blacks and Hispanics are also more likely to be poor than whites non-Hispanics, and poor families are far more susceptible to disasters.

Worse still, the proportion of minorities in metropolitan areas are often far above the national average, compounding the vulnerability of minorities. In fact, in all but one of the 10 largest metropolitan areas on the coast, the minority population is growing faster than the white non-Hispanic population.

Supply chains

Even if Americans do have the funds necessary to pay for critical goods, those goods may not be available during a disaster.

Without access to pharmaceuticals, medical equipment and fuels, many people would die. Many of these critical goods are exclusively produced overseas; in fact, the 30 most critical pharmaceuticals, such as insulin for Type 1 diabetes and heparin for blood thinning, are all produced in whole or in part abroad. Sometimes the goods are produced in a single geographic area or even by a single facility.

That makes the supply of these critical goods very vulnerable to natural disasters or other emergencies. If a global pandemic affects China or India as well as the U.S., there would be almost no way to source the critical goods necessary to save Americans infected by the disease.

At the same time that production of many critical goods are moving abroad, stockpiles and storage are exceptionally low for most goods. Goods often arrive at the consumer continuously, just in time for when they are needed. The rapidly growing international transportation industry can deliver quickly and reliably, leaving little reason for hospitals to spend on substantial storage of most goods.

Some U.S. hospitals receive critical pharmaceuticals as often as three times per day. On a regular day, it's possible for an efficient system to keep emergency rooms stocked, but during a disaster – when workers are absent, transportation is slowed and production abroad is potentially knocked out – Americans are left incredibly vulnerable. There's little margin for error, and that margin shrinks apace with the expansion of "just-in-time" systems.

***Morten Wendelbo** is Research Fellow and Policy Sciences Lecturer, Texas A&M University.*

Preparing for a Complex Coordinated Terrorist Attack

By Deanne Criswell

Source: https://www.domesticpreparedness.com/preparedness/preparing-for-a-complex-coordinated-terrorist-attack/

Jan 17 – **Complex coordinated terrorist attacks (CCTAs) are exactly as the name implies: large-scale attacks that are multifaceted, well-planned, and often involve multiple perpetrators.** These individuals are often unknown to law enforcement, making them difficult to identify during pre-operational planning activities. Because of their size and complexity, these types of attacks far too often have a devastating impact across jurisdictions, disciplines, and even state lines.

Needless to say, responding to a CCTA attack is highly complex, creates confusion, and is difficult to know what will happen next. Preparation begins with the local patrol officer and must expand to include the whole community. The best way to prepare for, and respond to, a CCTA is to think outside the proverbial box – as well as outside the lines of traditional jurisdictions, disciplines, and states. CCTAs require a whole community response, with decision-making before, during, and after this type of event being a collective effort. Coordination is paramount.

Simply knowing where to start can be a challenge for communities to establish coordination and create a collective response. Challenges can also occur when working across disciplines and jurisdictions – particularly when each is "in charge" of its own community and operations. To help with the preparedness process, the steps are mapped, challenges identified, and solutions provided to aid emergency managers in creating the community response necessary for an effective CCTA response plan.

Step 1: Bring the Community Together

One of the first, and most important, steps is to bring the whole community together. CCTA preparedness activities must be tailored to each jurisdiction and account for complex and evolving terrorist tactics, techniques, and procedures. The solution will not be found by utilizing a government-centric approach. It will require coordination from the entire community. Start by contacting established relationships – those who are already involved. Then include stakeholders from other jurisdictions and disciplines, as well as law enforcement, hospitals, and firefighters. Define the role that each stakeholder plays and determine the resources that each organization could provide.

After establishing the baseline, think about what might be missing. For example, consider including nonprofits such as the Red Cross, government agencies, local military installations, and community stakeholders outside the emergency management community, such as academia and the private sector. **This is a lot of people to invite to the planning table.** However, through this approach, everyone who may have even the smallest role is invited to participate. The result is a collaborative planning process that gains stakeholder buy-in, fosters new relationships, and encourages open communication.

Step 2: Identify Gaps

Once everyone is at the table, the next step is to conduct a gap analysis to identify: what is missing; strengths and weaknesses of the entire plan (in training, exercising, and personnel); and any skill-set short falls. Because most jurisdictions have not experienced a CCTA event, it is imperative that there is also a review of past events – after action reviews, best practices, and/or capabilities – and how they might apply to a specific jurisdiction. This is also a good time to identify policy gaps, such as mutual aid agreement and communications plans. One of the greatest challenges in cooperation across jurisdictions and disciplines is **successful communication**. Each group has its own well-established methodologies, yet a joint effort requires agreement on a single solution that may be different than some groups are accustomed to. Discuss topics such as communication protocols, communication frequencies, back-up communication methodologies, and who will take the lead on communications efforts.

Step 3: Plan How to Work Together

With a room full of leaders, it may be challenging to determine who will have which responsibilities – that is, developing an understanding of how a multidisciplinary, multijurisdictional response will come together. When planning for a CCTA at the Office of Emergency Management for the City of Aurora, Colorado, a core group of stakeholders from multiple disciplines actively discussed the pros and cons of different response scenarios. The group discussed how to move forward in each scenario, who was trained for which types of event, and the best solutions.

For example, the group determined that, in an active shooter scenario**, the best course of action would be to have the paramedics enter with the SWAT team to neutralize the threat while treating potential victims.** Different scenarios saw different approaches based on training and skillsets. Every jurisdiction has unique needs; therefore, multiple scenarios should be planned with the understanding that different events may require different approaches. The more conversation and planning, the better.

Step 4: Train & Exercise

Planning and reality are dramatically different. Although planning can occur years in advance, reality almost never mimics that plan. The best way to truly understand preparedness levels for a CCTA is to train and exercise – specifically, cross-disciplinary training:

- **Train to multiple scenarios.** Even the most outlandish scenarios can become real, and the more outlandish, the greater the threat. Plan for the unexpected.
- **Train across disciplines and jurisdictions**. The goal is to use cross-discipline and cross-jurisdictional resources to thwart a potential CCTA. The only way to know if a plan will be successful is to conduct trainings using all the resources involved in the plan. Training piecemeal does not work.
- **Most importantly, train to failure.** As a former colleague from the City of Aurora would often say, "a training exercise that goes perfectly had a really bad design."

Although communities hope never to experience a CCTA, they should all be prepared for the possibility in a way that is specific to a CCTA-type of incident. A complex, coordinated incident requires an equally complex, coordinated response. It requires the whole community; it requires careful attention to potential pitfalls or gaps in the plan; and it requires training and exercises that go beyond the routine and scale to the size of a potential large, complex, coordinated incident.

Deanne Criswell *has more than 25 years of emergency management experience, including federal, military, and local government response to complex incidents and disasters. She served as the leader of one of the Federal Emergency Management Agency's (FEMA's) National Incident Management Assistance Teams (N-IMAT). She also served in the National Guard, and was the manager of the Office of Emergency Management for the City of Aurora, Colorado, where she led strategic change in the city's emergency and disaster planning. She currently serves as principal in the homeland security sector for Cadmus. She is a certified emergency manager by the International Association of Emergency Managers.*

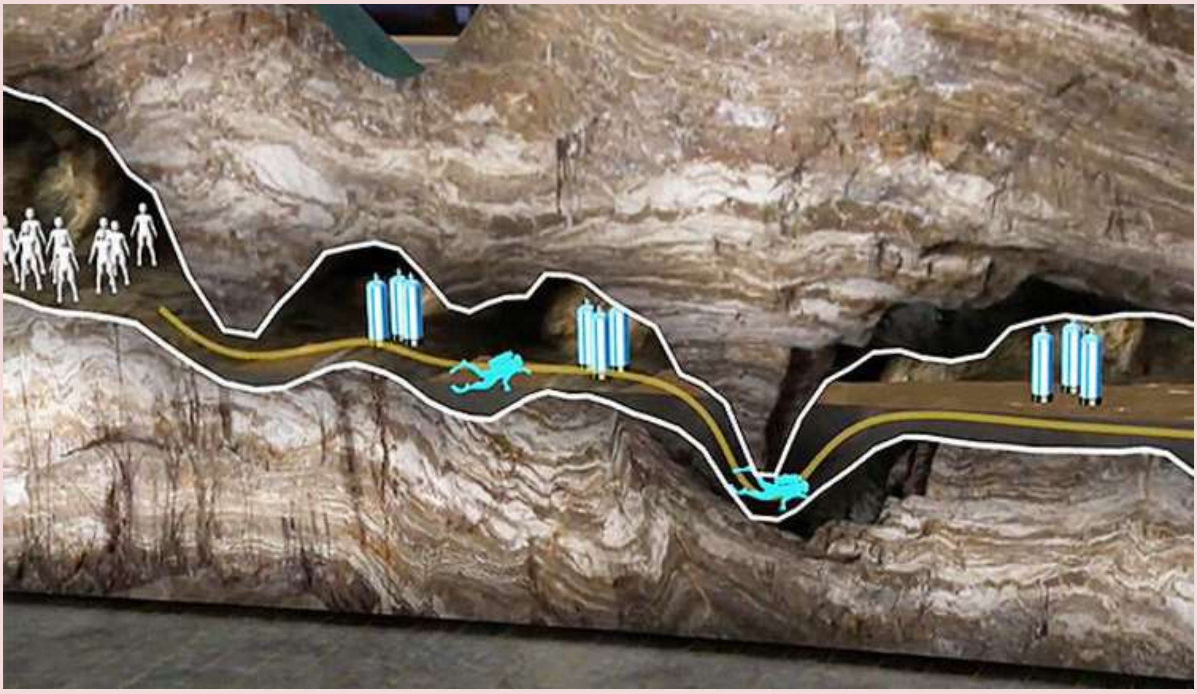
How does it Work? Israeli Communication Tech that Supports Thailand Rescue Operation

Source: https://i-hls.com/archives/84010

July 06 – Emergency mobile communications technology developed by an Israeli company is being used by rescue teams working to save 12 teenagers and their coach trapped in a flooded cave in Thailand.

The lack of communication between first responders has been a challenging problem. Shortly after the boys went missing, the Thai naval special forces contacted Maxtech Networks' agent in Thailand. The company engineer equipped with 17 of the company's emergency Max-Mesh radio units, without charge, immediately arrived at the site to help train the first responders how to use the technology, according to .israel21c.org.

Maxtech's device looks like a simple walkie-talkie, but has sophisticated software algorithms that allow users to communicate with each other up to more than 3 kilometers.



According to the company, "any country in the world that has a rescue team needs to have such a system in their hands. It's not a matter of choice, it's a matter of saving lives".

The Max mesh professional mobile radio is a software layer that effectively combines the advantages of fixed mesh and mobile dynamic ad-hoc networks, based on the end unit for voice, data and video applications, according to the company website.

The system automatically adapts to varying network conditions, degrees of client mobility, and relevant RF environmental conditions on a packet-by-packet basis, creating a virtual infrastructure with a powerful, ad-hoc, self-healing and self-routing multi-user network.

These features, along with a very effective bandwidth allocation method, enable the deployment and operation of true mesh networks with high performance and low costs.

The max mesh core is a breakthrough software algorithm that enables all mobile radios and communication devices to become part of a Mobile Ad Hoc Network (MANET). The technology is centered on an optimized and proven hybrid routing algorithm that combines both proactive and reactive routing techniques to enable a highly scalable network solution.

Greece wildfires: At least ~~20~~ 52 killed near Athens as residents and tourists flee

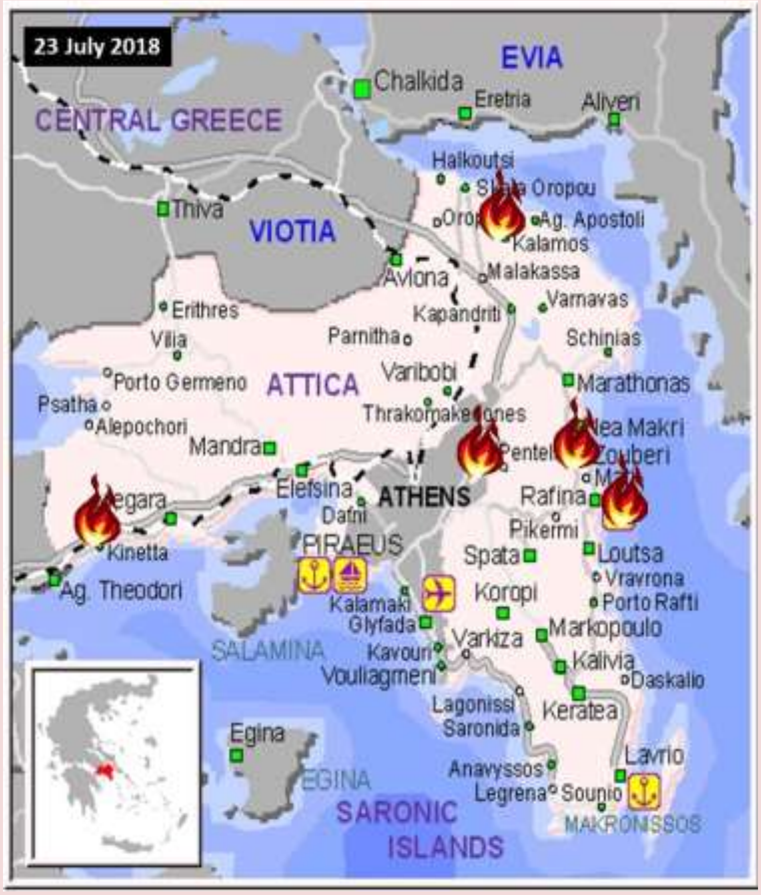
Source: https://www.telegraph.co.uk/news/2018/07/24/greece-wildfires-least-20-killed-near-athens-residents-flee/

July 24 – The worst Greek forest fires in a decade killed more than ~~20~~ 52 people near Athens on Monday while scores of others were injured (11 critical/intubated).

The fire in Mati village, 18 miles east of Athens, was by far the country's worst since blazes devastated the southern Peloponnese peninsula in August 2007, killing dozens.

Monday's fire, which sent residents and tourists scrambling to safety, was one of several that broke out in the country amid a sweltering heat wave, with authorities declaring a state of emergency in the western and eastern parts of Attica.

"Mati doesn't even exist as a settlement anymore," one woman told Greece's Skai TV. "I saw corpses, burned-out cars. I feel lucky to be alive."



Mati is in the Rafina region which is popular with local tourists, particularly pensioners and children at holiday camps.

A woman walks in front of burnt cars at the village of Mati during a wildfire near Athens Credit: AFP

As the fire still raged and darkness fell, the extent of the disaster was impossible to gauge.

"We are dealing with something completely asymmetric," Greek Prime Minister Alexis Tsipras said after cutting short a visit to Bosnia.

"It's a difficult night for Greece," he added.

Flames rise as a wildfire burns in the town of Rafina, near Athens Credit: AFP

Dimitris Tzanakopoulos, a government spokesman, said more than 20 people had died, the majority of whom were found in their homes or cars in Mati.

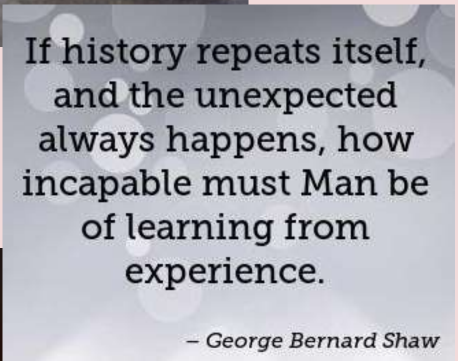
More than 104 were injured, he added, including 11 seriously. There were 16 children among the injured, he said.

One of the youngest victims was thought to be a six-month-old baby who died of smoke inhalation.

I will survive!

Mati, Attica 2018 wildfires

Greek authorities were rushing to evacuate residents and tourists stranded on beaches in coastal areas early on Tuesday.



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

– George Bernard Shaw

Dozens of people scrambled into the ocean as the blaze raged close to the shore, and they were picked up by passing boats.

Nine coastal patrol boats, two military vessels and "dozens of private boats" assisted by army helicopters were mobilised to help those stuck in Rafina harbour.

A house burns in the town of Mati, east of Athens Credit: AP

Greece issued an urgent appeal for help to tackle fires which raged uncontrolled in several places across the country, destroying homes, disrupting major transport links and sending people fleeing for their lives.

Greece said it needed air and land assets from its European Union partners. Cyprus offered to send fire engines and personnel.

The first major fire broke out in a pine forest near the seaside settlement of Kineta, 30 miles west of Athens between the capital and Corinth. At least 220 firefighters were on the scene there while five water-dropping planes and seven helicopters helped to fight the blaze from the air. Reinforcements were sent in from across Greece.

A senior fire chief went on state TV to appeal to people to leave the area after some tried to stay on their properties.

"People should leave, close up their homes and just leave. People cannot tolerate so much smoke for so many hours," Achilleas Tzouvaras said. "This is an extreme situation."

The second major blaze broke out Monday afternoon in the Penteli and Rafina areas northeast of Athens. Children's summer camps and a seaside resort for military officers were evacuated, as well as residences in the area. Dozens of homes and cars were reportedly destroyed.

There was no official figure on how many people were evacuated overall.

The fire was burning into the town of Rafina, turning the sky above the nearby port that serves ferries to the Cycladic islands black from the smoke.

Witnesses reported seeing a hillside of homes gutted by flames east of Athens. A mayor said he saw at least 100 homes and 200 vehicles burning.

Greek authorities urged residents of a coastal region west of Athens to abandon their homes as a wildfire burned ferociously, closing one of Greece's busiest motorways, halting train links and sending plumes of smoke over the capital.

Wildfires are not uncommon in Greece, but a relatively dry winter created tinder box conditions. It was not clear what ignited the fires.

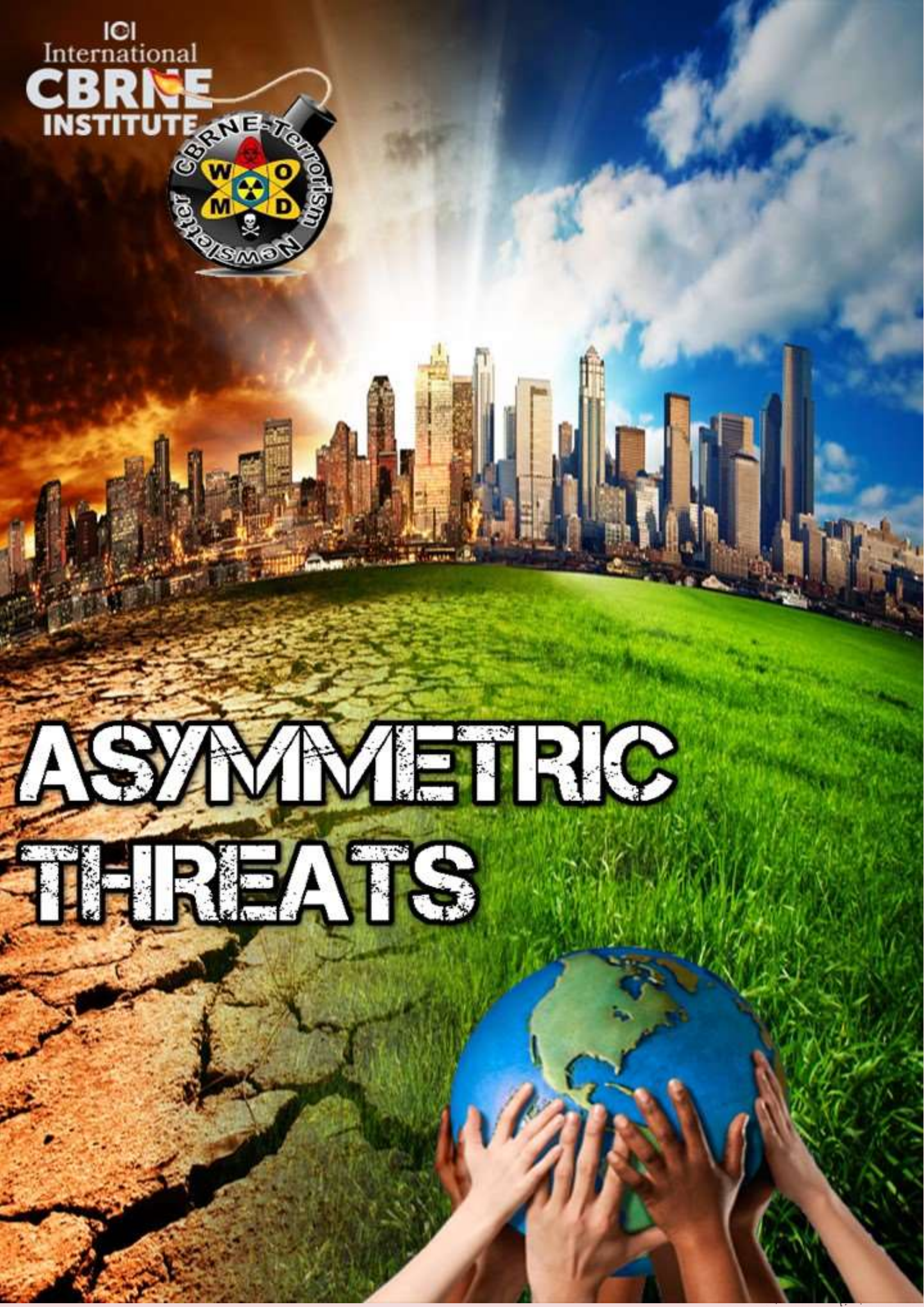
The main Athens-Corinth motorway, one of two road routes to the Peloponese peninsula, was shut and train services were cancelled.

Fire raged around the Saronicos Gulf, ravaging tracts of pine forest, and was visible for miles. An ominous cloud of black-orange smoke hung over the Acropolis hill and the Parthenon temple in Athens on Monday afternoon.

Cars are blocked at the closed National Road during a wildfire in Kineta Credit: AFP

Several other fires broke out across the country, including in northeastern Greece and the southern island of Crete, stretching Greece's firefighting capabilities. Gale force winds that frequently changed direction and continued into the night were hampering firefighting efforts.

EDITOR'S COMMENT: Same old story al long as I can remember (60 years) – myself a victim in 2010 in one of the wildfires that from time to time hit Attica. Two main conclusions and one assumption. **The first** is the fact that there is no plan to handle megafires. Existing technologies (i.e. drones; sensors; satelites etc.) cannot bit human mentality and the perception that it will not happen to our territory. One more time it was proved that fire operations are too heavy for the fire service and the military should be involved in the early stages**. I am not talking about the heroic field fire men and women**; I am talking about officers in high places that they know all about water but not about strategic approach of wildfires. And the military know better – this is what they do. Now it is a good opportunity to change but I think that is two or three weeks the whole thing will be forgotten until then next August 2018 fire. **The second** is the combined responsibility of citizens and local perfectures nation-wide. For example, you cannot rely on the good will of people to cut the dry grass in and around of their properties. So they do it; others do not! Here comes the prefecture and make it mandatory with heavy penalties if you do not comply. I am sure that in just a few years citizens will learn (the hard way) that they have to protect their space and all together their communities. On the other hand, perfectures should clean side roads and remove existing biomass under small pine forests here and there; clear the emergency forest roads; map their areas and who is living where (in 2010 not a single person came to help us fight the fire and in the aftermath nobody care if we were still alive), etc. If you put these two together then a fire is so easy to happen. Was it a case or **pyroterrorism**? I could say yes. But the problem is that you cannot prove it if you do not catch the arsonists on the spot and confess their motivation and origin/organization. But if you think the position of Greece in the map and study its relations to close neighbours certain concutions might pop-up. I made same assumptions in 2017 and I almost got fired from my organization.



ASYMMETRIC THREATS

Dangerous climate change is likely: Study

Source: http://www.homelandsecuritynewswire.com/dr20180628-dangerous-climate-change-is-likely-study

June 28 – A new study has revealed sensitive regions of the world are still at risk from the dangerous and potentially irreversible effects of climate change; even if we meet the target of not increasing global temperature above 1.5°C over the next 100 years.

The research, led by The Open University in collaboration with the University of Sheffield, reviewed the targets set in the 2015 Paris Climate Agreement and concluded that regions of the world, such as the Arctic and South-East Asian monsoon region, could be damaged irreversibly as they are particularly sensitive to changes to global temperatures.

The international team of researchers developed a three-dimensional climate-carbon cycle model, and simulated the different climate futures.

Dr. Philip Holden, Lecturer in Earth Systems Science at The Open University and lead researcher of the study, said: “The regional uncertainties associated with the Paris Climate Agreement have not been explored before. This is because, until now, researchers have used either very simple models or models that were too complex to investigate the range of possibilities.”

Sheffield says that on a more optimistic note, the research also concludes that meeting the target set by the 2015 Paris Climate Agreement of limiting the increase in global average temperatures to well below 2°C does not depend on future generations to remove vast amounts of carbon from the Earth’s atmosphere.

Instead, governments can achieve the goals through emission reductions, but only if they act now to promote a range of policies to fully support the existing pace of technological change, as described in a related paper in *Nature Climate Change*.

New study

“Our models show that it is possible to meet the 2015 Paris Agreement, but only if governments take decisive and urgent action through strengthening climate change policies to encourage rapid divestment from fossil fuels,” continued Holden.

Professor Richard Wilkinson, from the University of Sheffield’s School of Mathematics and Statistics (SoMaS) and contributing author, said: “By accounting for climate-carbon cycle uncertainties we have been able to show that there is an approximate 50 percent probability that we can limit peak post-industrial peak global warming to less than 1.6 degrees Celsius.

“This has been made possible by using Gaussian process emulation to find plausible climate trajectories at a fraction of the computational cost”

— Read more in P. B. Holden et al., “Climate–carbon cycle uncertainties and the Paris Agreement,” Nature Climate Change (25 June 2018).

Snow Job: Iran accuses its enemies of “stealing clouds” to create drought

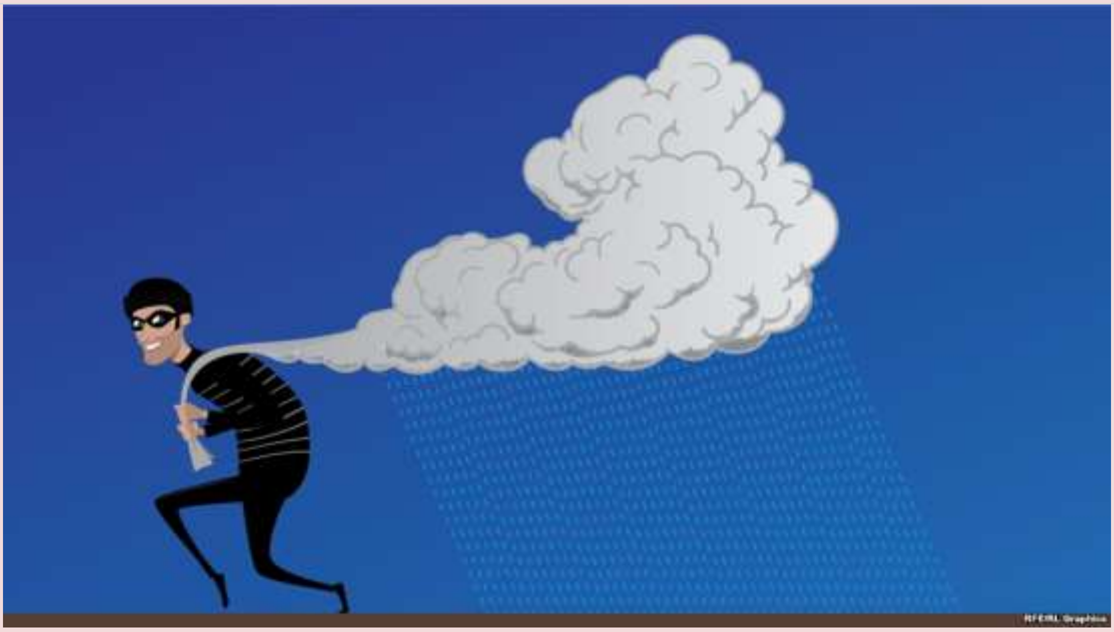
Source: http://www.homelandsecuritynewswire.com/dr20180703-snow-job-iran-accuses-its-enemies-of-stealing-clouds-to-create-drought

July 03 – A senior Iranian official has accused Iran’s foreign enemies, including Israel, of modifying the weather in the country in order to create drought.

“Foreigners are suspected of intervening in the country’s climate,” Gholamreza Jalali, the head of Iran’s Passive Defense Organization, a subdivision of the armed forces, said on 2 July in the Iranian capital, Tehran.

He made the remarks at an event focusing on agriculture amid recent protests over water scarcity in the southwest of the country. In the past few days, residents have taken to the streets to demonstrate against shortages of drinking water.

Jalali claimed that a study conducted by “scientific centers” in Iran had confirmed that the weather had been modified by outsiders.



“Over the past four years, the highlands from Afghanistan to the Mediterranean have been studied. The findings are that areas above 2,200 meters were full of snow but our highlands have remained dry,” he said.

“Joint teams from Israel and one of our neighboring countries make clouds that are entering Iran” and which are unable to produce rain, Jalali added. He did not specify which neighboring country he was referring to.

“In addition to that, we have the issue of ‘cloud-stealing’ and ‘snow-stealing,’” he was quoted as saying by domestic media, but he did not give any further explanation or present any evidence.

His claim was dismissed by an official from the country’s Meteorological Organization, who said that “it was not possible for a country to steal snow or clouds.”

Ahmad Vazifeh, head of the weather forecasting and warnings unit at the Meteorological Organization, said he wasn’t aware of the study Jalali was referring to but said that the country has, indeed, been hit by years of drought.

“Iran has been facing continuous droughts. This is a worldwide trend,” Vazifeh told the semiofficial ILNA news agency, adding that Iraq, Turkmenistan, and a number of other countries are also suffering from lack of rain.

Vazifeh said Jalali’s comments distract the country from seeking real solutions to the problem.

Experts have blamed climate change and also mismanagement for the water crisis in Iran, where over the past few months there have been several protests around the country over water shortages.

Iranian officials have identified the crisis as a national-security issue.

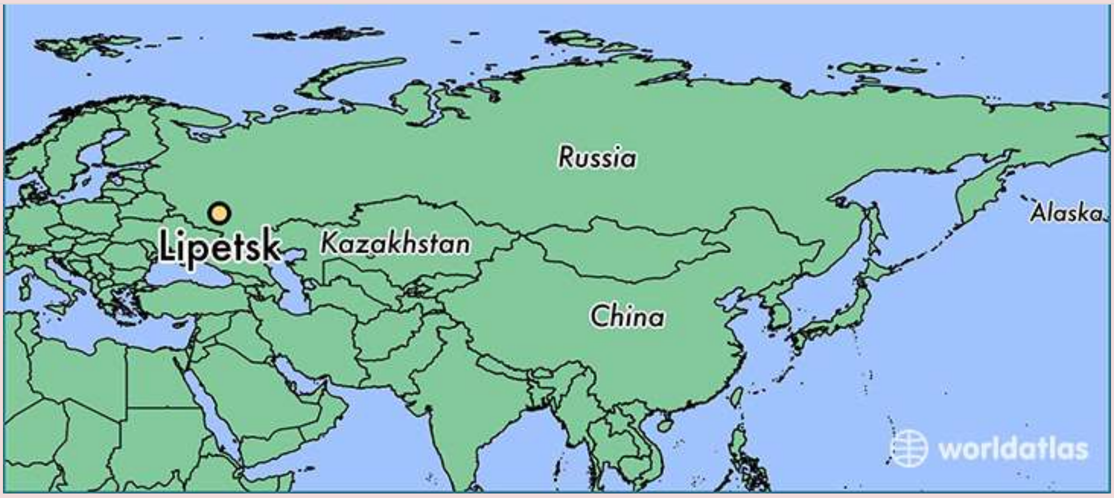
Meteoroid explodes over Russian city without warning

Source: http://www.homelandsecuritynewswire.com/dr20180703-meteoroid-explodes-over-russian-city-without-warning

July 03 – A meteoroid exploded over the city of Lipetsk in western Russia last week without warning, lighting up the summer sky with a bright flash. While some enjoyed the light show, others are worried that we didn’t see it coming.

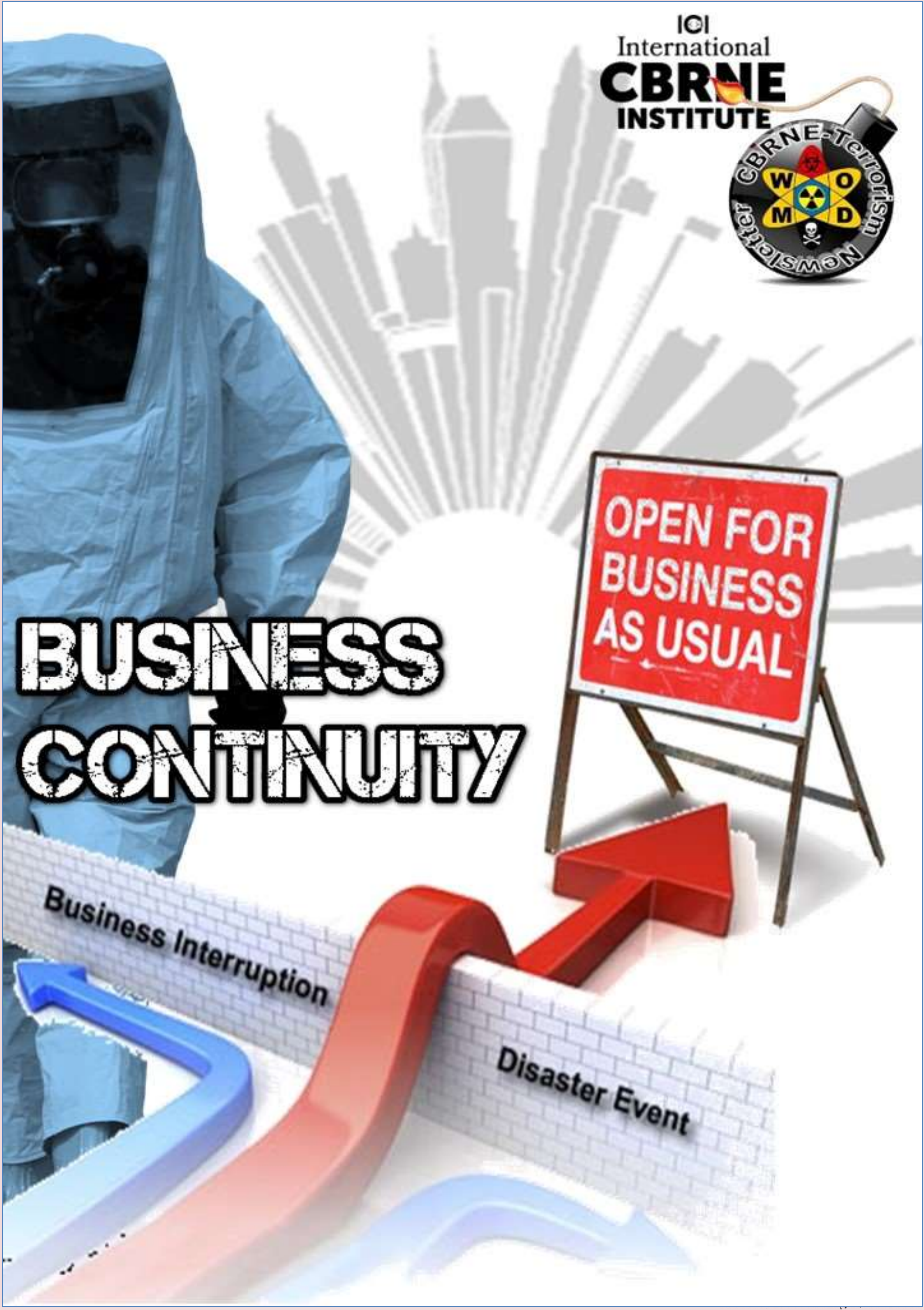
NASA is part of an international effort to detect objects that enter our atmosphere from space, but they generally only see larger objects. Meteoroids with a diameter of less than 20 feet or so are unlikely to cause any harm, so it isn’t really necessary to keep an eye on them.

“We didn’t see this one coming because it was just too small,” said Jay Melosh, a professor of earth, atmospheric, and planetary sciences at Purdue. “The meteoroid that exploded over Chelyabinsk, Russia in 2013 and caused a lot of damage on the ground was around 60 feet wide. The one that exploded last week was only about 15 feet.”



Purdue notes that the danger from an incoming asteroid of this size isn't that it will crush buildings or people (although falling meteorites have occasionally done that), but the shock wave from the explosion, which can be comparable to a small nuclear explosion.

Meteoroids of this size are fairly common, plunging toward the Earth about once a year. Because an object of this size doesn't pose any real danger, this is more of an opportunity for collectors to pick up fallen pieces of debris, Melosh said. Although the meteoroid disintegrated before reaching Earth, some small pieces might be lying around the region near the explosion. Pieces of freshly-fallen rock can be valuable to both collectors and scientists and are often sought by meteoroid hunters along the projected path of such a fireball.


International CBRNE Institute
CBRNE-Terrorism Newsletter
W O M D
BUSINESS CONTINUITY
OPEN FOR BUSINESS AS USUAL
Business Interruption
Disaster Event

Latest Strategic guidance on Building decontamination for CBRN

Source: http://www.continuityforum.org/content/page/latest-strategic-guidance-building-decontamination-cbrn

This document replaces guidance published in 2004 by the Department for Environment, Food and Rural Affairs, and the Office of the Deputy Prime Minister (now the Department for Communities and Local Government).

An incident, whether deliberate or accidental (HazMat), involving chemical, biological, radiological or nuclear materials can potentially lead to the loss of life, contamination of the built and open environment, disruption of society and consequential damage to the UK economy. It is therefore important that plans are in place to minimise the effects of such an event, and to plan for recovery following this type of incident.
This guidance builds on the 2004 documents, and offers improved signposting and updated information in a shorter and more accessible format. It also covers key elements in the decontamination process following an incident – from developing the initial recovery strategy through to managing waste and returning things to normal.
The principal roles and responsibilities of key organisations have been identified and listed, and planning and precautionary measures have been highlighted to promote better preparedness.
In view of the different types of potential incidents, and the variety of buildings, environments and infrastructure that could be affected, the guidance in this document is necessarily generic. It provides a starting point for the development of more detailed contingency plans to deal with specific incidents. This document also describes the current legal powers available to local authorities in the event of such an incident.

Evacuate or Shelter in place?

Source: http://www.continuityforum.org/content/news/2009/11/evacuate-or-shelter-place

From a Business Continuity or Emergency Planning perspective is it better to evacuate people in the vicinity of a serious chemical fire or should they remain where they are?
A study* comparing the health outcomes in sheltered and evacuated populations after a chemical fire suggests that there are health advantages in people sheltering rather than evacuating. The study is published in the BMJ and was based on a real incident in 1999. It involved collaboration between public health staff at a local health authority and national health experts (now at Bristol University and the Health Protection Agency).
In the event of a serious chemical incident where the public may be exposed to smoke from a fire, two main options of protective action exist - sheltering or evacuation. The prevailing expert view is to shelter, based largely on experimental and modelling studies.
This new study published in the British Medical Journal looks at a typical business continuity challenge, a fire started in a factory manufacturing plastic goods in southwest England. The factory was situated on an industrial estate adjoining a large residential area.
The initial response of the emergency services was to begin evacuating residents from their homes to a nearby leisure centre. This decision was subsequently reviewed and residents were advised to stay inside their homes and shelter. The resultant partial evacuation offered a rare opportunity to compare the relative health protection offered by these two modes of intervention.
A postal questionnaire survey was carried out on residents in the affected area and compared the health outcomes among the people evacuated (one third) and sheltered (two thirds).
In the two groups of residents similarly exposed to smoke plume from the chemical incident, the survey showed that evacuation did not confer any additional health benefit over sheltering. If anything, evacuated residents seemed to have more ill health effects soon after the incident than sheltered residents, although the difference did not seem to persist beyond two weeks.
Although the study has its limitations, it is a comparative study based on a real incident. The results reinforce the prevailing expert view that favours sheltering over evacuation as a response to protect populations exposed to chemical air pollution incidents. It is consistent with UK policy and practice in dealing with emergencies.

** Kinra S, Lewendon G, Nelder R, Herriott N, Mohan R, Hort M, Harrison S and Murray V, (2005). Evacuation decisions in a chemical air pollution incident: cross-sectional survey. BMJ, 330, 1471-1474.*

FORUM COMMENT

For some time the evidence has been mounting for the benefits of 'Shelter in Place' (SiP) as opposed to evacuation for incidents of this type.

The latest Expert advice from Government currently recommends the value of SiP as a viable and effective alternative to evacuation for the management of local incidents based on, real life experience gained under a variety of circumstances. Currently, there is a belief that, on balance, for many types of incidents the difficulties of a even a minor evacuation expose those in the affected area to greater health risks than SiP.

The issue that this raises for those working in the BC arena is twofold, firstly, understanding your local risks, and secondly, ensuring that your planning is connected with that of the Local Authority and Emergency Services and that the decision to Shelter in Place can be effectively communicated to those on-site, particularly as employees and visitors may be anxious, or even panic when faced with the reality of an incident.

Potential Third Party risks, such as a Plastics or Chemical Factory in the general vicinity of your site/s should feature in the risk assessment/BIA of the BCP highlighting the location and type of facility, along with any other details that may be needed quickly in the wake of an incident. Local liaison is vital too, discuss the local plan for the management of any incident and ensure that there is a clear connection between YOUR response and that of the Emergency Services. Local Authorities should be able to provide detailed advice, and facilitate discussions with other services such as the Local Fire Service and Police should additional detail or measures be needed as there may be specific measures that need to be introduced such as turning off Air Conditioning Systems, which could compromise the benefits of SiP.

Remember though that plans can change and it is important to check back regularly to ensure your planning is still in tune with your local partners. It also pays to check quickly exactly what you are dealing with especially in built up areas and City Centres where the source may not be immediately clear.

Decontamination following a CBR Event

Source: http://www.continuityforum.org/content/news/2009/10/decontamination-following-cbr-event

The planning for business continuity and disaster recovery post CBR chemical biological radiological is often ignored or even potentially worse, incorrectly assessed. This assessment can be assimilated as that of a hazard assessment when the risk manager doesn’t know of combined or symbiotic effects. Post CBR planning may be difficult to assess due to limited knowledge, experience or facts but various information is available on which to assert assumptions.

This article attempts to alert the planner to some elements that should be considered.

Insurance

The backbone of all historic plans, where risk appetite is assessed and shortfalls in acceptance are covered by insurers. Insurers with a wealth of experience simply balance profit by subtracting possible cost against premium. The terrorist cover available to cover IRA type bombings saw premium rates hiked by several percent to accommodate or spread all risks and profits amongst all business policies.

The IRA type terrorists provided known risks and known or estimated costs to restore affected buildings with ample contractors but what of CBR contamination.

TRIA the UK equivalent of Pool Re (Terrorist Risk Insurance Act 2002) signed by President Bush was intended to provide a temporary insurance cover for America until such time as US insurers assessed premiums, but American insurers refused to offer insurance as they probably estimated premiums could not possibly cover estimated claim costs.

The American insurance industry has some first hand experience of CBR and decontamination costs. The Hart building and Brentwood mail handling facility saw decontamination take two years and cost over $130 million. That was from just two letters containing anthrax, and the Brentwood facility, which absorbed most of the cost, only had the letters pass through unopened.

Pool Re in the UK backed by the government has said they will insure against terror event. The term terrorist event may be extremely loose and cover may not be as global as advertised.

Take for example a dirty bomb release. The RDD radiological dispersion device is detonated and wind shift carries contamination through 360 degrees. You notice the expected contamination plume so often described as the "Hot Zone has been replaced by non directional spread, a symptom or the urban environment.

Your building wasn't obviously affected by blast but it may suffer secondary contamination. Apart from the initial reaction not discussed in this paper you have left the building and now require employees to return to work the following day, week, month even year. You may wish to get a clearance certificate to satisfy H&S, insurance or simple employee or Union concerns. Who will undertake this, who will provide a guarantee of safety, who would have suitable insurance to provide a safety certificate? What of secondary aerosols which is where contamination (dust) is moved by air movement and this may contain radiation and enter your building days or weeks after the event or indeed the clearance inspection?

A huge potential liability for clearance certification and employers. Would Pool Re pay for this inspection, investigation? The answer is nobody knows, at some point they must say you were outside the probable contamination "Hot Zone" but where is that and who assessed it?

Contamination events are known and expected to travel and affect people miles from the detonation or release area. Chernobyl for example spread across all of Europe,

The building survey alone could take weeks, how would you pay employees, manage your business, fund secondary locations. How many seats and weeks/months have you purchased from your Hot Site provider? Many questions exist regarding Pool Re and other insurance policies; many will not be answered until case law is established possibly years after the terrorist event. Could you survive long exclusion from your property? Could you afford to pay for decontamination if your policy excludes it?

You should be aware that many policies already exclude contamination; even mould is excluded from many water damage claims. The cost of decontamination as we have already seen in the US is likely to be uneconomical in most buildings and therefore the leasehold and freehold liabilities or values must be re-assessed. How many companies faced with compound uninsured losses in excess of tens of millions could survive?

Government Assistance

The government have recognised the potential problems regarding decontamination and launched the GDS Government Decontamination Service. Fully operational on the 16th October 2005 their mission is to provide a directory of suitable contractors and consultants to oversee the decontamination of public or government buildings.

The GDS require the appointed private sector companies to fully equip and become available for a possible event or training on a annual or perhaps three yearly contract but without retainer. This wish list may require substantial investment from competing companies with no guarantee of return and it's success is likely to be limited unless changes in the procurement process are made. The carrot is the belief that contractors can charge what they want as long as it is reasonable. These words still echo from the foot and mouth epidemic where contractors provided cleaning and sanitation works at exorbitant costs only to find no payment forthcoming as contracts were disputed after the event.

The experience following the outbreak of Foot and Mouth should also be learnt from. The Foot and Mouth outbreak followed almost exactly the parameters of the 1967 outbreak, but of the lessons of that outbreak were acted on and the infection spread across the whole of the UK and resulted in a bill which cost the UK Billions! Contamination may not just affect people and buildings. CBR contamination may spread as witnessed with Chernobyl and affect livestock and crops too.

Following the various CBR incidents there (Brentwood Hart buildings) the American Government found many expected decontamination procedures were not effective. Many high tech solutions ranging from Chlorine Dioxide to Thermal fogging were utilised to varying effects but generally hard work and simple cleaning coupled to audit procedures provided the best results.

The GDS is promoting decontamination procedures that must be seen as doubtful even before use. The British recommendations include the sand blasting of buildings, unfortunately for neighbours their building is likely to be cross contaminated and even worse blasting is likely to push contamination into the building envelope. Sand blasting unless at very high pressure is extremely slow and cost factors may be challenged when the time line to completion is assessed.

Spraying bleach is another recommended procedure that is unlikely to have any affect other than create toxic clouds and pollution run off. These and other decontamination procedures can be seen and should be considered in the DEFRA Strategic National Guidance published in March 2004.

When you assess the likely response from the GDS you might be concerned that they will accept no liability whatsoever for the actions or failures of the contractors they propose, (not recommend). This places the liability directly onto the shoulders of the hiring local authority. They must therefore be capable of assessing the competence and costs of the proposed contractors. Without training or guidance, these employers (local authorities) under the H&S at Work 1974 regulation 3 may be seen as liable for their actions too and the CEO may even face personal prosecution.

Decontamination of each building is likely to take months and therefore huge strains on the local economy and business district should be considered.

There may be a shortage of available contractors and the new CCA civil contingencies act has removed the likelihood of commercial availability. The CCA has specifically stated that any commercially available resources can be commandeered for use by government authorities. While this could be seen as beneficial to the country, it will prevent commercial organisations setting up contracts for possible contamination events as they would most likely have equipment & employees confiscated, with no recourse or indeed right to appeal.

Contamination spread

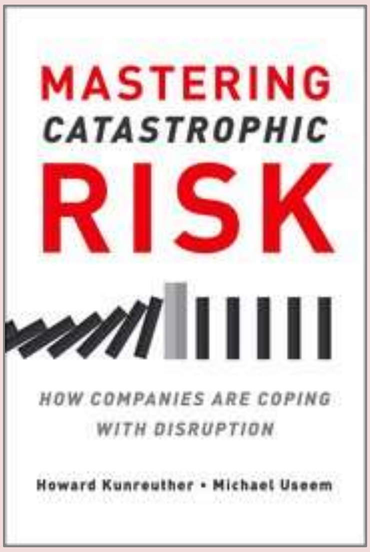
Contamination will continue to spread, known as secondary aerosolisation days and weeks after the initial release depending on the agent released. Although plumes are constantly discussed regarding safe direction upwind etc, the reality is that in the urban environment wind speeds vary so much and building shapes, height and other factors result in swirls and constant directional changes, as wind simply bounces off other buildings. These swirls constantly change the direction in which contamination will travel and unless wind speeds reach 25 Km plus the contamination should be expected to have little or no direction. This means that almost any building could be affected and contaminated, requiring clearance today or tomorrow unless controls are installed.

Facing “a new era of catastrophes,” book by Wharton profs offers tips for business leaders

By Lauren Hertzler

Source: http://www.homelandsecuritynewswire.com/dr20180703-facing-a-new-era-of-catastrophes-book-by-wharton-profs-offers-tips-for-business-leaders

July 03 – For firms large and small, with each day comes a new possibility for disruption. Perhaps there’s a natural disaster, a terrorist incident, or an economy-wide shock, like the 2008 U.S. financial crisis. Threats can emerge within a firm’s own walls, or through a government regulation, or even come in the form of a technological breakthrough—overturning business models that have been in place for years.



MASTERING
CATASTROPHIC
RISK
HOW COMPANIES ARE COPING WITH DISRUPTION
Howard Kunreuther • Michael Useem

No matter the cause, there’s little doubt about the trend: The country, and world, face “a new era of catastrophes,” says Howard Kunreuther, the James G. Dinan Professor at the Wharton School and co-director of the Wharton Risk Management and Decision Processes Center. Kunreuther, along with Michael Useem, the William and Jacalyn Egan Professor of Management at the Wharton School and the director of the school’s Center for Leadership and Change Management, recently published *Mastering Catastrophic Risk: How Companies are Coping with Disruption*. The book showcases what Useem calls the “hidden story” within S&P 500 companies that have ramped up risk-management after being overcome by their own worst-case scenarios, including catastrophes like the 9/11 terrorist attacks, Hurricane Katrina in 2005, the financial crisis of 2008-09, and the Japanese earthquake and tsunami in 2011.

“We wanted to find out what’s going on, in-depth, inside these companies,” Useem says.

By interviewing leaders at over 100 large, diverse global companies about their most adverse risks—and, importantly, how they rebounded from them—Useem and Kunreuther were able to identify effective practices for catastrophe risk management, distilling important information for other business leaders, their governing boards, and decision makers at all levels, including those in nonprofit organizations and government agencies.

Interestingly, since they’ve finished writing their book, Useem says, the issue of catastrophic risk for companies has “become all much more evident.” He notes, specifically, the disasters that have struck Facebook, Volkswagen, and Wells Fargo. “Seeing this happen repeatedly to others is causing companies to double down on their own risk management.”

Kunreuther and Useem end their book with a “mission-critical checklist” as a means of “transforming deliberative thinking into deliberative action.”

Here’s a glimpse into the Top 5 guidelines, out of 10:

1. ***Catastrophes are on the rise, and your firm may be next in line to suffer one.*** Don’t pretend it can’t happen to you, and instead imagine five potential disruptions that could hit this year or next if one of your current assumptions turns out to be wrong.
2. ***Involve personnel at all levels in designing risk-management and crisis-response strategies.*** Involve company directors, top executives, managers, and front-line employees in taking steps now to prepare for the unexpected. Tapping outside expertise can help you put the different parts of the puzzle together and save you time.
3. ***Recognize behavioral biases and simplified rules that misdirect company decisions.*** Engage in deliberative thinking and systematic analysis by recognizing that intuitive ideas can lead business leaders to misestimate their low-probability risks and then mismanage recovery efforts when they materialize.
4. ***Identify and appraise the risks you face.*** Prioritize the enterprise risks that demand attention now by building on what directors, executives, and managers separately see, and recognize the hazards that can threaten the firm as a whole.
5. ***Define your firm’s risk appetite and risk tolerance.*** Identify and balance risk appetite and tolerance in mapping your company’s overall strategy.

“The ‘unthinkable’ has gone from not being on anyone’s radar screen to now being central,” says Useem, director of Wharton’s Center for Leadership and Change Management. “But to think about it, you need tools, and wisdom.”

Kunreuther, who co-directs the Wharton Risk Management and Decision Processes Center, says a major challenge firms face is the tendency to be myopic.

“Managers in firms think about the next year instead of the long term,” Kunreuther explains. “As a result, disasters are viewed as low probability events. They think, ‘It’s not going to happen to me.’”

This sometimes causes a decision maker to be shortsighted when faced with the expense of investing in protection against a high-consequence event—the near-term payoffs don’t appear to justify the up-front costs.

“But if they stretch the time horizon to 10 or 20 years, then the likelihood of at least one catastrophe occurring during this period is high enough for them to pay attention to the consequences and justify the investment,” Kunreuther says.

But, says Useem, cautioning that he doesn’t want to seem “too somber,” but the world is “becoming a riskier place to inhabit. Recognizing risk and its impact, and thinking through preparations for it and responses to it, is for everybody.”

The growing concern of risk, explain Kunreuther and Useem, is evident in influential business gatherings. They note, particularly, the World Economic Forum, on which they’ve collaborated together for years.

“In the 1990s, the Forum devoted only a few sessions in its annual meeting in Davos, Switzerland, to risk issues,” they write. “Of its nearly 250 sessions at the at the 1997 annual gathering, for instance, just a dozen were explicitly focused on the topic. By the mid-2000s, however, a third of its sessions touched on risk, and by the 2010s nearly half.”

In an earlier volume, *Learning from Catastrophes: Strategies for Reaction and Response*, published in 2010, Kunreuther and Useem featured the contributions of leading experts in risk assessment, risk perception, risk management, and disaster recovery, identifying the behavioral biases that misinform leaders about the likelihood and consequences of catastrophes.

With their new “Mastering Catastrophic Risk,” they take their mission up a notch.

“Companies must get their act together, and get it together now,” says Useem.

***Lauren Hertzler** is staff writer at Penn Today.*

ISO 22330 “Guidelines for people aspects of business continuity” is here!

Source: https://powertorecover.com/news/iso-22330/

June 2018 sees the publication of the long awaited and much needed international standard ISO 22330 “Guidelines for people aspects of business continuity.” This new document expands on the guidance in ISO 22301 and ISO 22313 providing a uniform approach relevant to any size of organisation that needs to prepare for, and respond to, events that are disruptive, challenging or distressing for its people.

For too long, the focus has only been on the practicalities of restoring business operations whilst forgetting that people underpin the processes. People are the greatest asset in any business and it’s encouraging that their safety and well-being now warrants a standalone document. We were delighted to be involved in drawing up these guidelines and contributing to the management of the psychological aspects.

As well as business continuity, it will be of interest to people working in risk management, crisis response, human resources, health and welfare, leadership roles.

Although it is not a definitive guide to managing an incident, ISO 22330 does provide a useful starting point for considering where an organisation currently sits in its people response. It will be useful for considering blind spots – the things we don’t know that we don’t know – gaps in existing policies and processes, current strengths and areas for improvement and where it may necessary to bring in additional technical expertise.

ISO 22330 details recommendations across the phases of preparation, response, recovery and restoration. Two informative annexes focus on psychological response management and relatives’ response teams. The document is a good framework for creating policies and procedures and clear pathways of care for any size of organisation. Once they have identified the "what to do," organisations can more effectively utilise existing internal resources and / or identify the areas of external expertise required to implement the "how to do it."

The first Annex, along with the clear definitions at the beginning of the document, provide concrete advice on steps that can be taken to provide a continuum of care. It emphasises 2 clinically effective, immediate actions that all organisations should be taking after a crisis or potentially traumatic event: providing psychological education and workplace support. Psychological education normalises responses and empowers people to become active in their own recovery. Workplace support can vary from the basic, humane care that we would want to offer and receive to trained peer supporters. Managers and supervisors often want to do the right thing but don't know what this is and for many lower risk profile organisations, training peer supporters is simply not an appropriate option.

KRTS International developed a ground-breaking App to allow organisations to provide psychological education and workplace support immediately after an incident in a simple, global but cost-effective way. It is the first intervention on a needs-based continuum care and for the majority of people will be enough. This allows resources to be targeted where they are needed most.

- For more information on the App, go to www.powertorespond.com
- For a preview of ISO 22330 go to https://www.iso.org/obp/ui/#iso:std:iso:ts:22330:ed-1:v1:en

A DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN? I APPLAUD YOUR PROACTIVE THINKING SMITH BUT THIS FIRM HAS BEEN IN BUSINESS FOR 23 MILLION YEARS AND NOTHING'S HAPPENED YET! I'LL KEEP THIS ON FILE.