May 2015

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

10 years

www.cbrne-terrorism-newsletter.com

29 years after the Chernobyl disaster

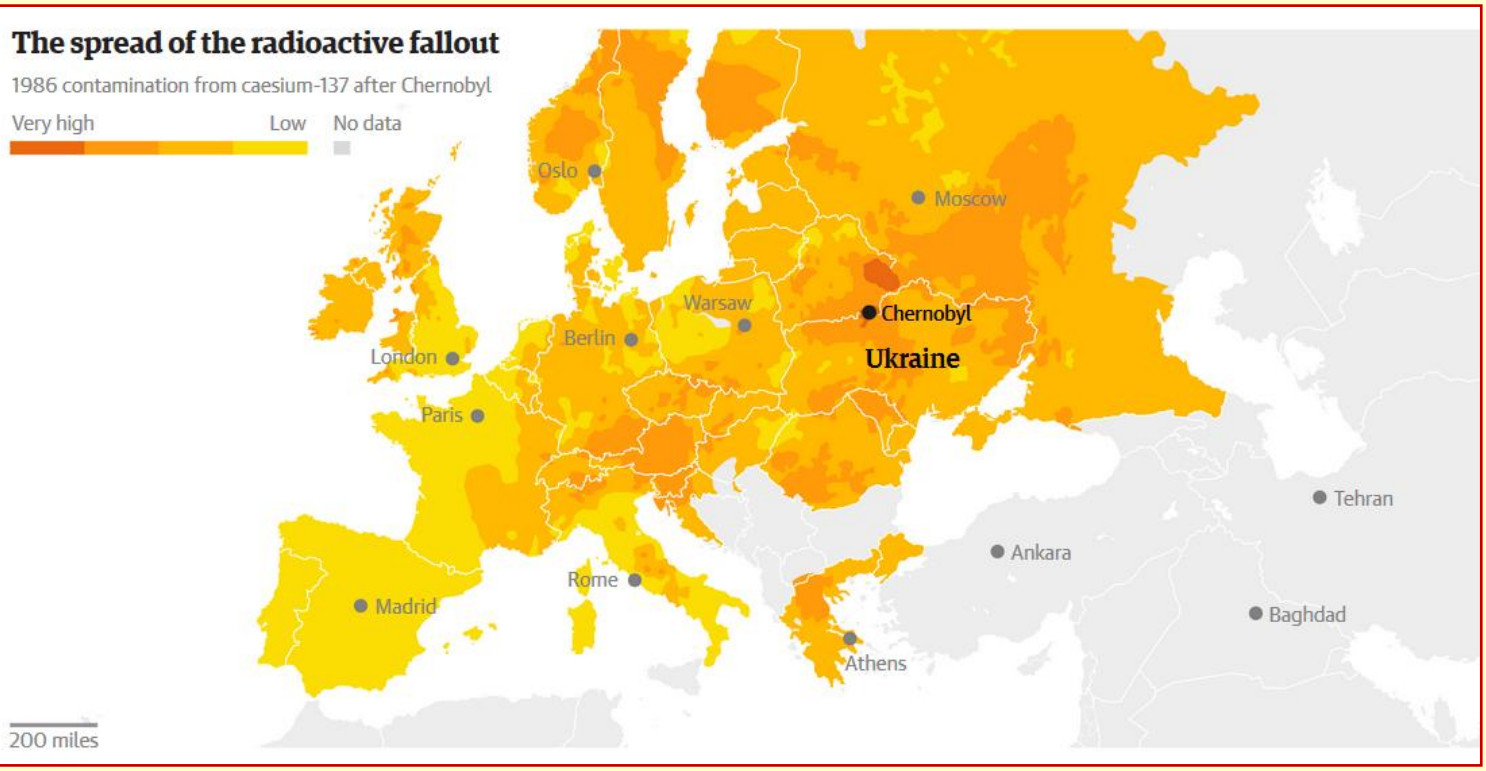
Chernobyl arch faces €265m funding gap ahead of disaster's 29th anniversary

Source: http://www.theguardian.com/environment/2015/apr/24/chernobyl-arch-faces-265m-funding-gap-ahead-of-disasters-29th-anniversary

Apr 24 – **A massive engineering project to make the Chernobyl nuclear power plant safe is facing a €265m (£190m) funding shortfall.**

Next week a conference held by Germany in London will call on countries to make up the gap, but the European Bank for Reconstruction and Development (EBRD) has said it may have to ask its shareholders to make up the shortfall if donations dry up.

This Sunday marks the 29th anniversary of the world's worst nuclear disaster, when a power surge blew the roof off a reactor, spewing radioactive clouds across Russia, and Eastern Europe.



A makeshift sarcophagus built in the explosion's aftermath was supposed to protect the environment from radiation for at least 30 years. But it has since developed cracks.

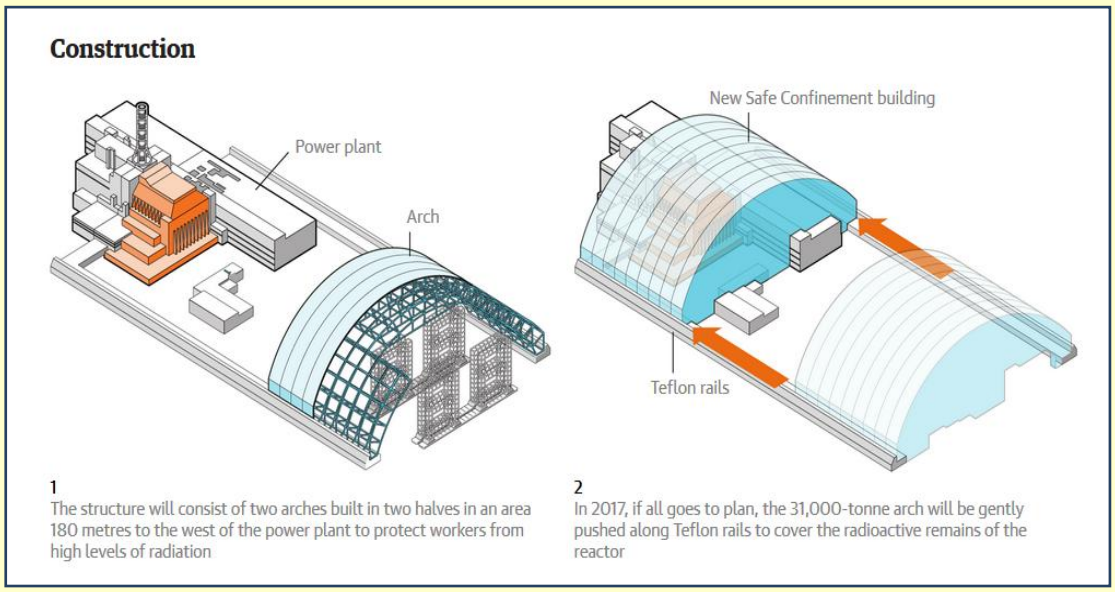
The project to build a new radiation container had been due for completion this year but the deadline slipped to November 2017, as costs mushroomed from an initial estimate of €800m (£572m) to more than €2.15bn today.

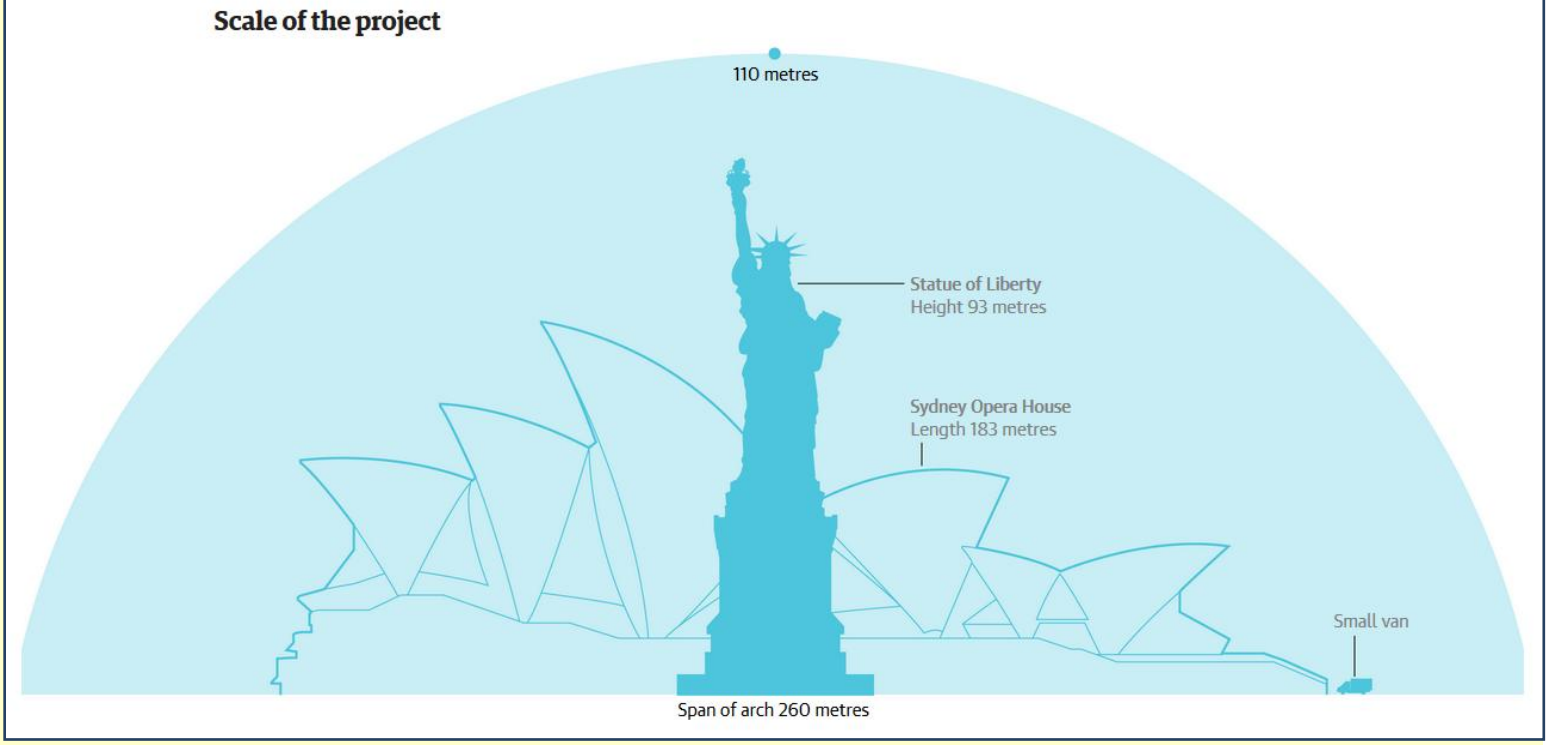
Over 40 governments and the European commission have committed to help a Chernobyl Shelter Fund tasked with sealing off the 100 tonnes of uranium and one tonne of plutonium that remain within the site.

"If countries recognise the nature of the problem in Chernobyl and its importance for human security in Ukraine and ecological security in Europe, there is a hope that the gap could be closed at the donor conference on April 29," Anton Usov, an EBRD spokesman told the Guardian. "Verbally the donors are committed to contribute more funds."

The bank believes there is a broad understanding among nations of the threat that radioactive dust on the site still poses to Kiev, around 70km away.

But "if there is a shortfall, then we will speak to the bank's management and





shareholders and it may be funded by EBRD reserves," Usov added. "Theoretically, that is something we could do."

The 31,000 tonne protective steel arch is an engineering project of staggering dimensions – 100m high, 165m long, with a span of 260m. When finished, it will be slid across teflon pads to entomb the burned out reactor, and is intended to remain effective for a century.

"The are no parallels in the history of world engineering," Usov said. "No-one has even undertaken a project like this before."

Construction of the stainless steel arch has been hampered by factors ranging from optimistic early architectural designs to heavy snows in the winter of 2013/14, which caved in part of a roof near the stricken Unit 4 reactor shelter. Workers were evacuated from nearby sites, as radiation levels surged.

The reactor itself is still too contaminated for workers to approach. Removal of radioactive materials there will only begin once the new confinement structure has been finished.

Why nuclear dominoes won't fall in the Middle East

By Dina Esfandiary and Ariane Tabatabai

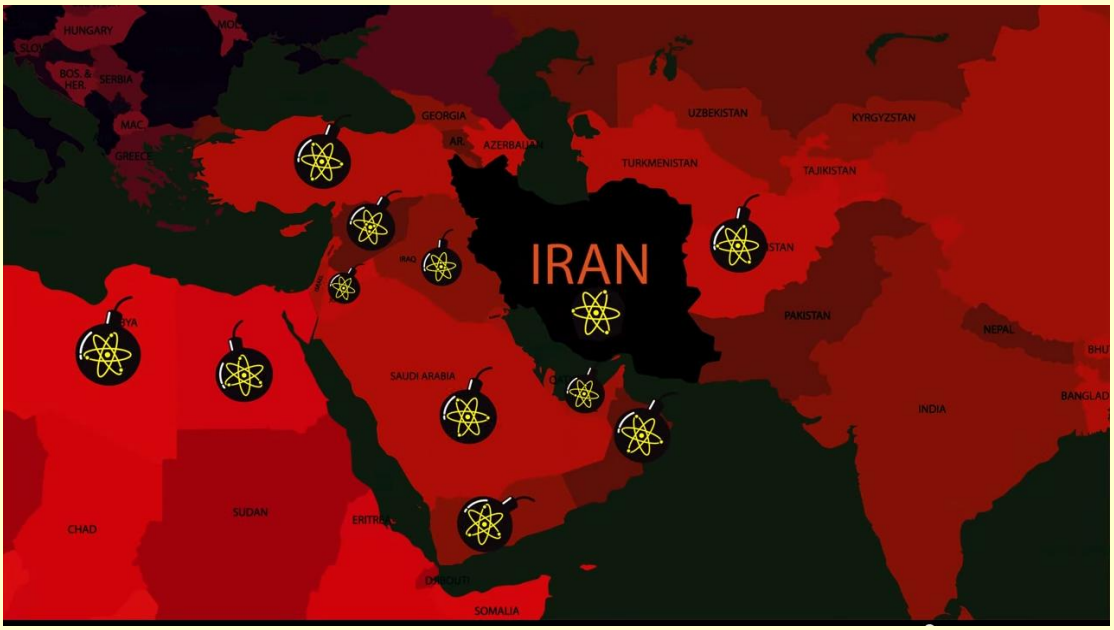
Source: http://thebulletin.org/why-nuclear-dominoes-wont-fall-middle-east8236

A highly regarded member of Saudi Arabia's royal family recently repeated assertions that Riyadh will want the same capabilities that Iran is allowed under a final agreement on its nuclear program. The Saudi stance, articulated most recently by former intelligence chief Prince Turki al-Faisal, has raised fears that a nuclear agreement between six world powers and Iran will produce a regional domino effect that could spread civilian nuclear programs across the Middle East and increase the number of nuclear weapons states in the region.

Although such a possibility can't be dismissed entirely, **a close analysis of probable scenarios suggests that a final Iranian nuclear agreement is unlikely to trigger a regional nuclear weapons cascade.**

On their own, civilian nuclear programs do not necessarily imply a military threat. Under the Non-Proliferation Treaty (NPT), member countries are allowed to pursue civilian nuclear programs. Because of a growing energy demand, many countries in the Middle East are exploring nuclear power as part of their energy mix. While some, including the United Arab Emirates, have succeeded in starting civilian nuclear power programs, others face serious financing and technical capacity issues. Developing a nuclear

program is neither easy nor cheap. Nuclear power plants cost $4 billion to $10 billion each,



and acquiring nuclear technologies requires significant financial and scientific investment and, for most countries in the Middle East, foreign help.

To be sure, civilian nuclear programs have been used as cover for nuclear weapons acquisition. The front and back ends of the fuel cycle for a nuclear power plant provide technology—uranium enrichment and spent nuclear fuel reprocessing—that can provide the nuclear material needed to build nuclear weapons. Because this fuel cycle paves the path to nuclear weapons, many experts call for limiting its spread and suggest that countries creating nuclear power industries develop international sources for their fuel needs. And most countries that are considering nuclear power in the Middle East don't yet have concrete plans to develop a domestic fuel cycle that includes enrichment or reprocessing. But the NPT has no prohibition against non-nuclear weapons states developing a domestic nuclear fuel cycle.

Just the same, capabilities alone do not determine whether a country acquires nuclear weapons. Intentions matter, and placing a high price on weapons acquisition or offering credible security guarantees can influence a state's nuclear intentions.

Developing a nuclear bomb is hard. It took the United States, with its vast resources and advanced know-how, six years to develop a nuclear device. It took China roughly 10 years and Pakistan more than two decades. There are two ways a country can pursue the fissile material needed for a bomb: one that produces highly enriched uranium, and another that extracts plutonium from used fuel. Both processes involve complicated technologies that are subject to strict international controls. Countries in the Middle East have forgone these options, or accepted strict controls on their nuclear programs, or do not have the technical know-how to develop enrichment or reprocessing capabilities. And although some countries in the region possess the financial means to overcome these technical constraints, political obstacles will hamper their progress toward nuclear weapons capability.

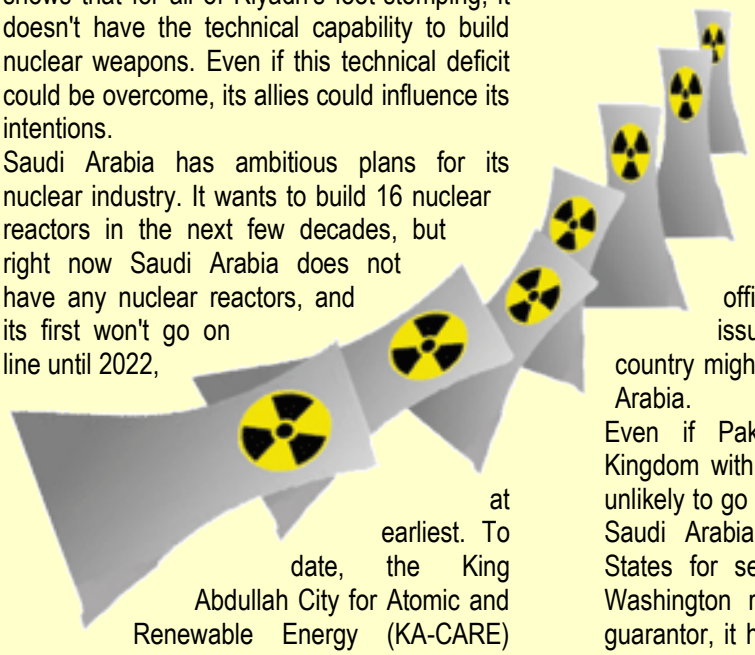
Of course, there is an alternative to building a bomb: Buying or stealing one. For political, legal, and practical reasons, the first is difficult, and the second extremely unlikely. And countries in the Middle East that attempt to create their own nuclear power sectors face many obstacles that make nuclear weapons development quite difficult and unlikely. The factors that will likely inhibit nuclear weapons proliferation in the region vary from country to country. But it is clear that, in each country, the technical and political forces arrayed against nuclear weapons production are significant.

Saudi Arabia: The human and technical impediments to a nuclear arsenal

Saudi Arabia is viewed as the Middle East's most likely nuclear proliferator. Riyadh has been the loudest voice in the region, claiming it'll "go nuclear" should Iran do so. It also wants an enrichment

capability to mirror Iran's. An assessment of the nascent Saudi nuclear power program shows that for all of Riyadh's foot-stomping, it doesn't have the technical capability to build nuclear weapons. Even if this technical deficit could be overcome, its allies could influence its intentions.

Saudi Arabia has ambitious plans for its nuclear industry. It wants to build 16 nuclear reactors in the next few decades, but right now Saudi Arabia does not have any nuclear reactors, and its first won't go on line until 2022, at earliest. To date, the King Abdullah City for Atomic and Renewable Energy (KA-CARE) has scouted out foreign suppliers and developed regulatory frameworks—but gone no further down the nuclear path.



Riyadh lacks the human capacity to develop and operate its own nuclear infrastructure in the foreseeable future. But Saudi Arabia is aware of its technical shortcomings, and it's looking for other options

After contributing financially to Pakistan's nuclear weapons program and defense sector, the Saudis may want Islamabad to return the favor, some observers believe. The Saudi leadership plays along with suggestions it may acquire nuclear technology from Pakistan. In March 2015, King Salman bin Abdulaziz urgently summoned Pakistani Prime Minister Nawaz Sharif to Riyadh to discuss strategic cooperation efforts, while calling for Pakistani involvement in Saudi efforts in Yemen. This was intended to remind nuclear weapons state negotiators that Riyadh is keeping its nuclear options open.

But it is unlikely the Saudis will get a nuclear weapon from Pakistan. Pakistan—which covertly developed its nuclear arsenal outside the nuclear nonproliferation regime—aims to normalize its nuclear status, rather than becoming further alienated from the international community. Islamabad was already singled out for the activities of the world's biggest and most successful illicit nuclear trafficking network, led by a key figure in its nuclear weapons program, A.Q. Khan.

What's more, Islamabad is extremely proud of its nuclear achievements. In the words of Zulfiqar Ali Bhutto, "We will eat grass, even go hungry, but we will get one of our own [bomb]." Pakistanis didn't eat grass, but they endured a great deal of hardship to get the bomb. The program was extremely costly for the country. So, it's no surprise that many Pakistani officials and former officials take issue with assertions that their country might give nuclear weapons to Saudi Arabia.

Even if Pakistan agreed to provide the Kingdom with the bomb, the Saudis are very unlikely to go through with such an acquisition. Saudi Arabia is dependent on the United States for security guarantees. As long as Washington remains Riyadh's main security guarantor, it has the power to influence Saudi decision making on other issues, including, specifically, nuclear weapon acquisition. And the Kingdom would find it very difficult to attract another country willing to supply the security and trade guarantees that the United States now provides. It is hard to imagine any of the world's major powers agreeing to be viewed as a supporter of nuclear proliferation.

It is reasonably likely that Saudi Arabia will continue its efforts to develop a civilian nuclear program. **Saudi Arabia recently signed a nuclear cooperation agreement with South Korea to explore the feasibility of building two nuclear reactors in the Kingdom.** Moving forward with South Korea as the main supplier raises a key issue: Washington says that Seoul's reactors are US designs, and that, if that technology is to be sold, the countries acquiring it must enter into nuclear cooperation contracts (known as 123 agreements, because they are based on Section 123 of the US Atomic Energy Act) with the United States. Although South Korea disputes the need for a 123 agreement, if Saudi Arabia does agree to enter into such a pact, it could well mean a ban on enrichment and reprocessing in the Kingdom, closing domestic paths to the bomb.

Riyadh could of course acquire nuclear technology from the two other countries that have developed nuclear power plants on an international basis, France and Russia. But given Paris's hardline stance on nonproliferation, it's unlikely to oblige

an effort by Saudi Arabia to develop the enrichment or reprocessing capabilities needed to produce fissile material in the Kingdom. Moscow, too, would think twice before allowing Riyadh to go nuclear, particularly given the competition between the two countries in world petroleum markets and their divergence on regional security matters.

Turkey: Unlikely to weaponize for strategic and political reasons

Like most of the region, Turkey's stated goal for developing a nuclear program is to meet its energy needs. But Turkey's nuclear journey has been a long and difficult one so far.

Ankara has faced a number of regulatory challenges in the development of its nuclear program. As is the case for most of the region's nuclear newcomers, Turkey's leading nuclear partner is Russia's Rosatom. The two countries concluded a so-called "BOO" [build, own, and operate] agreement. At the current pace, Turkey's first nuclear power plant won't be ready before 2022. The severe impact of sanctions on the Russian economy may further slow progress. In addition to Russia, Turkey is also working with a Franco-Japanese consortium that would build a second plant in the Black Sea town of Sinop by 2023.

To date, Turkey denies any plans to develop an enrichment or reprocessing capability. In addition, Turkey has entered a safeguards agreement with the International Atomic Energy Agency (IAEA) and has agreed to the Additional Protocol, putting Ankara's program under strict IAEA monitoring and making it difficult to divert fissile material for use in a weapons program.

Aside from the technical limitations, there are strategic and political reasons why Turkey isn't likely to weaponize. As a member of NATO and a US ally, Turkey benefits from Washington's nuclear umbrella. Its defense needs are met without it having to go through the trouble of developing its own nuclear capability—a resource-heavy endeavor for a country struggling to build a nuclear energy program. A military nuclear program would most likely result in a loss of the US as a strategic ally and the NATO nuclear umbrella.

Egypt: Some capability, little apparent interest

Egypt is unique among the countries under discussion; it's the only one that has had a nuclear weapons program. But it decided to give up its attempts to acquire nuclear weapons in 1968, following the country's disastrous defeat in the 1967 Six-Day War with Israel. In the 1970s, Egypt backed Iran when the Shah proposed the idea of a nuclear weapon-free zone in the Middle East. Yet, some argue that Egypt could reverse course and again decide to seek its own bomb if Iran and Saudi Arabia do so. Cairo, after all, doesn't want hand over leadership of Arab world to others.

To be sure, Egypt's nuclear infrastructure is more developed than nuclear newcomers in the region. But so far, Cairo's program has remained research and development-focused. It operates two research reactors but hasn't built a power reactor, and the country doesn't have an enrichment or reprocessing capability. It does, however, have small-scale spent-fuel-management and plutonium-separation capabilities.

In recent years, Egypt's political climate has inhibited any focus on a nuclear program. Following the Arab Spring, there were multiple changes in government, domestic unrest, and economic near-collapse. Since the Arab Spring, the real threat to Egypt's security has been internal rather than external.

Those who argue that Egypt is likely to weaponize if Iran is allowed a civilian nuclear program are ignoring the Israeli factor. Egypt shares a border and has fought wars with Israel, which has a nuclear arsenal. Egypt's effort to establish a weapons of mass destruction-free zone in the Middle East is focused on Israeli disarmament. If a nuclear-armed Israel didn't cause Egypt to pursue the bomb, why would a final agreement that limited the Iranian nuclear program to civilian concerns? Some argue that Cairo's nuclear ambitions aren't security-focused but are based on the country's quest for regional leadership. Right now, however, the Egyptian establishment doesn't seem to believe nuclear weapons to be in its interest.

Jordan: A nonproliferation advocate that lacks resources for a nuclear weapons program

Jordan too has ambitious plans for a civilian nuclear program, which it developed in response to growing energy needs and its over-reliance on foreign energy supply; **some 97 percent of its**

energy was imported in 2011. With the help of a South Korean consortium, Jordan is building a 5 megawatt research and training reactor at the Jordan University of Science and Technology. It also wants to build a nuclear plant with two 1,000-megawatt reactors; the plant aims to provide 30 percent of Jordan's electricity by 2030. In February 2015, Jordan signed an agreement with Russia's Rosatom, which will build and operate both nuclear units.

But Jordan's nuclear program stops there. **The country lacks the technology, human resources, experience, or infrastructure necessary for a nuclear weapons program.**

There is one cause for concern: Amman's refusal to sign a 123 nuclear cooperation agreement with the United States. Jordan has significant uranium reserves and wants to preserve the option of domestic enrichment. Among countries in the Middle East who want to preserve the "right to enrich,"Jordan's claims may make the most sense economically and practically. To this end, Amman pursued mining and milling options with foreign companies. To date none has panned out.

Jordan's plans for nuclear power are grounded in long-standing energy concerns that emerged long before the start of nuclear talks with Iran and that are unlikely to be affected by Iranian nuclear plans. Jordan has been an upstanding non-proliferation advocate and party to the NPT. The country has an Additional Protocol and a series of other non-proliferation commitments in place. It has a sterling track record: It was not found in violation of any of its non-proliferation commitments. What's more, like Saudi Arabia, Egypt, and Turkey, its security depends on its alliance with the United States—an alliance Amman will not lightly jeopardize.

United Arab Emirates: The gold standard for nonproliferation

Of all the countries in the region, the UAE is the least likely to proliferate. While the country has the most developed nuclear energy program among the newcomer states of the region and is likely to operate the second power plant to open in the Middle East (after Iran's Bushehr), the plant will be under strict controls and self-adopted restrictions.

Because of its growing energy requirements, in 2006 the UAE began exploring options for a nuclear energy program. Like others in the region, the UAE had no nuclear infrastructure or specialized human capital, but it did have a mature energy sector, a civil construction industry, and an advanced educational system that a nuclear energy program could build on. Most important, the UAE had the economic means to pursue its nuclear energy ambitions.

After establishing governmental and private-sector organizations to supervising the program's safety and security, the UAE has begun building two of four reactors, in collaboration with a South Korean consortium; they are due for completion in 2020.

Like Jordan, the UAE is an exemplary member of the international non-proliferation regime. Along with the NPT and safeguards agreement with the IAEA, it also adopted the Additional Protocol. Unlike others in the region, Abu Dhabi relinquished domestic enrichment and reprocessing in January 2009, signing a 123 agreement with the United States that sets what is often called the "gold standard" for civilian nuclear programs. This agreement effectively bars the country from pursuing enrichment and reprocessing, the only indigenous paths to the bomb.

The conventional wisdom is wrong

Conventional wisdom holds that a nuclear Iran will lead to a nuclear weapon proliferation cascade in the highly volatile Middle East, making an already rough neighborhood even more unstable and insecure. After all, a combination of fragile and failed states, terrorist organizations, and nuclear weapons could well constitute a horror story.

Nuclear history shows us that nuclear arms races are the exception rather than the rule. A final agreement between six world powers and Iran to limit the Iranian nuclear program would aim to keep Tehran from acquiring a nuclear weapon. But if an agreement is not reached or Iran cheats and acquires nuclear weapons, a nuclear weapons race is still unlikely to unfold in the Middle East. A number of political and technical challenges are likely to prevent it. No country in the region currently has the technical ability to develop a nuclear weapon by itself. Most regional candidates to become nuclear weapons states—especially ones most vocal in claiming they'll go nuclear, if Tehran does—depend heavily on the United States and other Western states for their security, providing the West with significant leverage over them.

But the international community must draw lessons from the Iran case. In Iran, foreign suppliers left a vacuum when they stopped their involvement in the Iranian nuclear program. This created an opportunity for Tehran to undertake and justify activities that would have been difficult to pursue, had the United States, Germany, Japan, and France continued helping it acquire nuclear technology. Foreign suppliers should remain active in nuclear newcomers' programs in the region, taking away any excuse to develop an indigenous nuclear fuel cycle. This kind of engagement will go a long way toward ensuring Middle Eastern nuclear programs remain peaceful.

Dina Esfandiary *is a MacArthur Fellow at the Centre for Science and Security Studies at King's College London.*

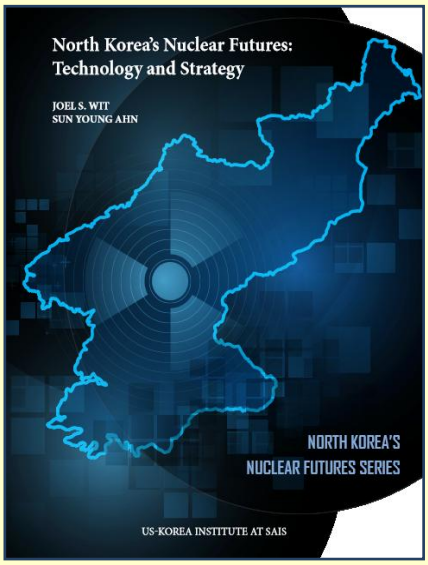
Ariane Tabatabai *is a visiting assistant professor in the Security Studies Program at the Georgetown University School of Foreign Service, and an associate in the Belfer Center's International Security Program and Project on Managing the Atom at Harvard University. Previously, she was a nonresident research associate with the James Martin Center for Nonproliferation Studies. She was a Stanton Nuclear Security Fellow at the Belfer Center in 2013 and 2014. Her work has appeared in the Financial Times, the Boston Globe, the National Interest, Haaretz, and Al-Monitor, among other publications. She is a frequent media commentator on nuclear issues in English, French, and Persian, on such outlets as NPR, the BBC, Al-Jazeera, and France24.*

EDITOR'S COMMENT: Although the approach of analysis is logical, are we sure that Turkey's ambitions are those described herein?

Just How Many Nuclear Weapons Does North Korea Have? A Look at the Numbers

Source: http://blogs.wsj.com/chinarealtime/2015/04/23/just-how-many-nuclear-weapons-does-north-korea-have-a-look-at-the-numbers/

Estimating the size of North Korea's nuclear arsenal is a high-stakes guessing game. Nuclear specialists look at a range of variables, including the country's capacity to produce centrifuges needed to enrich uranium, and how much of the end product would likely go into each bomb.



The latest Chinese estimate that North Korea could have 20 warheads today and 40 by 2016, reported exclusively by the Wall Street Journal on Thursday, surpasses that of most U.S. experts.

The current U.S. Congressional estimate is that North Korea has 10-16 nuclear weapons. The Chinese estimate for 2016 falls near the highest end of a range presented in a report published in February by the US-Korea Institute at the Johns Hopkins School of Advanced International Studies.

That report gives a low-end estimate of 10 nuclear weapons at the end of last year and 20 by 2020. Such a scenario assumes North Korea would stop nuclear tests, possibly under Chinese pressure, would struggle to find the resources for its nuclear program, and might conclude that an arsenal of 20 was a strong enough deterrent.

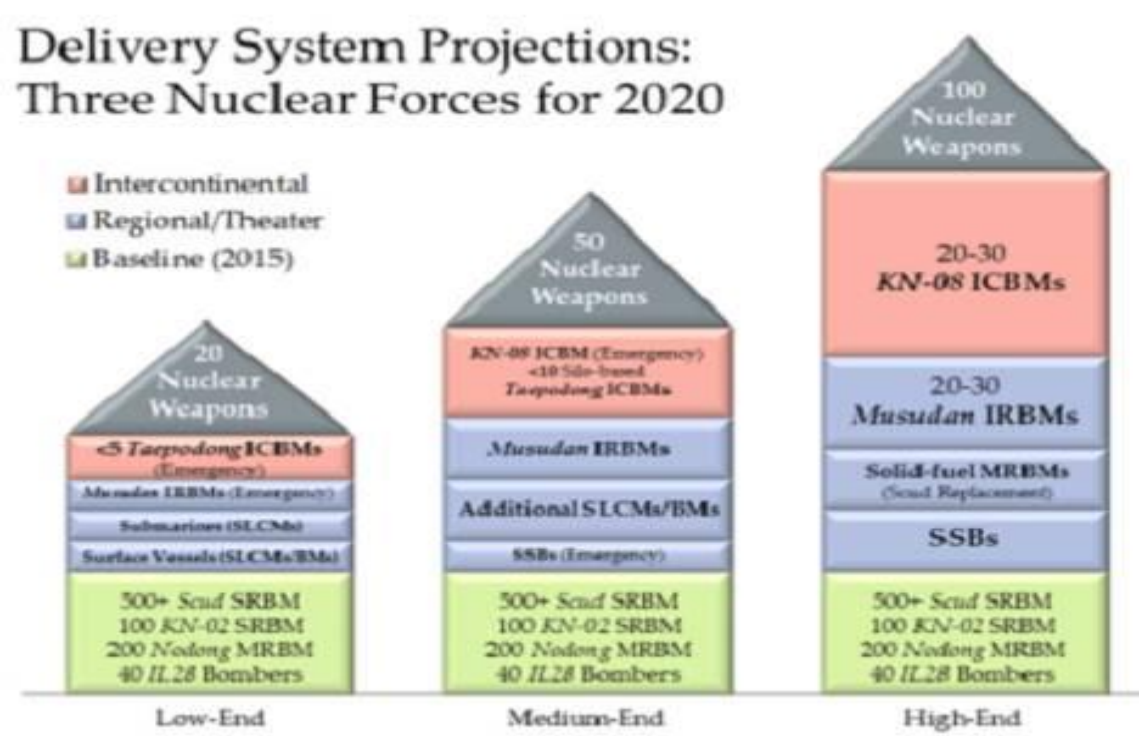
"A North Korea armed with 20 nuclear weapons and only minor improvements in its current force of delivery systems seems likely to continue to rely on a policy of assured retaliation, threatening the

use of these weapons in response to a nuclear attack by the United States," the report said.

The report's mid-range estimate was that North Korea had 16 nuclear bombs at the end of last year and could have 50 by 2020. This assumes that the North Koreans continue nuclear tests every three to four years, improve their bomb design skills, and get some limited assistance from Iran.

"With a nuclear deterrent of 50 nuclear weapons, a growing range of yields, additional mobile theater-range delivery systems possibly including greater numbers based at sea, and an emerging intercontinental force, Pyongyang will possess a more survivable and robust assured retaliatory capability able to more credibly threaten the United States," it said.

An illustration of three potential scenarios for the growth of North Korea's nuclear arsenal and missile capabilities by 2020. ICBM = inter-continental ballistic missile, IRBM = intermediate range ballistic



missile, MRBM = medium range ballistic missile, SRBM = short range ballistic missile, SLCM/BM = submarine-launched cruise missile/ballistic missile. The US-Korea Institute at SAIS

At the high end, the report estimated that North Korea had 16 nuclear weapons at the end of last year and could have 100 by 2020. That assumed it would conduct nuclear tests once a year, acquire foreign nuclear technology and data, and dedicate more resources to its nuclear program, possibly because of a more threatening security environment, an improving civilian economy or cutbacks to conventional military spending.

"A North Korea armed with 100 low, medium and high-yield nuclear weapons that can be mounted on an array of battlefield, theater and intercontinental delivery systems would certainly have an even more robust assured retaliatory capability," the report said.

That would allow North Korea to consider threatening "first use" under certain conditions, it said. "In that context, battlefield nuclear weapons would be integrated into Pyongyang's war plans and the limited use of these weapons on the peninsula would be provided for under certain conditions. The threshold for use against Japan would be lowered as well," the authors wrote.

▶ **Read the report at:** http://38north.org/wp-content/uploads/2015/02/NKNF-NK-Nuclear-Futures-Wit-0215.pdf

Preventing a Fukushima-like disaster in Europe

Source: http://www.homelandsecuritynewswire.com/dr20150429-preventing-a-fukushimalike-disaster-in-europe

Apr 29 – **In 2005, Europe was exposed to a potential risk of a nuclear disaster caused by the flooding of the Loviisa nuclear power plant in Finland. Sea levels rose by 1.73 meter above normal levels, due to a storm. As a result, flood defenses have been reinforced.**

However, latest research reveals that more improvements could still to be made to optimize safety and better protect people from potential future accidents. Youris says that floods are likely to occur more frequently than anticipated when nuclear power plants where built, due to climate change.

In Finland several changes in accident management have been introduced, to prevent future nuclear waste leaks. "From our point of view, the priority is to ensure that there is an alternative route to the plant accessible in a flood. By using our pumps and the Loviisa plants' own equipment, water at the site can be reduced," says Peter Johansson, CEO of the Fire and Rescue Services of the local Eastern Uusimaa department attached to the Loviisa power plant.

Further precautions have also been taken. "The latest security investment is the building of four cooling towers that are independent from seawater intake, which are built ten meters above the sea level to avoid them from being flooded," explains Samuli Savolainen, group leader at the Loviisa plant.

The Fukushima accident, in March 2011, brought renewed scrutiny towards the resistance of nuclear power plants to natural disasters. The EU stress tests required after the meltdown in Japan, led to the introduction of a precise Severe Accident Management plan,

according to Thomas Buddas, vice-CEO of the Loviisa nuclear power plant. "We are confident that flooding events can be predicted well in beforehand as we cooperate with the Finnish Meteorological Institute," Buddas tells youris.com. He explains that the top priority is to protect the reactor and the fuel tanks from seawater, and a series of waterproof doors and flood gates have been installed.

Nuclear plants, in particular, are one of the focus infrastructures of interest to a European project called RAIN, due to be completed by the end of 2017. It aims to detect system vulnerability and identify hazards as a result of extreme weather events. As part of the project, Timo Hellenberg, CEO of critical infrastructure protection consultancy Hellenberg International, based in Helsinki, Finland, conducted an analysis of the crisis management process.

Despite all these measures, his findings show that there is still room for improvement.

"Foreign specialists should be involved in the emergency training sessions. There is too little inter-agency cooperation. But this is a general European trend," explains Hellenberg. "Emergency trainings should be organised between Finnish agencies and neighbouring countries."

"Finland is in the forefront in nuclear safety, including technological solutions and nuclear safety culture," notes Christer Pursiainen, professor of Societal Safety and Environment at the Department of Engineering and Safety of the Arctic University of Norway in Tromsø. Nevertheless, "The risk of a serious nuclear accident remains always above zero anywhere as a possibility of unexpected phenomena taking place exists."

Hybrid organizations have greater motivational and operations ability for RN trafficking

Source: http://www.start.umd.edu/news/hybrid-organizations-have-greater-motivational-and-operations-ability-rn-trafficking

Apr 29 – With characteristics of both transnational criminal organizations (TCOs) and terrorist organizations, **hybrid organizations have demonstrated greater motivation and operational ability to traffic radiological/nuclear material illicitly,** according to recent research from the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Of the 143 terrorist and 381 TCOs identified for examination, only a handful possess both high motivation and operational capacity to engage in illicit RN material trafficking if given the access and opportunity.

The research team focused on Western and Eastern Europe as well as North, Sahelian and West Africa to ascertain whether the terrorist organizations and TCOs in these areas could and would engage in illicit RN material trafficking. While connection between the TCOs and terrorist organizations is unclear in terms of RN trafficking, there is clear evidence that a number of terrorist organizations are engaging in other criminal activities to fund their terrorist operations.

Led by START researchers Amy Pate, Steve Sin, Marcus Boyd and Salma Bouziani, the team also found that when it comes to the threat of RN trafficking, most traditional TCOs lack the motivation to carry out these operations despite having the capacity to do so.

"As organizations primarily interested in sustained profit generation, TCOs were found to be lower in their threat level to willingly engage in illicit RN material trafficking," Sin said. "The risks and consequences associated with RN material smuggling just isn't worth the potential payoff for these groups."

In addition to examining the group dynamics and operations in the regions, the research team examined potential routes in which RN materials could be transported. **Using START's TransIT geospatial modeling tool**, the team identified illicit transport routes used by TCOs and found that TCOs adapt to the changing dynamics of their operating environment by selecting routes that optimize efficiency while minimizing the risk of detection. The TransIT tool allowed the team to create an illustrative model that identified several transportation chokepoints within the studied regions.

"It showed us that there is consistent travel of a wide variety of TCOs through a limited number of key nodes in this network," said Boyd, who headed up the Geographic Information Systems (GIS) component.

Funded by the Department of Homeland Security, the two-year study, "Organized and/or

Transnational Criminal Cartel Nexus with Illicit Radiological/Nuclear (RN) Trade, Smuggling and/or Terrorism in Europe and North, Sahelian, and West Africa," yielded additional policy considerations. The researchers encourage those leading U.S. efforts in these regions to continue to engage with the region's sovereign state government, but also devise parallel policies designed to concurrently engage with select local tribal leadership to raise their awareness, secure their buy-in, and enlist their cooperation.

The team found that although technical detection methods can effectively aid in the successful interdiction of illicit trafficking attempts, non-technical detection methods, such as actionable intelligence and situationally alert law enforcement or customs officials, account for the majority of successful interdiction cases.

Additional work by the team included a case study that focused on the abuse of diplomatic immunity. The team examined documented cases in which diplomatic bags - which are exempt from inspection - had been employed in smuggling operations ranging from drug trafficking to state-sponsored kidnapping. The study highlighted the potential threat of such dimplomatic pounches being employed to traffick RN materials and the international legal hurdles to remedying this frightening vulnerability.

Read more on the case study mentioned in this article at:
http://www.cbrneportal.com/tradition-or-threat-the-diplomatic-pouch-and-the-potential-for-rn-smuggling/

NTI Nuclear Materials Security Index

Source: http://www.clarionproject.org/analysis/britains-muslims-poised-be-swing-vote-uk-elections

The NTI Nuclear Materials Security Index is a first-of-its-kind public benchmarking project of nuclear materials security conditions on a country-by-country basis in 176 countries. Initially launched in 2012, the NTI Index, prepared with the Economist Intelligence Unit (EIU), helped spark international discussions about priorities required to strengthen security and most important, is encouraging governments to provide assurances and take actions to reduce risks.

On January 8, 2014, the second edition of the NTI Index was released.

The project draws on NTI's nuclear expertise and the EIU's experience in constructing indices, and the reach of the EIU's global network analysts and contributors. NTI—working with an international panel of nuclear security experts and a number of technical advisors—focused on the framework and priorities that define effective nuclear materials security conditions. The EIU was responsible for developing the Excel-based model and gathering the data.

The 2014 NTI Index assesses the contribution of 25 states with one kilogram or more of weapons-usable nuclear materials towards improved global nuclear materials security conditions, using five categories: 1) Quantities and Sites 2) Security and Control Measures 3) Global Norms 4) Domestic Commitments and Capacity and 5) Risk Environment. An additional 151 states, with less than one kilogram of material or none at all, are assessed on the last three of these categories. The NTI Index includes three elements:

- The **print report** with NTI findings and recommendations, a complete discussion of the EIU methodology, and selected data.

- A **web site** at www.ntiindex.org with high-level results in an easily accessible format, including all country summaries.
- A **downloadable version of the NTI Index**, available through the website, with complete results and data and extended interactive features, in an Excel format.

2014 Key Trends

States are making progress. Since the beginning of 2012, 7 states—Austria, the Czech Republic, Hungary, Mexico, Sweden, Ukraine, and Vietnam—have removed all or most of their weapons-usable nuclear materials, according to the U.S. National Nuclear Security Administration. Thirteen other states have decreased their quantities of materials over the most recent four-year period measured by the NTI Index; 6 states have strengthened physical protection measures and the ability to mitigate the insider threat; 3 states have updated regulations for transporting materials; 7 states have signed or ratified key international legal agreements; and 4 states have made new voluntary commitments that support global efforts to improve security.

Nuclear Security Summits have had an impact. At the 2010 and 2012 summits, many states with weapons-usable nuclear materials committed to decreasing their quantities, to ratifying relevant treaties, or to taking other actions. Twelve specific score improvements in eight states captured in the NTI Index were a direct result of those summit commitments.

Global stocks of weapons-usable nuclear materials are decreasing overall, but some states are still increasing their stocks. Despite the reduction of nuclear materials in 13 states, 4 states have increased their stocks of weapons-usable nuclear materials during the most recent four-year period measured by the NTI Index. Japan and the United Kingdom have increased quantities in their civilian sectors; India and Pakistan have increased quantities for both civilian and military purposes. North Korea has also taken new steps necessary to produce new weapons-usable nuclear materials, which may increase its quantities.

Eight states improved their physical protection, control, and accounting measures, including through regulations on on-site physical protection, control and accounting procedures, insider threat prevention, and physical security during transport when materials are most vulnerable.

States with no weapons-usable nuclear materials or with less than one kilogram are supporting global norms and implementing international commitments. For example, 22 more of these states became parties to key international legal agreements on nuclear security since research for the 2012 NTI Index ended in September 2011, and 19 states made new voluntary commitments.

Country Highlights

Australia again ranks first among 25 states with weapons-usable nuclear materials, scoring well across all five categories and demonstrating that all states can do more to improve.

Belgium, Canada, and Japan are the most improved states.

Among nuclear-armed states, Pakistan is most improved through a series of steps to update nuclear security regulations and to implement best practices, though it ranks 22nd overall. France, the United Kingdom, and the United States lead the nuclear-armed states in scoring, with France tied for 7th with the Netherlands, and the United Kingdom and the United States tied for 11th.

Remaining Challenges

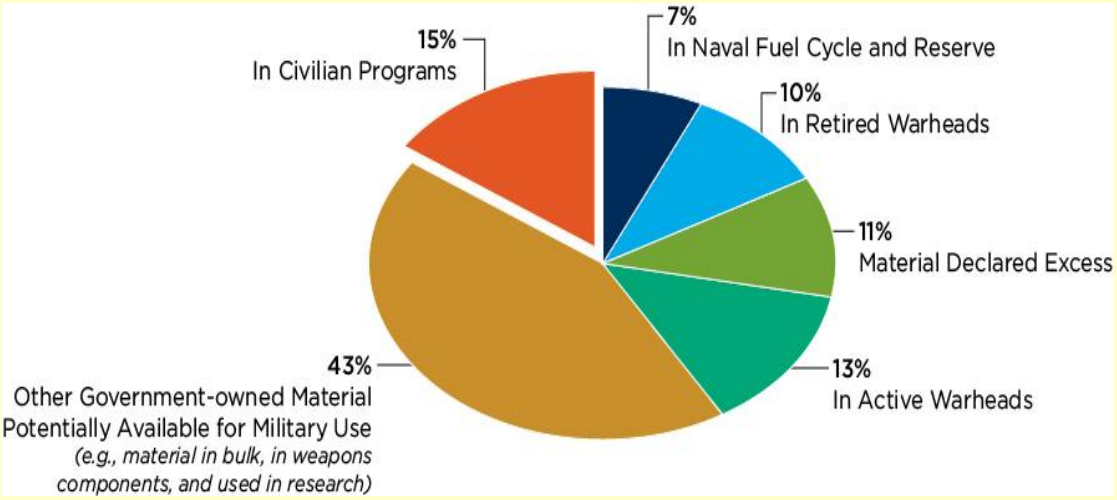
The lack of an effective global system for securing weapons-usable nuclear materials is a major challenge. Despite progress since 2012, there is still no effective global system for how nuclear materials should be secured. Because each state considers materials security an exclusively sovereign, not shared, responsibility, approaches to nuclear security vary widely with little sense of accountability, even though poor security in any one state can affect all other states. Several factors addressed by the NTI Index underscore this fundamental deficit:

- The existing legal foundation for global nuclear security remains weak. A key legal agreement related to nuclear security—the CPPNM and its 2005 Amendment—provides an important initial foundation for nuclear materials security. However, the 2005 Amendment still has not entered into force. A separate agreement, the International Convention for the Suppression of Acts of Nuclear

Terrorism, commits states to criminalize acts of nuclear terrorism. However, each of those agreements has limitations: they are not universally implemented; they have no enforcement or accountability mechanisms; and the CPPNM and 2005 Amendment cover only civilian materials, which make up only 15 percent of global stocks of weapons-usable nuclear materials.

- Participation in international peer review is still limited. Of the 25 states with weapons-usable nuclear materials, only 18 have invited a peer review in the past five years, and 6 have never invited a peer review, even though it is a critical tool for strengthening a state's security practices and assuring others about the effectiveness of an individual state's security.
- The vast majority of global stocks of weapons-usable nuclear materials—approximately 85 percent—is military or other non-civilian material and remains outside any of the existing international nuclear security mechanisms.

Most Nuclear Materials Are Outside International Mechanisms



In 2011, the total weapons-usable nuclear material inventory was estimated at 1,440 metric tons of HEU and 495 metric tons of separated plutonium (IPFM). Of this, 1,400 metric tons of HEU and 240 metric tons of plutonium were estimated to be outside of civilian programs. The estimated range of uncertainty regarding the total quantity of materials was ±140 metric tons.

About 85 percent of the global stocks of weapons-usable nuclear materials are outside civilian programs.

Those weapons-usable nuclear materials include the vast majority of highly enriched uranium (HEU) and about half the total amount of separated plutonium in the world, which are located in nine nuclear-armed states. Because the materials are categorized as military or non-civilian, they are not subject to International Atomic Energy Agency guidelines or to the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment, which apply only to civilian materials. If the world is to gain confidence in the security of such materials, they must be subject to best-practice exchanges, information sharing, peer review, or other voluntary mechanisms.

A truly comprehensive global nuclear security system would include all weapons-usable nuclear materials, not just the 15 percent in civilian programs.

What Is Military or Other Non-Civilian Material?

Material categorized as military or non-civilian is diverse and can be found in different forms, at different facilities, and for different uses. Most is located in the United States and Russia.

Many believe that military and other non-civilian materials are under military protection, and they assume that such materials are better protected than are those in civilian programs. However, that assumption is not necessarily the case. For example, in the United States, some of that material is in the custody of the U.S. Department of Energy and is protected by civilian security contractors. Even material under

military control is not perfectly secured, and measures can be improved.
Certain incidents—such as the serious security breach at the HEU storage facility at the Y-12 National Security Complex in Oak Ridge, Tennessee, and the removal of the deputy commander of the U.S. Strategic Command, which oversees all U.S. nuclear weapons, because of gambling-related allegations that called into question his reliability—suggest that it is dangerous and inappropriate to take the security of those materials for granted. Insider and outsider threats are real for those material inventories.

The Summit Process
The 2010 and 2012 Nuclear Security Summits reaffirmed the "fundamental responsibility of states … to maintain effective security of all nuclear materials, which includes nuclear materials used in nuclear weapons, and nuclear facilities under their control." NTI recommends that leaders at the 2014 summit act on this statement and begin to explore mechanisms to provide greater confidence about the security of military or non-civilian materials. There is clearly a need to protect sensitive information about such material. The United States and Russia have developed some limited but important models for assurances that could provide a template for how other nuclear-armed states could provide confidence in the security of their military or other non-civilian materials.

How the NTI Index Accounts for These Materials
The NTI Index includes all weapons-usable nuclear materials and does not distinguish the 85 percent in military or other non-civilian use from the 15 percent of material in civilian use. However, the EIU uses different measures, proxies, or assumptions when assessing the security of military or non-civilian material because of the lack of public information about this category.

▶ **Explore NTI's interactive map at:** http://ntiindex.org/data-results/interactive-map/

North Korea 'may have restarted Yongbyon nuclear reactor'

Source: http://www.bbc.com/news/world-asia-32529406

Apr 30 – **A US think-tank says satellite pictures taken earlier this year suggest North Korea may have restarted one of its nuclear reactors.**

The Institute for Science and International Security says images of the Yongbyon plant show patterns of melting snow indicating new activity.
Yongbyon's reactor was shut down in 2007 but was restarted in 2013.
Six-nation talks aimed at ending North Korea's nuclear programme have been stalled since early 2009.

The think-tank's report says that its assessment in late 2014 was that the reactor at Yongbyon, in the country's west, had been "shut down or partially shut down" but more recent images suggested the plant "may be operating at low power or intermittently".
As well as the patterns of melting snow, the satellite photos are also said to capture a stream of warm water coming out of the reactor's discharge pipeline and steam rising off the turbine.
In 2008, North Korea walked away from six-party talks with South Korea, the US, China, Japan and Russia on its denuclearisation.
The other countries have since tried to persuade North Korea to return to the negotiating table.
Earlier this year North Korea offered to stop nuclear tests if the US stopped holding military drills with Seoul, but the offer was rejected.
North Korea has conducted three nuclear tests, in 2006, 2009 and 2013.
Also on Thursday, Russia said the North Korean leader Kim Jong-un had cancelled his plans to attend World War Two victory commemorations in Moscow.
The visit next week would have been his first trip abroad since taking power three years ago. However, a Kremlin spokesman said Mr Kim had decided to stay in North Korea due to "internal issues".

Analysis: Jonathan Marcus, BBC diplomatic correspondent

North Korea often boasts of its "nuclear deterrent" in state-run media
This study is a powerful reminder that North Korea's nuclear weapons programme has not gone away.
It also shows the important role that independent analysts with access to civilian satellite imagery can play in helping to publicise what previously would have been top secret material available only to a handful of governments.
The winter snow and ice provides a helpful environment to reveal tell-tale signs that the Yongbyon reactor may have restarted. There's still considerable uncertainty about the scale of North Korea's nuclear arsenal.
Recently Chinese nuclear experts provided their US counterparts with a new assessment of North Korea's nuclear capabilities suggesting it may already have 20 warheads with the capacity to double this total by next year. US estimates are much more conservative.
It means that over the past 12 years Pyongyang has developed an expanding arsenal which many see as a significant threat to the region.

Mexico Recovers Stolen Radioactive Material

Source: http://www.ndtv.com/world-news/mexico-recovers-stolen-radioactive-material-757403

Apr 23 – A toolbox-sized container with radioactive material that was stolen last week from a truck in southeastern Mexico was found Wednesday abandoned under a bridge, authorities said.

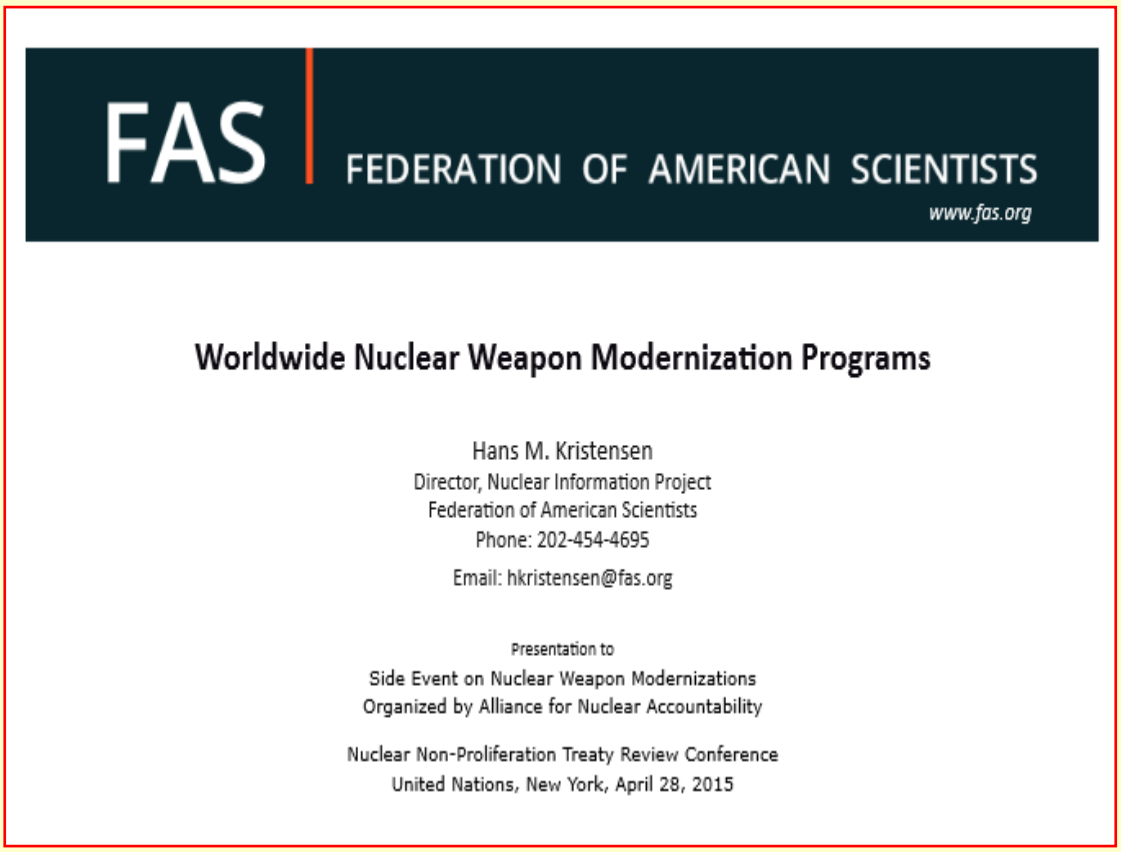
The April 13 theft of the box carrying Iridium-192 in Cardenas, Tabasco state, marked the fourth time since 2013 that robbers snatched radioactive material in Mexico.
"There are no signs that the container was opened," Christian Romero, deputy director for radiological emergencies at the national nuclear commission, told AFP.
Officials had stressed that the source posed no threat as long as it was kept under seal.
Officials believe that, like in the previous three cases, the thieves were unaware that they had stolen a radioactive source and were more interested in stealing the truck and other goods. The material was recovered every time.

National civil protection coordinator Luis Felipe Puente said the Iridium-192 source was "under guard" after the National Nuclear Safety and Safeguards Commission confirmed that it was recovered.
Iridium-192 is used for industrial radiography to check welding seams. The theft had prompted authorities to issue alerts and activate federal forces in five southern and eastern states.
It can cause burns, radiation sickness and permanent injury if a person comes in contact with it for minutes or hours. It is fatal if exposure lasts hours or days.

The theft was reported by the company Garantia Radiografica e Ingenieria.
The container was found near Tabasco's capital, Villahermosa, Romero said. The state government reported that it was abandoned under a bridge.
The night of the theft, the robbers had taken the container along with other objects inside the radiology company truck, which had been parked in the parking lot of a residential area in Cardenas.
The thieves left that vehicle alone and fled in another stolen truck.

Previous radioactive alerts

Nuclear commission officials say companies are not required to have a security detail accompany material like Iridium-192. Security forces do escort more lethal material.
The biggest scare came in **December 2013,** when thieves took a truck containing a cancer-treating medical device with highly radioactive cobalt-60 near Mexico City.
Authorities arrested and hospitalized five suspects in that case after recovering the potentially lethal material, which the thieves intended to sell as scrap metal. They all survived.
That theft prompted the International Atomic Energy Agency to issue an alert for "extremely dangerous" material while US officials kept tabs on the situation.
More recently, **in February 2015**, authorities recovered three stolen trucks in central Mexico transporting radioactive material for industrial use.
A similar incident took place in July 2014, also without causing harm to the population.


FAS | FEDERATION OF AMERICAN SCIENTISTS
www.fas.org

Worldwide Nuclear Weapon Modernization Programs

Hans M. Kristensen
Director, Nuclear Information Project
Federation of American Scientists
Phone: 202-454-4695
Email: hkristensen@fas.org

Presentation to
Side Event on Nuclear Weapon Modernizations
Organized by Alliance for Nuclear Accountability

Nuclear Non-Proliferation Treaty Review Conference
United Nations, New York, April 28, 2015

Source: http://fas.org/wp-content/uploads/2014/05/Brief2015_NPT1a.pdf

Britain Reports Active Nuclear Procurement Involving Sanctioned Companies

Source: http://www.iranwatch.org/our-publications/nuclear-iran-weekly/britain-reports-active-nuclear-procurement-involving-sanctioned-companies

May 05 – The British government informed the U.N. Panel of Experts in April of "an active Iranian nuclear procurement network" involving two blacklisted Iranian companies, according to a *Reuters* report published on April 30. If confirmed, Iran's continuing efforts to procure uranium enrichment technology would represent a violation of U.N. Security Council resolutions and once again raise the question of how illicit procurement will be handled in a comprehensive nuclear deal with Iran.

A draft of the U.N. Panel's annual report, according to Reuters, disclosed: "The UK government informed the Panel on 20 April 2015 that it 'is aware of an active Iranian nuclear procurement network which has been associated with **Iran's Centrifuge Technology Company (TESA) and Kalay Electric Company (KEC).** Kalaye Electric is under U.N. Security Council sanctions, while TESA has been sanctioned by the United States and European Union. Both companies have been linked to Iran's uranium enrichment program. The report did not offer any additional details, and the Panel said the information had been received too recently to be independently verified.

Kalaye Electric, based in Tehran, has long been associated with Iran's uranium enrichment program and was among the first entities sanctioned by the U.N. Security Council in 2006. A state-owned company subordinate to the Atomic Energy Organization of Iran, Kalaye Electric was the primary site for the assembly and testing of IR-1 centrifuges between 1997 and 2002 until operations were moved to Natanz. It supplied the Pilot Fuel Enrichment Plant at Natanz and was also responsible for the construction of the Fordow Fuel Enrichment Plant. Kalaye Electric had operated in secret until it was discovered and declared to the International Atomic Energy Agency (IAEA) in 2003. The facility lived on as a centrifuge research workshop and contributed to the development of the IR-2, IR-3, IR-4, and IR-5 centrifuge designs.

According to *Wired* reporter Kim Zetter's 2014 book, *Countdown to Zero Day*, Kalaye Electric was targeted in a May 2010 attack by the Stuxnet computer worm, reportedly as a means of spreading Stuxnet to Natanz.

TESA manufactures centrifuge parts and, according to the U.S. Treasury Department, "plays a crucial role in Iran's uranium enrichment nuclear program." The company is involved in the production of Iran's IR-1 centrifuges, operates an assembly complex at Natanz, and carries out work for Kalaye Electric. TESA was sanctioned by the European Union in 2010 and by the United States in 2011.

The British government's warning to the U.N. Panel of Experts is the latest sign of Iran's continued defiance of U.N. Security Council resolutions, which prohibit Iran's access to proliferation-sensitive items. Just last month, the U.S. Justice Department indicted four companies and five individuals for participating in an illicit Iranian procurement network that conspired to circumvent export controls on dual-use goods. TESA, in fact, was named as a client of one of the indicted companies. The framework agreement for the nuclear deal with Iran reportedly includes a dedicated procurement channel for Iran's nuclear program. But how will the agreement deal with violations, if Iran continues to rely upon its existing procurement networks to supply its nuclear program?

Nuclear forensics science helps thwart terrorist use of nuclear materials

Source: http://www.homelandsecuritynewswire.com/dr20150507-nuclear-forensics-science-helps-thwart-terrorist-use-of-nuclear-materials

There's still much too much material — nuclear, chemical, biological — being stored without enough protection. There are still terrorists and criminal gangs doing everything they can to get their hands on it. And make no mistake, if they get it, they will use it; potentially killing hundreds of thousands of innocent people, perhaps triggering a global crisis.

–President Barack Obama, National War College, 2012

A nuclear weapon in the hands of terrorists is the stuff of nightmares, especially for U.S. agencies charged with preventing a devastating attack. When security or law enforcement agents confiscate nuclear or radiological weapons or their ingredients being smuggled domestically or internationally, they must quickly trace them back to their source.

This is where **the science of nuclear forensics** comes in. Defined by the U.S. Department of Homeland Security as "the ability to trace the source of interdicted materials to their place of origin," nuclear forensics ranks as a "keystone" of U.S. anti-terrorism policy.

Now, Oregon State University is about to become a player in that effort. An OSU release reports that a new graduate emphasis in nuclear forensics is being launched in OSU's Department of Nuclear Engineering and Radiation Health Physics with funding from Homeland Security. Courses in nuclear materials science, nuclear forensics analysis, and detection of special nuclear material will be added to existing core courses such as radiophysics, radiochemistry, and applied radiation safety. Faculty expertise in nuclear engineering, radiation health physics, radiation detection, and radiochemistry will anchor the program, along with state-of-the-art lab and spectroscopy facilities in the Radiation Center, says OSU researcher Camille Palmer, who will lead the nuclear forensics emphasis.

Brittany Robertson, who holds bachelor's degrees in chemistry and psychology from Carnegie Mellon University, is poised to become the first OSU student to earn a Ph.D. in this up-and-coming field — just as soon as she finishes her master's in nuclear chemistry.

"The use of nuclear materials in several capacities is being pursued, and the reality of the world is that not everyone doing so has honorable intentions," says Robertson. "I believe in being proactive so that we don't have to be reactive. A nuclear tragedy anywhere, whether intentional or accidental, has the potential to affect everywhere."

Nuclear forensics (NF) is critical in interdiction of nuclear or radiological materials as well as analysis of post-detonation radioactive debris, according to Homeland Security. Through NF analyses, it's possible to determine the physical, chemical, elemental, and isotopic characteristics of nuclear and radiological materials to identify how and where they were created.

"Almost by definition, nuclear forensics combines problem solving with innovation to form a field in which engineers, chemists, computer scientists, physicists, policymakers, diplomats, and others must work together to achieve something much bigger than themselves," Robertson observes.

She says OSU's nuclear forensics emphasis was launched at an ideal time for her. "I originally wanted to pursue a route similar to this one, but I couldn't find a school with this nuclear forensics path when I first applied to graduate school," she explains. "The fact that one is currently being developed, and I have the opportunity to be a part of it, is pretty amazing."

Camille Palmer emphasizes OSU's strengths this way: "Oregon State is one of a handful of universities in the world positioned to make a significant impact in nuclear forensics education and research. Our human capital, facilities and proximity to U.S. national laboratories make us a natural fit for a forensics program, and our goal is to continue to strengthen research collaborations to ensure that we are consistently relevant and productive in this field."

Chernobyl: the true scale of the accident

20 Years Later a UN Report Provides Definitive Answers and Ways to Repair Lives

Joint News Release WHO/IAEA/UNDP

Source: http://www.who.int/mediacentre/news/releases/2005/pr38/en/

5 September 2005 | Geneva - A total of up to 4000 people could eventually die of radiation exposure from the Chernobyl nuclear power plant (NPP) accident nearly 20 years ago, an international team of more than 100 scientists has concluded.

As of mid-2005, however, fewer than 50 deaths had been directly attributed to radiation from the disaster, almost all being highly exposed rescue workers, many who died within months of the accident but others who died as late as 2004.

The new numbers are presented in a landmark digest report, "Chernobyl's Legacy: Health, Environmental and Socio-Economic Impacts," just released by the Chernobyl Forum. The digest, based on a three-volume, 600-page report and incorporating the work of hundreds of scientists, economists and health experts, assesses the 20-year impact of the largest nuclear accident in history. The Forum is made up of 8 UN specialized agencies, including the International Atomic Energy Agency (IAEA), World Health Organization (WHO), United Nations Development Programme (UNDP), Food and Agriculture Organization (FAO), United Nations Environment Programme (UNEP), United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA), United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR), and the World Bank, as well as the governments of Belarus, the Russian Federation and Ukraine.

"This compilation of the latest research can help to settle the outstanding questions about how much death, disease and economic fallout really resulted from the Chernobyl accident," explains Dr. Burton Bennett, chairman of the Chernobyl Forum and an authority on radiation effects. "The governments of the three most-affected countries have realized that they need to find a clear way forward, and that progress must be based on a sound consensus about environmental, health and economic consequences and some good advice and support from the international community."

Bennett continued: "This was a very serious accident with major health consequences, especially for thousands of workers exposed in the early days who received very high radiation doses,

and for the thousands more stricken with thyroid cancer. By and large, however, we have not found profound negative health impacts to the rest of the population in surrounding areas, nor have we found widespread contamination that would continue to pose a substantial threat to human health, within a few exceptional, restricted areas."

The Forum's report aims to help the affected countries understand the true scale of the accident's consequences and also suggests ways the governments of Belarus, the Russian Federation and Ukraine might address major economic and social problems stemming from the accident. Members of the Forum, including representatives of the three governments, will meet September 6 and 7 in Vienna at an unprecedented gathering of the world's experts on Chernobyl, radiation effects and protection, to consider these findings and recommendations.

Major study findings

Dozens of important findings are included in the massive report:

- Approximately 1000 on-site reactor staff and emergency workers were heavily exposed to high-level radiation on the first day of the accident; among the more than 200 000 emergency and recovery operation workers exposed during the period from 1986-1987, an estimated 2200 radiation-caused deaths can be expected during their lifetime.
- An estimated five million people currently live in areas of Belarus, Russia and Ukraine that are contaminated with radionuclides due to the accident; about 100 000 of them live in areas classified in the past by government authorities as areas of "strict control". The existing "zoning" definitions need to be revisited and relaxed in light of the new findings.
- About 4000 cases of thyroid cancer, mainly in children and adolescents at the time of the accident, have resulted from the accident's contamination and at least nine children died of thyroid cancer; however the survival rate among such cancer victims, judging from experience in Belarus, has been almost 99%.
- Most emergency workers and people living in contaminated areas received relatively low whole body radiation doses, comparable to natural background levels. As a consequence, no evidence or likelihood of decreased fertility among the affected population has been found, nor has there been any evidence of increases in congenital malformations that can be attributed to radiation exposure.
- Poverty, "lifestyle" diseases now rampant in the former Soviet Union and mental health problems pose a far greater threat to local communities than does radiation exposure.
- Relocation proved a "deeply traumatic experience" for some 350,000 people moved out of the affected areas. Although 116 000 were moved from the most heavily impacted area immediately after the accident, later relocations did little to reduce radiation exposure.
- Persistent myths and misperceptions about the threat of radiation have resulted in "paralyzing fatalism" among residents of affected areas.
- Ambitious rehabilitation and social benefit programs started by the former Soviet Union, and continued by Belarus, Russia and Ukraine, need reformulation due to changes in radiation conditions, poor targeting and funding shortages.
- Structural elements of the sarcophagus built to contain the damaged reactor have degraded, posing a risk of collapse and the release of radioactive dust;
- A comprehensive plan to dispose of tons of high-level radioactive waste at and around the Chernobyl NPP site, in accordance with current safety standards, has yet to be defined.

Alongside radiation-induced deaths and diseases, the report labels the mental health impact of Chernobyl as "the largest public health problem created by the accident" and partially attributes this damaging psychological impact to a lack of accurate information. These problems manifest as negative self-assessments of health, belief in a shortened life expectancy, lack of initiative, and dependency on assistance from the state.

"Two decades after the Chernobyl accident, residents in the affected areas still lack the information they need to lead the healthy and productive lives that are possible," explains Louisa Vinton, Chernobyl focal point at the UNDP. "We are advising our partner governments that they must reach people with accurate information, not only about how to live safely in

regions of low-level contamination, but also about leading healthy lifestyles and creating new livelihoods." But, says Dr Michael Repacholi, Manager of WHO's Radiation Program, "the sum total of the Chernobyl Forum is a reassuring message."

He explains that there have been 4000 cases of thyroid cancer, mainly in children, but that except for nine deaths, all of them have recovered. "Otherwise, the team of international experts found no evidence for any increases in the incidence of leukemia and cancer among affected residents."

The international experts have estimated that radiation could cause up to about 4000 eventual deaths among the higher-exposed Chernobyl populations, i.e., emergency workers from 1986-1987, evacuees and residents of the most contaminated areas. This number contains both the known radiation-induced cancer and leukaemia deaths and a statistical prediction, based on estimates of the radiation doses received by these populations. As about quarter of people die from spontaneous cancer not caused by Chernobyl radiation, the radiation-induced increase of only about 3% will be difficult to observe. However, in the most exposed cohorts of emergency and recovery operation workers some increase of particular cancer forms (e.g., leukemia) in particular time periods has already been observed. The predictions use six decades of scientific experience with the effects of such doses, explained Repacholi.

Repacholi concludes that "the health effects of the accident were potentially horrific, but when you add them up using validated conclusions from good science, the public health effects were not nearly as substantial as had at first been feared."

The report's estimate for the eventual number of deaths is far lower than earlier, well-publicized speculations that radiation exposure would claim tens of thousands of lives. But the 4000 figure is not far different from estimates made in 1986 by Soviet scientists, according to Dr Mikhail Balonov, a radiation expert with the International Atomic Energy Agency in Vienna, who was a scientist in the former Soviet Union at the time of the accident.

As for environmental impact, the reports are also reassuring, for the scientific assessments show that, except for the still closed, highly contaminated 30 kilometer area surrounding the reactor, and some closed lakes and restricted forests, radiation levels have mostly returned to acceptable levels. "In most areas the problems are economic and psychological, not health or environmental," reports Balonov, the scientific secretary of the Chernobyl Forum effort who has been involved with Chernobyl recovery since the disaster occurred.

Recommendations

Recommendations call for focusing assistance efforts on highly contaminated areas and redesigning government programs to help those genuinely in need. Suggested changes would shift programs away from those that foster "dependency" and a "victim" mentality, and replacing them with initiatives that encourage opportunity, support local development, and give people confidence in their futures.

In the health area, the Forum report calls for continued close monitoring of workers who recovered from Acute Radiation Syndrome (ARS) and other highly exposed emergency personnel. The Report also calls for focused screening of children exposed to radioiodine for thyroid cancer and highly exposed clean-up workers for non-thyroid cancers. However, existing screening programs should be evaluated for cost-effectiveness, since the incidence of spontaneous thyroid cancers is increasing significantly as the target population ages. Moreover, high quality cancer registries need continuing government support.

In the environmental realm, the Report calls for long term monitoring of caesium and strontium radionuclides to assess human exposure and food contamination and to analyse the impacts of remedial actions and radiation-reduction countermeasures. Better information needs to be provided to the public about the persistence of radioactive contamination in certain food products and about food preparation methods that reduce radionuclide intake. Restrictions on harvesting of some wild food products are still needed in some areas.

Also in the realm of protecting the environment, the Report calls for an "integrated waste management program for the Shelter, the Chernobyl NPP site and the Exclusion Zone" to ensure application of consistent management and capacity for all types of radioactive waste. Waste storage and disposal must be dealt with in a comprehensive manner across the entire Exclusion Zone, according to the Report.

In areas where human exposure is not high, no remediation needs to be done, points out Balonov. "If we do not expect health or environmental effects, we should not waste resources and effort on low priority, low contamination areas," he explains. "We need to focus our efforts and resources on real problems."

One key recommendation addresses the fact that large parts of the population, especially in rural areas, still lack accurate information and emphasizes the need to find better ways both to inform the public and to overcome the lack of credibility that hampered previous efforts. Even though accurate information has been available for years, either it has not reached those who need it or people do not trust and accept the information and do not act upon it, according to the Report.

This recommendation calls for targeting information to specific audiences, including community leaders and health care workers, along with a broader strategy that promotes healthy lifestyles as well as information about how to reduce internal and external radiation exposures and address the main causes of disease and mortality.

In the socioeconomic sphere, the Report recommends a new development approach that helps individuals to "take control of their own lives and communities to take control of their own futures." The Governments, the Report states, must streamline and refocus Chernobyl programs through more targeted benefits, elimination of unnecessary benefits to people in less contaminated areas, improving primary health care, support for safe food production techniques, and encouragement for investment and private sector development, including small and medium-size enterprises.

Notes Vinton, "The most important need is for accurate information on healthy lifestyles, together with better regulations to promote small, rural businesses. Poverty is the real danger. We need to take steps to empower people."

Answers to Longstanding Questions

How much radiation were people exposed to as a result of the accident?

With the exception of on-site reactor staff and emergency workers exposed on 26 April, most recovery operation workers and those living in contaminated territories received relatively low whole body radiation doses, comparable to background radiation levels and lower than the average doses received by residents in some parts of the world having high natural background radiation levels.

For the majority of the five million people living in the contaminated areas, exposures are within the recommended dose limit for the general public, though about 100 000 residents still receive more. Remediation of those areas and application of some agricultural countermeasures continues. Further reduction of exposure levels will be slow, but most exposure from the accident has already occurred.

How many people died and how many more are likely to die in the future?

The total number of deaths already attributable to Chernobyl or expected in the future over the lifetime of emergency workers and local residents in the most contaminated areas is estimated to be about 4000. This includes some 50 emergency workers who died of acute radiation syndrome and nine children who died of thyroid cancer, and an estimated total of 3940 deaths from radiation-induced cancer and leukemia among the 200 000 emergency workers from 1986-1987, 116 000 evacuees and 270 000 residents of the most contaminated areas (total about 600 000). These three major cohorts were subjected to higher doses of radiation amongst all the people exposed to Chernobyl radiation.

The estimated 4000 casualties may occur during the lifetime of about 600 000 people under consideration. As about quarter of them will eventually die from spontaneous cancer not caused by Chernobyl radiation, the radiation-induced increase of about 3% will be difficult to observe. However, in the most highly exposed cohorts of emergency and recovery operation workers, some increase in particular cancers (e.g., leukemia) has already been observed.

Confusion about the impact has arisen owing to the fact that thousands of people in the affected areas have died of natural causes. Also, widespread expectations of ill health and a tendency to attribute all health problems to radiation exposure have led local residents to assume that Chernobyl related fatalities were much higher than they actually were.

What diseases have already occurred or might occur in the future?
Residents who ate food contaminated with radioactive iodine in the days immediately after the accident received relatively high doses to the thyroid gland. This was especially true of children who drank milk from cows who had eaten contaminated grass. Since iodine concentrates in the thyroid gland, this was a major cause of the high incidence of thyroid cancer in children.
Several recent studies suggest a slight increase in the incidence of leukemia among emergency workers, but not in children or adult residents of contaminated areas. A slight increase in solid cancers and possibly circulatory system diseases was noted, but needs to be evaluated further because of the possible indirect influence of such factors as smoking, alcohol, stress and unhealthy lifestyle.

Have there been or will there be any inherited or reproductive effects?
Because of the relatively low doses to residents of contaminated territories, no evidence or likelihood of decreased fertility has been seen among males or females. Also, because the doses were so low, there was no evidence of any effect on the number of stillbirths, adverse pregnancy outcomes, delivery complications or overall health of children. A modest but steady increase in reported congenital malformations in both contaminated and uncontaminated areas of Belarus appears related to better reporting, not radiation.

Did the trauma of rapid relocation cause persistent psychological or mental health problems?
Stress symptoms, depression, anxiety and medically unexplained physical symptoms have been reported, including self-perceived poor health. The designation of the affected population as "victims" rather than "survivors" has led them to perceive themselves as helpless, weak and lacking control over their future. This, in turn, has led either to over cautious behavior and exaggerated health concerns, or to reckless conduct, such as consumption of mushrooms, berries and game from areas still designated as highly contaminated, overuse of alcohol and tobacco, and unprotected promiscuous sexual activity.

What was the environmental impact?
Ecosystems affected by Chernobyl have been studied and monitored extensively for the past two decades. Major releases of radionuclides continued for ten days and contaminated more than 200 000 square kilometers of Europe. The extent of deposition varied depending on whether it was raining when contaminated air masses passed.
Most of the strontium and plutonium isotopes were deposited within 100 kilometres of the damaged reactor. Radioactive iodine, of great concern after the accident, has a short half-life, and has now decayed away. Strontium and caesium, with a longer half life of 30 years, persist and will remain a concern for decades to come. Although plutonium isotopes and americium 241 will persist perhaps for thousands of years, their contribution to human exposure is low.

What is the scope of urban contamination?
Open surfaces, such as roads, lawns and roofs, were most heavily contaminated. Residents of Pripyat, the city nearest to Chernobyl, were quickly evacuated, reducing their potential exposure to radioactive materials. Wind, rain and human activity has reduced surface contamination, but led to secondary contamination of sewage and sludge systems. Radiation in air above settled areas returned to background levels, though levels remain higher where soils have remained undisturbed.

How contaminated are agricultural areas?
Weathering, physical decay, migration of radionuclides down the soil and reductions in bioavailability have led to a significant reduction in the transfer of radionuclides to plants and animals. Radioactive iodine, rapidly absorbed from grasses and animal feed into milk, was an early concern and elevated levels were seen in some parts of the former Soviet Union and Southern Europe, but, given the nuclide's short half life, this concern abated quickly. Currently and for the long term, radiocaesium, present in milk, meat and some plant foods, remains the most significant concern for internal human exposure, but, with the exception of a few areas, concentrations fall within safe levels.

What is the extent of forest contamination?

Following the accident, animals and vegetation in forest and mountain areas had high absorption of radiocaesium, with persistent high levels in mushrooms, berries and game. Because exposure from agricultural products has declined, the relative importance of exposure from forest products has increased and will only decline as radioactive materials migrate downward into the soil and slowly decay. The high transfer of radiocaesium from lichen to reindeer meat to humans was seen in the Artic and sub-Arctic areas, with high contamination of reindeer meat in Finland, Norway, Russia, and Sweden. The concerned governments imposed some restrictions on hunting, including scheduling hunting season when animals have lower meat contamination.

How contaminated are the aquatic systems?

Contamination of surface waters throughout much of Europe declined quickly through dilution, physical decay, and absorption of radionuclides in bed sediments and catchment soils. Because of bioaccumulation in the aquatic food chain, though, elevated concentrations of radiocaesium were found in fish from lakes as far away as Germany and Scandinavia. Comparable levels of radiostrontium, which concentrates in fish bone, not in muscle, were not significant for humans. Levels in fish and waters are currently low, except in areas with "closed" lakes with no outflowing streams. In those lakes, levels of radiocaesium in fish will remain high for decades and, therefore, restrictions on fishing there should be maintained.

What environmental countermeasures and remediation have been taken?

The most effective early agricultural countermeasure was removing contaminated pasture grasses from animal diets and monitoring milk for radiation levels. Treatment of land for fodder crops, clean feeding and use of Cs-binders (that prevented the transfer of radiocaesium from fodder to milk) led to large reductions in contamination and permitted agriculture to continue, though some increase in radionuclide content of plant and animal products has been measured since the mid-1990s when economic problems forced a cutback in treatments. Some agricultural lands in the three countries have been taken out of use until remediation is undertaken.

A number of measures applied to forests in affected countries and in Scandinavia have reduced human exposure, including restrictions on access to forest areas, on harvesting of food products such as game, berries and mushrooms, and on the public collection of firewood, along with changes in hunting to avoid consumption of game meat where seasonal levels of radiocaesium may be high. Low income levels in some areas cause local residents to disregard these rules.

What were radiation-induced effects on plants and animals?

Increased mortality of coniferous plants, soil invertebrates and mammals and reproductive losses in plants and animals were seen in high exposure areas up to a distance of 20-30 kilometers. Outside that zone, no acute radiation-induced effects have been reported. With reductions of exposure levels, biological populations have been recovering, though the genetic effects of radiation were seen in both somatic and germ cells of plants and animals. Prohibiting agricultural and industrial activities in the exclusion zone permitted many plant and animal populations to expand and created, paradoxically, "a unique sanctuary for biodiversity."

Does dismantlement of the Shelter and management of radioactive waste pose further environmental problems?

The protective shelter was erected quickly, which led to some imperfections in the shelter itself and did not permit gathering complete data on the stability of the damaged unit. Also, some structural parts of the shelter have corroded in the past two decades. The main potential hazard posed by the shelter is the possible collapse of its top structures and the release of radioactive dust.

Strengthening those unstable structures has been performed recently, and construction of a New Safe Confinement covering the existing shelter that should serve for more than 100 years, starts in near future. The new cover will allow dismantlement of the current shelter, removal of the radioactive fuel mass from the damaged unit and, eventually, decommissioning of the damaged reactor.

A comprehensive strategy still has to be developed for dealing with the high level and long-lived radioactive waste from past remediation activities. Much of this waste was placed in temporary storage in trenches and landfills that do not meet current waste safety requirements.

What was the economic cost?

Because of policies in place at the time of the explosion and the inflation and economic disruptions that followed the break-up of the Soviet Union, precise costs have been impossible to calculate. A variety of estimates from the 1990s placed the costs over two decades at hundreds of billions of dollars. These costs included direct damage, expenditures related to recovery and mitigation, resettlement of people, social protection and health care for the affected population, research on environment, health and the production of clean food, radiation monitoring, as well as indirect losses due to removing agricultural lands and forests from use and the closing of agriculture and industrial facilities, and such additional costs as cancellation of the nuclear power program in Belarus and the additional costs of energy from the loss of power from Chernobyl. The costs have created a huge drain on the budgets of the three countries involved.

What were the main consequences for the local economy?

Agriculture was hardest hit, with 784 320 hectares taken from production. Timber production was halted in 694,200 hectares of forest. Remediation made "clean food" production possible in many areas but led to higher costs in the form of fertilizers, additives and special cultivation processes. Even where farming is safe, the stigma associated with Chernobyl caused marketing problems and led to falling revenues, declining production and the closure of some facilities. Combined with disruptions due to the collapse of the Soviet Union, recession, and new market mechanisms, the region's economy suffered, resulting in lower living standards, unemployment and increased poverty. All agricultural areas, whether affected by radiation or not, proved vulnerable.

Poverty is especially acute in affected areas. Wages for agricultural workers tend to be low and employment outside of agriculture is limited. Many skilled and educated workers, especially younger workers, left the region. Also, the business environment discourages entrepreneurial ventures and private investment is low.

What impact did Chernobyl and the aftermath have on local communities?

More than 350 000 people have been relocated away from the most severely contaminated areas, 116 000 of them immediately after the accident. Even when people were compensated for losses, given free houses and a choice of resettlement location, the experience was traumatic and left many with no employment and a belief that they have no place in society. Surveys show that those who remained or returned to their homes coped better with the aftermath than those who were resettled. Tensions between new and old residents of resettlement villages also contributed to the ostracism felt by the newcomers. The demographic structure of the affected areas became skewed since many skilled, educated and entrepreneurial workers, often younger, left the areas leaving behind an older population with few of the skills needed for economic recovery.

The older population has meant that deaths exceed births, which reinforces the perception that these areas are dangerous places to live. Even when pay is high, schools, hospitals and other essential public services are short of qualified specialists.

What has been the impact on individuals?

According to the Forum's report on health, "the mental health impact of Chernobyl is the largest public health problem unleashed by the accident to date." People in the affected areas report negative assessments of their health and well-being, coupled with an exaggerated sense of the danger to their health from radiation exposure and a belief in a shorter life expectancy. Anxiety over the health effects of radiation shows no signs of diminishing and may even be spreading. Life expectancy has been declining across the former Soviet Union, due to cardiovascular disease, injuries and poisoning, and not radiation-related illness.

How have governments responded?

The resettlement and rehabilitation programs launched in Soviet conditions proved unsustainable after 1991 and funding for projects declined, leaving many projects unfinished and abandoned and many of the promised benefits under funded. Also, benefits were offered to broad categories of "Chernobyl victims" that expanded to seven million now receiving or eligible for pensions, special allowances and health benefits, including free holidays and guaranteed allowances. Chernobyl benefits deprive other areas of public spending of resources, but scaling down benefits or targeting only high-risk groups is unpopular and presents political problems.

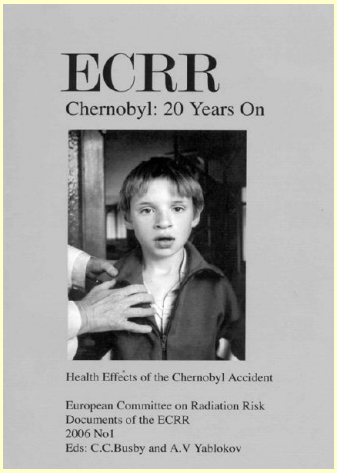
Given significant reduction of radiation levels during past twenty years, governments need to revisit the classification of contaminated zones. Many areas previously considered to be at risk are in fact safe for habitation and cultivation. Current delineations are far more restrictive than demonstrated radiation levels can justify.

The report identifies the need to sharpen priorities and streamline the programs to target the most needy, noting that reallocating resources is likely to face "strong resistance from vested interests". One suggestion calls for a "buy out" of the entitlement to benefits in return for lump sum start-up financing for small businesses.

ECRR - New Publication Reveals True Consequences of Radioactive Exposures (2006)

Source: http://www.euradcom.org/publications/chernobyleflyer.pdf

The Chernobyl accident contaminated large parts of the Soviet Union and Europe. Radioactivity was ultimately detected everywhere in the northern hemisphere. Doses to the emergency workers from external gamma-rays and internal fission-product radionuclides were significantly high, many died at the time. 20 years later, many liquidators still die and all are ill. The radionuclide contamination of the environment was significant and long-lasting. This resulted in chronic internal low dose exposure to millions of people, to animals and plants. Foodstuffs became contaminated with Caesium-137, Strontium-90 and uranium fuel particles containing a range of novel radioactive elements.



Rather than use this opportunity to investigate the health effects of these exposures, the international radiation risk community has ignored the many reports of ill-health emerging from the contaminated territories. International and National bodies (e.g. ICRP, UNSCEAR, BEIR, WHO), whose remit is the evaluation of ionising radiation effects on health, have glossed over, marginalized, ignored or denied the existence of the terrible consequences of the Chernobyl fallout. Research papers have been excluded from official reports. Cries for help have been dismissed as due to 'Radiophobia'.

Research into these effects has been mainly published in Russian language journals; these valuable contributions have (perhaps purposely) rarely been translated into English. To do so would have been fatal to the nuclear industry which routinely discharges the same radioactive substances into the environment under license.

This new ECRR publication presents the true consequences of the Chernobyl accident. Eminent scientists examine and review the data and show that, rather than fading away, the effects are only beginning to show themselves. The phenomenon of 'genomic instability', discovered in the laboratory in the UK in the 1990s, is seen now in its terrible effects on the animals, plants and human victims of the Chernobyl exposures. It is seen at doses that would have been, and still are, dismissed as vanishingly small by the current radiation protection laws.

Here are data from the real world: the world of the Chernobyl laboratory. The lessons contained in these chapters should be borne in mind by policy makers who are, even now, discussing new investments in nuclear energy and ways in which

historic and future radionuclide waste can be disposed of into the environment. The committee recommends this book to scientists, policymakers and concerned members of the public, in the hope that the huge amount of work carried out by scientists publishing their results in Russian language journals and others studying the effects of the Chernobyl accident will influence their decisions in this important area of public health.

CONTENTS

"In 20 years it has become clear that not tens, hundreds or thousands, but millions of people in the Northern hemisphere have suffered and will suffer from the Chernobyl catastrophe...
...Official secrecy (until May 23rd, 1989) and irreversible state falsification of medical data during the first three years after the catastrophe, as well as an absence of authentic medical statistics in the former USSR, highlights the inadequacy of material concerning primary epidemiological consequences of this catastrophe...
...The ... average age of 162 liquidators who died during last 10 years in the town of Tolliyaty (Samarskaya province, Russia) was about 46.2 years old (Tymonin, 2005). The average lifespan for 169 liquidators from nuclear industry institutes who died between 1986 – 1990 was 45.5 years (Tukov et al., 2000). In the Kaluga province - National register data, - the average age of death for 84.7 % of liquidators was only 30 - 39 years old (Lushnykov and Lanzov, 1999)... ***A.V. Yablokov***

"The dose dependence of the radiation effect may be non-linear, non-monotonic and polymodal in character...Over certain dose ranges, low-level irradiation is more effective with regard to the results of its action on an organism or a population than acute high-level radiation...
...Radiation-induced changes in the population structure result in an unpredictable response of the population to various events. In the work by A.P. Akif'ev et al. [12], an apparently healthy population of the posterity of exposed Drosophila exhibited a so-called 'populational breakdown' in one of its generations and was ruined by a law other than that for other generations. In the work by I.I. Pelevina et al. [13], it was shown that 15 generations of cells irradiated with the doses 10 to 50 cGy "remember" the irradiation and respond to external stimuli differently than the control...
....The results of surveys and biological monitoring of children and adults of Chernobyl point unambiguously to a steady, rapid and dramatic (for an individual human life) deterioration of health of all victims of the radiation impact of the Chernobyl accident..." ***E.B. Burlakova & A.G. Nazarov***

"According to a wide range of scientific data reviewed, the following hypotheses can be proposed: 1) exposure to low-dose ionizing radiation is a risk factor for accelerated aging processes and neurodegeneration; 2) aging and neurodegeneration processes after exposure to ionizing radiation could be enhanced by the synergetic influence of heterogeneous pathogenetic factors, such as immunological, oxidative stress and molecular-genetic changes." ***K.N. Loganovsky***

"The detected cytogenetic effects of chronic low-intensive irradiation in the germ and somatic cells of wild animals exceeded the expected levels deduced from extrapolation of the data from the high-dose range of acute or chronic irradiation. In wild murine rodents increased frequencies of cytogenetic injuries in somatic and germ cells, as well as embryonal lethality, were shown to remain over the life spans of no less than 22 generations (Goncharova & Ryabokon, 1998)..." ***E. Yu. Krysanov***

"In addition, a view of the radiobiological processes induced in plants by chronic irradiation should elucidate the main tendencies in the formation of late effects of irradiation. As this takes place we bear in mind that these late effects in plants could not be related to 'radio-phobia', as it is called, as there is a tendency to assign the cause of injuries observed after the Chernobyl catastrophe merely to a fear of irradiation. We have seen, since the accident, clear and diverse effects of irradiation in plants over time...
...It appears that there are two adaptive strategies to stress impacts in plants, namely; ontogenetic and population or phylogenetic adaptation. The first type of adaptive strategy is revealed by radioadaptation and resides in an augmentation of radioresistance after irradiation in low doses. The second type of adaptive strategy lies in an increase in frequency of genetic diversification, which enlarges the possibilities for active natural selection..." ***D.M. Grodzinsky***

"Using new infant leukaemia data from the UK supplied by the Childhood cancer research Group, Oxford, it is possible to combine the populations of Germany, Greece and the UK and carry out a meta analysis of infant leukaemia in those children who were in the womb at the time of the fallout. Using published exposure doses to the foetus the infant leukaemia yield in Europe is more than 160 times higher than that predicted on the basis of the external irradiation yields found by the obstetric X-ray data studies. This means that the ICRP risk model is in error here by a factor of at least 160. The dose response is biphasic..." ***C. Busby***

"Clearly, the true damage to health attributable to the Chernobyl disaster has been kept from the general public through poor and incomplete scientific investigation..." ***R. Bertell***

The European Committee on Radiation Risk was formed in 1997 following a resolution made at a conference in Brussels arranged by the Green Group in the European Parliament.
The ECRR's remit is:

- To independently estimate, based on its own evaluation of all scientific sources, in as much detail as necessary and using the most appropriate scientific framework, all of the risks arising from exposure to radiation, taking a precautionary approach.
- To develop the best scientific predictive model of detriment following exposure to radiation, presenting observations which appear to support or challenge this model, and highlighting areas of research which are needed to further complete the picture.
- To develop an ethical analysis and philosophical framework to form the basis of its policy recommendations, related to the state of scientific knowledge, lived experience and the Precautionary Principle.
- To present the risks and the detriment model, with the supporting analysis, in a manner to enable and assist transparent policy decisions to be made on radiation protection of the public and the wider environment.

The Committee now has more than 50 experts from many countries collaborating on the issue of radiation risk and has set up a number of sub-committees and groups. The Committee's risk model was presented in 2003 in Brussels and is published as the *ECRR2003 Recommendations: the Health Effects of Ionising Radiation Exposure at Low Dose for Radiation Protection Purposes: Regulators' Edition* (ISBN 1897761 24 4). The report, now in its second printing, has been widely circulated. It is published in French, Russian, Spanish and Japanese.
The Committee wishes to emphasise that the health phenomena described in the Chernobyl sub-Committee's present work are predicted and explained by the radiation risk model put forward in the *ECRR2003 Recommendations.* This is in marked contrast to the dissonance between the predictions of the International Commission

Cloud control: Climatologist Alan Robock on the effects of geoengineering and nuclear war

Source: http://bos.sagepub.com/content/71/3/1.abstract

Abstract

In this interview, Rutgers University climatologist Alan Robock talks with Elisabeth Eaves from the *Bulletin* about geoengineering and nuclear winter. He says that geoengineering is not the solution to global warming because of its many risks and unknowns. He notes that some of the technology that would be required to implement geoengineering has not been developed and that many socio-political questions would have to be resolved before it could be put into practice. The world would have to reach agreement on a target temperature and on what entity should do the implementing. Robock's biggest fear with regard to geoengineering is that disputes over these questions could escalate into nuclear war which in turn could cause nuclear winter, producing global famine among other effects. He goes on to describe his meeting with former Cuban President Fidel Castro and discuss the role of the arts in addressing existential threats.

Alan Robock's interest in climate science dates back to 1974, when his doctoral thesis advisor Edward Lorenz, the meteorologist known as the father of chaos theory, told him that "climate would be a good field to get into." Robock took the advice, and today he is a distinguished professor of climate science in the Department of Environmental Sciences at Rutgers University, where he also directs the undergraduate meteorology program. He served as a lead author for the Intergovernmental Panel on Climate Change's Fifth Assessment Report and is a vocal advocate for action on global warming.
Robock is an expert on the potential effects of geoengineering, those untried technologies aimed at manipulating the climate system in order to counter the effects of global warming. Interest in geoengineering has intensified since the National

Academy of Sciences released a report (http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=02102015) in February recommending federal funding for more research, including into what it calls "albedo-modification techniques," which would prevent sunlight from reaching Earth's surface. Robock doesn't think geoengineering is the right solution to climate change though, as he explains in this interview.

Robock is also one of the foremost experts on the potential climatic impacts of nuclear explosions. By producing smoke that blocks the sun's rays, a nuclear war could cause a nuclear winter, cooling the planet catastrophically and causing global famine. He calls nuclear weapons a more serious threat to humanity than global warming.

In this interview, conducted by contributing editor Elisabeth Eaves in January, Robock talks about geoengineering and nuclear winter, his encounters with the CIA and Fidel Castro, and what movie stars he thinks could best get his message across.

BAS: In the past, you've warned of geoengineering's potential dangers. Have any new techniques or studies led you to become more optimistic about it?

Robock: No. The solution to global warming is to stop putting out greenhouse gas. And we know how to do that. We have the technology. It's sun and wind. The problem is political, not technical.

If we try to compensate for warming with engineering projects on the only planet known to sustain intelligent life, it's still just too scary. If you could put a cloud in the stratosphere and maintain it there, it could cool the planet and counteract some of the negative aspects of global warming. But there are risks that haven't been addressed, such as how does the world decide what temperature it wants to be? What would happen if we started and then abruptly stopped, which could be catastrophic? Questions like these haven't been solved.

There's a new technique people are studying, which is to try to dissipate cirrus clouds to let heat escape. In theory, this doesn't come with some of the negative aspects of blocking out the sun. For example, it doesn't change precipitation patterns as drastically. But you would need fleets of airplanes to spray chemicals into the upper atmosphere, which is an undeveloped technology. I don't know of anybody who has come up with an idea of how to do it safely.

The one thing called geoengineering that probably is a good idea is to take carbon dioxide out of the atmosphere. Unfortunately, it has the same name—geoengineering—as these other proposals, but it's a completely different issue in terms of the technology, costs, and risks. If we could do it cheaply enough and find a place to store the carbon dioxide, that would take away the cause of global warming.

An even better idea, of course, is to not put the carbon dioxide in the atmosphere in the first place. You can do that by using energy more efficiently but also, if you're going to burn fossil fuels, by capturing the carbon dioxide out of the smokestack. It has a much higher concentration right when it leaves a fixed source than it does once it's free in the atmosphere, so it's much cheaper to capture.

BAS: Is there anything you fear could happen that would make geoengineering inevitable despite all its problems?

Robock: I don't really fear geoengineering because I don't think it's ever going to happen. There was a conference at Asilomar five years ago where a bunch of people got together and discussed the ethics of geoengineering. Robert Socolow, who is a professor at Princeton, went around asking people their greatest fears, and at the end of the week he read them off.

The greatest fear, which is also mine, was global nuclear war. Because if countries can't agree on what the temperature should be, and somebody is mad at somebody else for controlling their climate, the situation could escalate into hostilities. And different countries have different interests. People at high latitudes, like in Canada or Russia or maybe even the United States, might want to exploit the Arctic and send ships. So some people don't mind it a little bit warmer. But people in the Pacific, whose islands are sinking, want it to be cooler than it is today. They're already suffering. So there's a spectrum of different local impacts. I can't imagine how the world could agree on where to set the thermostat.

Let's say we get to the point where the feared emission of methane from the Arctic occurs, and the ocean starts bubbling up really fast, or there's even more catastrophic melting in Antarctica and Greenland. There might then be calls to implement

geoengineering until we get mitigation under control.

Once demand for geoengineering gets started, who's going to implement the process? Remember that whoever ends up doing it will have a huge financial interest in continuing to do it. Would you trust the planet to the BP Geoengineering Corporation, for example? I can't imagine the world agreeing.

BAS: So we might see calls for geoengineering, but then a fight about what to do?

Robock: Yes. People have said it's so cheap and easy that an individual could do it. Like, you know, Richard Branson is an environmentalist and he owns a lot of airplanes—how about him? But I find it hard to believe that any individual or country would do it. You could shoot their planes down once they started, so there's no way to do it without the agreement of the rest of the world. I guess a country could do it over its own territory.

Consultants for the CIA called me up four years ago and asked, "Could we detect somebody else trying to control our climate?" Well yeah, we could, because if somebody was creating a thin cloud in the lower stratosphere we could detect that with our current satellite and ground-based observational system. We can see the effects of various small volcanic eruptions. If somebody were sailing ships around the ocean brightening clouds, we could see the lines in the clouds with satellite imagery. And we could see the airplanes or the ships that were doing it. So it would be impossible to do it in secret.

Of course, what they were also asking is, "Can we control somebody else's climate?"

There's a big report on geoengineering [http://nas-sites.org/americasclimatechoices/public-release-event-climate-intervention-reports/] by the National Academy of Sciences that is being released. It was funded mainly by the CIA. The CIA asked several other agencies, like NASA and NOAA, to help fund it, so that the report would look like a joint effort, but I was told it was almost all the CIA, which goes by the "US intelligence community" in the report. What's wrong with this picture? The CIA wants to figure out how to control the globe's weather.

BAS: So they're taking it seriously.

Robock: I don't know what their motivations are. But the panel that did the report is very good. It's the top scientists, and I know a lot of them, and I reviewed part of the report. I don't think the report is influenced by the CIA. It seems like it was done very responsibly.

BAS: Are there other ethical issues raised by geoengineering you'd like to talk about?

Robock: Some people say we shouldn't do research because it's a slippery slope to deployment, or because it takes resources away from something more productive. But in my opinion, indoor geoengineering research—that is, studying data, studying past volcanic eruptions as analogues, doing climate modeling—is something we should do because we have to know what the possible impacts might be. If we are going to make policy decisions about this in the future, they should be informed, not emergency panic decisions.

Outdoor geoengineering research, such as actually spraying stuff into the atmosphere to brighten clouds or to create a cloud in the stratosphere, needs to be regulated. If the scientists can show that the amount of material they're going to spray is not going to be dangerous, is going to be very small, and is going to be a particular amount over a particular time, then that should be fine as long as their environmental impact statement is independently evaluated and monitored and they are sanctioned if they break the rules. Otherwise they could say, "Well, we didn't get a really strong signal, so let's just do it twice as long or put twice as much in or over twice the area." And there is no organization currently that can regulate outdoor geoengineering research. This infrastructure doesn't exist today. If you want to go out in the atmosphere over national territories there are environmental rules, but if you get over the ocean there are no rules.

BAS: Let's move on to talking about nuclear winter. How small a nuclear weapons exchange would be necessary to cause a climatic effect?

Robock: Well first of all I don't like the jargon of "exchange." It really sanitizes it. It sounds like you're going to take a sweater you got for Christmas back to the store. Rather you could ask, "How much burning of people and villages and cities do we need?"

The United States and Russia have enough nuclear weapons to produce nuclear winter. That is, the effects of smoke from burning cities and industrial areas could cause the temperature to go below freezing in the middle of the continents.

We did a scenario in which we looked at 50 Hiroshima-size atomic bombs being dropped on India and 50 being dropped on Pakistan on the targets that would produce the largest amounts of smoke. That's much less than one percent of the current global nuclear arsenal. We found that these 100 bombs would produce enough smoke to block out the sun and cause temperatures to fall lower than any temperature in recorded human history, colder than the Little Ice Age of several centuries ago which produced famines and revolutions.

BAS: What else could result?

Robock: China and the United States are the two biggest grain-growing regions in the world. Weather disruptions caused by that small nuclear war could cause production to go down by 10 to 40 percent for five years and 20 percent for ten years. This would be a huge hit to the world food supply.

BAS: You recently wrote that nuclear weapons are a more serious threat than global warming. Why is that so?

Robock: Because nuclear weapons produce climate change too, and the climate change caused by nuclear weapons could be much more devastating. It could have a much larger immediate impact on our food supply, producing social disruptions as well as famine.

Nuclear weapons are also an easier problem to solve than global warming: just don't use them. To solve global warming, you have to stop burning fossil fuels, and to do that you have to change the energy infrastructure of the planet and fight against very, very rich, well-funded multinational corporations that want to do business as usual.

BAS: You met with former Cuban President Fidel Castro in 2010 and 2011. How did that come about?

Robock: I had a student from Cuba, Juan Carlos Antuña, who got his PhD at Rutgers and then returned to Cuba, where he's a research meteorologist. He sent me an e-mail saying that the Cubans wanted me to come and talk about climate change. The next day, he sent me to a website where Castro was talking to the head of the Cuban weather service about nuclear winter.

As you know, Fidel fell down and broke his shoulder and his leg, and then he had these intestinal problems, and he was so sick he gave up power to his brother. But then he got better and he had free time on his hands that he never thought he would have. So somehow he discovered my work. He asked his son, Fidel Castro Diaz-Balart, to contact the head of the weather service, who contacted Juan Carlos, who contacted me and asked me to come.

BAS: What was it like to meet Castro?

Robock: Very surreal. I couldn't believe it was happening. But he's a really charismatic guy. The second time I met him, I sat across the table from him for more than three hours, and he went through his entire life history from his earliest childhood memories.

He talked about the Bay of Pigs invasion. He talked about Nixon and Kennedy and what movies you should see and said to read Anatoly Dobrynin's autobiography because that's the best record of what happened during the Cuban Missile Crisis.

Ten days after my first meeting with him, he said in his blog, "We've got to get rid of all nuclear weapons." And I was thinking, well, too bad he doesn't have nuclear weapons to get rid of. On the other hand, it's probably pretty good that he doesn't have them. I just have to convince people who have them.

BAS: What do you think small countries, like Cuba, can do about climate change and nuclear weapons, given that the superpowers control so much of what happens?

Robock: In the 1980s, the non-superpowers of the world realized, based on nuclear winter theory, that they could experience huge suffering even if no bombs were dropped on their countries. There was a lot of pressure from these countries on the United States and Soviet Union to stop the arms race. Because, for example, more people could die in China than in the United States and Russia combined, even if no bombs were dropped there. That pressure from all the rest of the world helped to end the arms race. And so I think that these conferences on the humanitarian impacts of nuclear weapons can have an effect.

But unfortunately Putin is sort of ramping up the Russian nuclear establishment, building new submarines and ordering threatening flights. And in order to sign New START, Obama had to agree to this $300 billion modernization of US nuclear weapons. And so those things have to be addressed.

BAS: You wrote a paper about weather imagery in Bob Dylan lyrics.

Robock: My best paper.

BAS: What role do you think artists can or should have in grappling with existential threats like nuclear weapons and climate change?

Robock: After my lecture in Cuba, they told me it would be broadcast on national television the next day at prime time. So we walked into a hotel bar with a television. And I looked and there was a Julia Roberts movie on. It was a DVD because they only have two channels there. And I said to the bartender, "Could you change the channel and see if I'm on?" He changed it and sure enough there I was. But what it taught me is that if you want to change the way people think you need a movie with Julia Roberts, not a professor giving a lecture.

I've been working with a colleague to write a screenplay for a feature film where this Russian climate scientist falls in love with an American one, and they discover what the climate effects of nuclear war would be. Meanwhile, on the India-Pakistan border there's an escalating conflict. I think you could write a screenplay with a little bit of sex. I'm not sure how to do the violence—whether to show the effects of what would happen in a dream, or let it really happen but not have a happy ending. I don't know. But I think if we had some entertainment like that, that's the way to educate people, not articles in the *Bulletin of the Atomic Scientists* or even TEDx talks.

Anybody who would be interested: If you know of any contacts who could write a movie about this, that would be great.

BAS: Do you envision any particular movie star in the role?

Robock: I'm old, so Julia Roberts would be fine for me, or Meryl Streep. But maybe some younger star so that it could appeal to young people too. Lizzy Caplan—she was in *Masters of Sex* and *The Interview*. She could be one of the scientists.

BAS: Is there anything you would like to add?

Robock: These are problems caused by humans. If we can cause them, we can fix them. We have free will. People say it can't be done, but of course it can be done because we created the problems in the first place. We just need somebody with the vision and the courage to solve them.

We worry about tipping points in the climate system but there are also tipping points in human behavior. If you look back at the United States 10 years ago, could you have imagined gay marriage or legalized pot or a black president?

These things have changed pretty rapidly, so I think it's possible we can get to the point of solving climate change and nuclear weapons too. I'm sort of optimistic, and that's why I keep working on them.

How South Korea Could Acquire and Deploy Nuclear Weapons

Source: http://npolicy.org/books/East_Asia/Ch4_Ferguson.pdf

CHAPTER 4

HOW SOUTH KOREA COULD ACQUIRE AND DEPLOY NUCLEAR WEAPONS

Charles D. Ferguson

INTRODUCTION: WHY STUDYING OPTIONS FOR NUCLEAR WEAPONS IS NECESSARY TO PREVENT FUTHER PROLIFERATION

Political leaders and defense planners in the Republic of Korea (ROK), or South Korea, are cognizant that worsening security in Northeast Asia could lead to additional states, including the ROK, to consider and even develop nuclear weapons. In particular, Korean President Park Geun-hye warned in May 2014 that another nuclear bomb test by North Korea (Democratic People's Republic of Korea or DPRK) would be "crossing a Rubicon" and would make it "difficult for us to prevent a nuclear domino from

With security concerns in Northeast Asia regarding North Korea's build up of its nuclear weapons arsenal, there is a possibility that states in the region, including South Korea and Japan, would consider and start to develop nuclear weapons. In a new paper published by the Nonproliferation Policy Education Center, FAS President Dr. Charles Ferguson examines the rationale for South Korea to acquire these weapons, and presents three acquisition scenarios. Ferguson also discusses the materials that ROK would need to acquire to make nuclear weapons, the design of the weapons and deployment of the bombs.

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

These robots are stranded inside a nuclear disaster

Source: http://i-hls.com/2015/05/these-robots-are-stranded-inside-a-nuclear-disaster/

A Tokyo utility company recently sent two specially-designed robots on an ill-fated mission into the Fukushima nuclear disaster site to assess the damage. Four years after an earthquake and tsunami destroyed Japan's Fukushima nuclear plant, Tokyo Electric Power Co. is still at work trying to clean up the scene.

TEPCO sent two specially-designed shape-shifting robots into the Fukushima No. 1 nuclear reactor to assess the damage. The first of the unnamed snake-like 60 cm (24 in) robots, which use wheels to roll along in a "C" shape and convert to an "I" shape to shimmy through pipes, got st uck after moving about 10 meters into the reactor's ruins on April 10, and was abandoned.

According to a report in *Defense One*, the second robot, which took a different route recently, completed its mission, but was also abandoned after it suffered damage to its camera from the high radiation levels.

◀ Packbot robot Rosemary robot ▶

Even if the robots hadn't been damaged, a Pixar-style "WALL-E" ending was never in the cards. As IEEE Spectrum notes, the robots became so radioactive that they would have been permanently stored in a shielded box if they had returned from their missions.

Before their demise, the robots – designed by the International Research Institute for Nuclear Decommissioning and Hitachi-GE Nuclear Energy – **measured radiation levels of 5.9 sieverts an hour.** By comparison, brief exposure to levels of 10 sieverts per hour would cause death within a few weeks for humans.

The anonymous snakebots may be done for, but there is still a vast robot menagerie working on the Fukushima cleanup. Other models, so-named primarily for their small sizes, include "Quince", "Packbot", "Raccoon", and "Rosemary".

New blood test quickly determines severity of radiation injur

Source: http://www.homelandsecuritynewswire.com/dr20150514-new-blood-test-quickly-determines-severity-of-radiation-injur

May 15 – **A novel blood test could greatly improve triage of victims of radiation accidents by rapidly predicting who will survive, who will die, and who should receive immediate medical countermeasures,** according to scientists at Dana-Farber Cancer Institute.

In pre-clinical trials, the test was able to reveal **within twenty-four hours whether survivable doses of radiation or doses that caused severe injury to the bone marrow and other organs would eventually prove fatal.** Use of such a test, the researchers said, could "facilitate timely medical intervention and improve overall survival of exposed individuals."

A Dana-Farber release reports that reporting in *Science Translational Medicine*, the scientists said that, unlike current methods, their blood biomarker test quickly determines the functional impact of radiation rather than simply the dose to which the individual was exposed. Often, the effects of severe radiation exposure develop slowly over weeks or months. Current methods — such as observing when radiation sickness appears – are inexact and don't measure the extent of long-term injury to the bone marrow and other organs.

"After a radiation release, there is currently no way to tell who was exposed and who wasn't, and if someone was exposed, is it lethal or not?" said Dipanjan Chowdhury, Ph.D., a principal investigator in Dana-Farber's Department of Radiation Oncology, the report's senior author. Drugs that can limit bone marrow damage are available but, to be effective, must be given before the appearance of radiation symptoms.

The need for faster, more definitive predictive tests was highlighted by radiation accidents such as the 2011 reactor meltdown at the Fukushima Daiichi plant in Japan, radiation releases from Chernobyl and Three Mile Island, as well as the potential for terrorist radiologic weapons. Chowdhury and his colleagues undertook the new study with federal funds designated for radiation exposure biomarkers research in the wake of the Fukushima accident.

In a search for such biomarkers, the investigators focused on microRNAs, or miRNAs. These are tiny RNA molecules, first identified about twenty years ago, that help regulate gene activity. They are made in cells, but some miRNAs are found in the bloodstream, and the scientists asked whether varying doses of radiation might cause corresponding changes in miRNA in the blood.

Experiments showed that 68 of 170 miRNAs detected in blood serum changed with radiation exposure, and these were narrowed down to a small number that acted as a "signature" of radiation dose. Mice exposed to two radiation doses, one lethal and one survivable, showed no outward differences for three to four weeks. **Using the miRNA signature, however, the scientists were able to predict within twenty-four hours which animals would survive.**

An indication that the test would work similarly in people came from experiments using mice who received transplants of human bone marrow. The blood test gave the same indication of damage to the human cells as it had in the previous experiments with non-humanized mice. In addition, when the researchers gave the mice a radiation protection drug that "rescued" many of the human cells, the miRNA test results confirmed this protective effect.

The scientists noted that the miRNA changes that can be seen at twenty-four hours after the exposure disappear in a matter of days, so they plan to look for

other miRNA signatures that have a longer duration.

— Read more in Dipanjan Chowdhury, "Serum microRNAs are early indicators of survival after radiation-induced hematopoietic injury," Science Translational Medicine (forthcoming)

Dimona: Israel's 'Little Hiroshima'

By Richard Silverstein

Source: http://www.middleeasteye.net/columns/dimona-israel-s-little-hiroshima-1962915520

May 19 – Despite the utter lack of utility of Israel's WMDs, the state's nuclear workers have paid a huge and terrible price

In the early 1950s, after Israel had fought a desperate war of independence in which thousands of Israelis died to ensure the founding of the state, David Ben Gurion, its first prime minister, decided the nation required an existential trump card to guarantee its survival. In 1955, he tasked his chief aide, Shimon Peres, with creating a nuclear programme that would lead to building a nuclear weapon.

The most critical part of this project was creating a nuclear reactor that would manufacture the fuel to make these weapons. In 1959, Israel began construction on its reactor in Dimona. Eventually, there were thousands of workers both building the plant and, once it was constructed, working within it to build the arsenal of 200 nuclear weapons Israel is reputed to possess. An excellent short overall history of the project can be found online.

In the early stages of research, before Dimona existed, there were accidents that exposed scientists to lethal levels of radiation. Some of them died and their names are known (though not well). Less known is that Dimona had a series of accidents - the most serious in 1966 - that exposed hundreds of its workers to similarly lethal doses.

Avner Cohen, the world's leading scholar of the Israeli nuclear programme, told me that **in the first 20-25 years the processes used to protect workers were primitive and sloppy.** Mistakes were common, often not intentionally, but because relatively little was known about the proper handling of radioactive materials. In some cases, documentation was fabricated.

This is the subject of Orna Ben Dor's riveting two-part documentary, *The Dark Secret of the Dimona Reactor*, produced for Israeli TV. Workers there call the nuclear plant "Little Hiroshima," alluding not only to the destructive power of what's produced there, but the tragic impact that the reactor has on those who work within it.

The documentary, while it exposes many secrets and crimes of the state against its workers, is also unintentionally maddening because it deals with a subject that the nation deems justifiably opaque. For that reason, no one in the Israeli Atomic Energy Commission, which runs Dimona, will speak on the record to the cameras. No journalist is allowed within the facility. Few if any records are made public regarding the functioning of the reactor.

According to Ben Dor, **the medical oversight of workers was a sham. They were given tests that were never processed and told they had a clean bill of health, only to find out months or years later they were dying of cancer.** The few records that are accessible happen only because of lawsuits that pry them loose from the fingers of the state.

The real story of the film is the extraordinary lengths to which the state will go to shield itself and its nuclear project from public awareness. Following on from this is the nation's willingness to treat those scientists, engineers and researchers who devoted their lives to this sacred project as refuse to be discarded once they get sick and die, no longer providing any useful service. There is a schizophrenic nature both to the documentary and the victims portrayed. On the one hand, they are patriots who understand the danger posed and accept it for the sake of protecting the state from its enemies. But on the other, they are human beings who demand that the country treat those who paid the ultimate sacrifice with dignity.

Treated as garbage

The "lowest of the low" (on the hierarchical totem-pole) were the nuclear technicians, the clean-up workers sent in to mop up after equipment malfunctions. Often, they were "children" of the reactor: raised in the town, attending the technical high school at the plant that taught them how to maintain it and its equipment. They faced the most danger. Yet no one warned them. They did their jobs anonymously. But when they got sick, the state tossed them overboard. One worker who was Mizrahi Jew was told that his cancer wasn't the result of his work at Dimona, but rather his Moroccan origin. His Sephardi genes somehow caused his illness. If it was only the racism of this claim that was involved it would be bad enough. But to use racism to cover up state crimes against its citizens is unforgivable.

The tragedy is that the victims themselves, through their own innate sense of patriotism, refuse to understand the contradiction inherent in what they demand of the state. Israel itself is a kingdom of secrets. Dimona is a secret within a secret; the holy of holies of Israel's nuclear religion. You cannot unravel the mysteries and expose the lies and crimes unless you tear the veil away. To do this, you must force Israel to end the opacity, end the secrecy. But no one in a position of power is willing to do this.

These are human beings feeling their way in a darkened hallway toward the light. They can't see what's around them, but can only touch the walls and try to make out where they are and what's around them. They are frightened. No one helps them understand where they are. They must make this journey alone.

In the second film, Ben Dor and two local residents visit a remote electrical station that supplies power to the plant. They note a stream flowing nearby that appears discoloured and polluted. Any journalist researching such a subject knows she must test the water to determine their level of purity. But Ben Dor tells us she can't. Anyone who brings a geiger counter to any Dimona facility or who tests the air, water or soil around it is committing a crime punishable by up to 15 years in prison.

Because the government forecloses access to sources, Ben Dor must allow the victims of Dimona to tell their story. They do so powerfully and tragically. Widows and orphaned children speak of their loved ones taken from them too early by a state that behaved cruelly and heartlessly. Courageous lawyers describe their years-long devotion to the search for justice. Medical doctors and researchers help sort through the miasma of lies and half-truths offered by the state, some at great risk to their careers by a vengeful IAEC.

The biggest problem with the film is the one that the nation itself faces. All the ills it portrays emanate from one powerful, poisonous fact: the nuclear project itself. In other words, when you decide to manufacture a nuclear bomb, you accept a cascade of choices that accompany that one fundamental decision. In legal terms, Israel's weapons of mass destruction (WMDs) are the poisoned tree and all the deaths, radiation poisoning and environmental damage are the fruit of this poisoned tree.

The documentary doesn't delve into deeper questions. It remains on the surface, dealing with important issues like environmental safety and worker mortality. These are the human-interest parts of the story, the ones an audience can immediately grasp, without having to ponder the more abstract and complicated issues.

Israel's 'KGB state'

Avner Cohen also faults the documentary producer for not confronting Israeli nuclear bureaucrats more aggressively and demanding that they reply to the accusations. He argues in the review he wrote for Haaretz's Hebrew edition that Israel must force those who devise Israel's nuclear policy to confront uncomfortable questions. Only in this way can change happen.

The secrecy of the nuclear programme, one interviewee calls it a "KGB state," goes hand in hand with the Israel's overall opacity around all manner of security issues. It's not surprising that Israel has put its fate in the hands of a few nuclear bureaucrats like those who run Dimona, because it runs its overall military apparatus in the same way. No civilian oversight to speak of. The generals get what they want. All in the name of protecting the state. It's a devil's bargain.

Ben Gurion could have chosen a different path. He could've followed the path Shimon Peres advocated to deter the 1973 war: he urged a public nuclear test to warn the Arab states what they confronted if they attacked. In the longer term, such transparency might've gone a long way to ameliorate some of the worst offenses of the nuclear security state. But Ben Gurion believed the quieter Israel was about it, the less opposition he might face from the world, especially the US.

He made a choice to create a nuclear arsenal in order to offer the state a mechanism to guarantee survival in the face of imminent defeat. But now Israel has ensured its existence. There is no existential threat (no matter what Bibi says regarding Iran). Nuclear weapons don't guarantee security. In fact, many serious analysts argue just the opposite.

Israel may eventually realise nuclear weapons are an albatross around its neck. They were never needed in the course of all Israel's previous wars and likely will never be needed (especially if it would agree to a regional nuclear-free zone - a prospect that is an anathema to it, so far). Yet despite the utter lack of utility of Israel's WMDs, its nuclear personnel have paid a huge and terrible price. It is shameful that the state that asked them to make the ultimate sacrifice defiles their memories with lies and stonewalling. It prefers this to paying them the few millions it would take to do justice to their pain and suffering.

***Richard Silverstein** writes the Tikun Olam blog, devoted to exposing the excesses of the Israeli national security state. His work has appeared in Haaretz, the Forward, the Seattle Times and the Los Angeles Times. He contributed to the essay collection devoted to the 2006 Lebanon war, A Time to Speak Out (Verso) and has another essay in the upcoming collection, Israel and Palestine: Alternate Perspectives on Statehood (Rowman & Littlefield).*

INL training military for response to radiological hazards

Source: http://www.homelandsecuritynewswire.com/dr20150519-inl-training-military-for-response-to-radiological-hazards

The van stops suddenly. The passengers move quickly to adjust personal protective equipment and move toward a facility several yards away. They immediately attend to the injured, survey the perimeter and question those on the scene. Days prior, this team of emergency responders was a group of individuals with different backgrounds and limited knowledge of radiological response.

Military branches from across the U.S. Department of Defense (DOD) registered top candidates for this intensive Radiological Hazards and Operators Training and Field Exercise course (RHOT) conducted by the U.S. Army Medical Center and School. These students were brought to the Department of Energy's Idaho National Laboratory (INL) site where they begin training to use radiological monitoring equipment, perform radiological calculations, and implement protective measures.

"Over the past decade, we have continued to refine the training to better prepare these radiological emergency responders for the situations they can anticipate in the real world," said Jennifer Turnage, INL program lead for Emergency Response and Readiness. "Our goal is to provide them with confidence in their equipment and the required skills to manage difficult situations without hesitation."

An INL release reports that two weeks of intense training have transformed these responders into a cohesive unit able to work together to take decisive actions to secure and survey an area for radiological hazards. Several days of instruction took place before the responders were put through a series of intense training environments designed to push their newly acquired

skills to the limit and force the newly formed team to rely on each other. The service members' specialized skills and knowledge are culled through several days of course work and practical exercises.

"We have some of the best and brightest who attend this course at Idaho National Laboratory, and they are challenged by the course work and training," said Captain Aaron Thompson, DOD lead coordinator for the course. "This training pushes them to excel and make the most of this valuable training experience that you just don't get anywhere else."

The students are met by a staff with decades of experience working with radiological materials and instrumentation. As one of the U.S. leading research institution for nuclear energy, INL employs experts with extensive knowledge in safeguards, forensics, measurement, and interrogation.

The INL release notes that INL is one of only a few locations able to provide a realistic training environment that immerses students in scenarios with authentic measurements, equipment and radiological source materials. Several locations across the laboratory's 890-square mile Site are employed for the training, presenting the students with a range of challenges that includes using their equipment in an isolated and rugged landscape and sweeping buildings with multiple levels and a large perimeter.

"The training objectives are about ensuring that at home and abroad we have radiological responders prepared to engage an environment without hesitation," said Major Kim Alston, RHOT lane officer in charge and instructor. "These service members will leave this training confident in their skills and ready to take on any situation they incur."

Since the inception of this joint-training program, hundreds of U.S. service members have been trained in radiation survey methods and techniques and proper use of radiation detection equipment. INL says that through the use of real-world situations, instructors are equipping the participants with the skills required to characterize and mitigate radiological and nuclear hazards, assess the risk, and provide recommendations to decision-makers on how to protect people and the environment from the potential harmful effects of radiation.

Inventing a stronger radiological waste bag for extra protection

Source: http://www.homelandsecuritynewswire.com/dr20150520-inventing-a-stronger-radiological-waste-bag-for-extra-protection

May 20 – At the Savannah River National Laboratory, the primary goal is innovation for safe and cost effective legacy waste cleanup. New methods are constantly being explored in order to protect workers and protect the environment. When Senior Scientist Dr. Aaron Washington realized that a radiological waste bag was not lasting as long as he would like, he set about inventing a new one. As a result, Washington and his team of researchers created a "double-ply" waste containment bag capable of better containing nuclear waste.


Prototype of Improved radiological containment bag

A Savannah River Lab release reports that much like a household garbage bag is used to protect waste from leaking into a garbage can, special radiological waste bags are used to keep radiation from leaking into a storage container. After time, materials used to create these bags fail due to damage from intense or long-term exposure to radiation. This can result in contamination and a need to repack age the contents. **This new invention uses nanotechnology to infuse radiation-resistant particles onto a sacrificial polymer layer.** By altering the material on a molecular level, it is now able to virtually eliminate

damage from high-energy alpha particles. Savannah River National Laboratory is in the process of patenting this technology.

"It can be thought of as adding an additional layer of containment. This inner polymer layer is highly resistant to radiation damage compared to the polyethylene alone and will extend the life of the bag by an order of magnitude without much additional cost," explained Washington. The improved containment bag will be vital in the cleanup and containment of high-energy waste such as plutonium.

This technology will save money, but more importantly, it will make the process safer. Alpha radiation generating waste with long-term storage often needs to be repackaged before it can be delivered for final disposal. "If we eliminate or significantly reduce this need for repackaging, we will save time, reduce the risk of personnel exposure, and reduce the environmental impact of generating more waste with failed contaminated bags. Additionally, by using inexpensive polymers and additives, the cost increase associated with making the improved bag is minimal," Washington said.

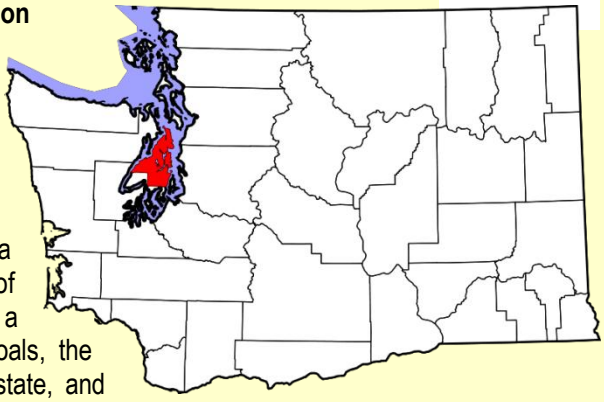
The special coating includes materials that may also be used as a sensor because the materials change color if the inner layer of the bag is breached. The research team is continuing to evaluate this coating for application to other plastics and surfaces.

Exercise simulates home-grown terrorists, nuclear incident

Source: http://www.homelandsecuritynewswire.com/dr20150522-exercise-simulates-homegrown-terrorists-nuclear-incident

May 22 – In a geopolitical environment with proliferating threats, a Defense Department whole-of-government exercise held 5-8 May provided a realistic way for federal, state, and local experts to interact in simulated situations involving mock home-grown terrorists and a nuclear incident.

This year's Nuclear Weapon Accident Incident Exercise, or NUWAIX 2015, took place on Naval Base Kitsap-Bangor located on the Kitsap Peninsula in the state of Washington.



As the home base for the Navy's fleet on West Puget Sound, NBK-B supports surface ships and fleet ballistic missile and other nuclear submarines whose home ports are Bremerton and Bangor.

DoD says that this set the stage for the actions required within a whole-of-government framework to mitigate the consequences of an incident involving a U.S. nuclear weapon in DoD custody at a military base in the continental United States. Among other goals, the exercise aimed to enhance the cooperative efforts of federal, state, and local response agencies.

Exercise participants

Federal participants in the exercise included the assistant secretary of defense for nuclear matters, U.S. Northern Command, the FBI, the Department of Energy, the Department of Homeland Security, the Federal Emergency Management Agency U.S. Coast Guard, the Department of Agriculture, the Environmental Protection Agency, and the Food and Drug Administration.

Other participants included the U.S. Navy Region Northwest, Strategic Weapons Facility-Pacific, Marine Corps Security Forces Battalion-Bangor, officials from the State of Washington, and Kitsap County, and others.

The Defense Threat Reduction Agency, or DTRA, was the DoD exercise lead.

"I'm very proud of the DTRA team that planned and executed NUWAIX 15, integrating and managing over 1,500 participants who made up a whole-of-government response," DTRA director Ken Myers said after the exercise. "DTRA's motto is 'Making the World Safer,' and I guarantee that our

world is a bit safer today because of the superb exercise this team developed and executed in Washington."

Preparation

The NUWAIX fifteen field-training exercise took three days to complete and a year to plan, DTRA lead and exercise project officer Army Maj. Matt Kershner told *DoD News* during a recent interview.

Planning included a concept development meeting to determine the elements that each participant wants the exercise to address.

"One agency might say that they need contamination," Kershner said. "Another agency might say, that they want to work on security, or another agency might say that they want to work on communications. We took all those and … and from there determined what the scenario needed to be in order to achieve as many of the training objectives as possible."

Next came the planning meetings — initial, mid and final.

The big concept

In the initial meeting, he said, we "hammered out all the differences with regards to the equities everybody wanted," the major said.

"At that point you agree to the big concepts. For example, we all agreed on the number of weapons systems, we all agreed there would be contamination — so you start trying to finalize as many of the details as possible," he added.

By the mid planning meeting the scenario was complete except for logistics, Kershner said — how many people and vehicles needed to be in each of three field-training sites for the exercise.

"The final planning meeting was fine tuning the last-minute details — the major logistics," he said, adding that one of the most complex jobs this year was scheduling and coordinating military flights for equipment and people from different organizations.

Remaining issues

In March, DTRA conducted a senior leader facilitated discussion to give senior leaders of those who would participate in the exercise an opportunity to work through and talk through remaining issues without going through the exercise, Kershner said.

The details of the exercise were closely held and never revealed to the players, he added.

During the week of the exercise, coordinators did last-minute fixes, trained the exercise observers/controllers, held safety and security briefings, and pre-staged three remote sites to be used in the exercise.

On 5 May, the exercise began. Here is the scenario:

A domestic terrorist organization with a transnational connection attacked a weapons convoy on Naval Base Kitsap-Bangor. An NBK-B weapons movement supervisor who works onsite helped the terrorists do this. The attack killed and injured many Marine Corps Security Force Battalion members. In the exercise, this was Site 1.

The attacking force then removed the weapon from the convoy and ran, with responders in pursuit. During pursuit and before leaving the base, the terrorists detonated an explosive device.

The site and weapon suffered damage, and the explosion caused radiological contamination. The Strategic Weapons Facility responded as the Navy Initial Response Force. This was Site 2.

Weapon incident response

Federal departments and agencies determined the weapon was in Kitsap County, and the Navy Region Northwest Response Task Force was activated on the base. Federal agencies deployed specialized personnel and technical teams to conduct weapon incident response operations in the Kitsap County area. This was Site 3, at a location near NBK-B.

After the weapon was returned to federal control and determined to be

safe, it was prepared for shipment and moved to a designated facility.
Describing the three remote sites, Kershner said Site 1, also known as the "Attack" site, was pre-staged with wrecked vehicles and dead and wounded bodies of Marines and terrorists. All bodies were adorned with realistic-looking mock wounds and injuries, a practice called moulage that is used for medical training.
"Site 2 was the explosion, where the U.S. stockpile weapon did not function as designed but was rather damaged, he said, adding that the explosion "gave us the contamination we needed for the event."

Tactical actions
Also at that site, Kershner said, technical assets from different government agencies were able to "get into the immediate actions of dealing with that type of weapon system."
Site 3, a geographically separated area about ten miles away, involved tactical actions and investigative issues that follow such an event, he said.
This included "tracking down leads and conducting interviews, that led to and culminated in tactical actions — tactical meaning civilian law enforcement assets forcefully capturing or killing terrorists," Kershner said.
The exercise was over when most or all training objectives were met and the exercise director determined that the exercise was complete.

After-action review
Immediately afterward, with input from the observers/controllers, the lead team offered what Kershner called a "hot wash," or a facilitated after-action review that provided initial feedback on the exercise performance.
In about ninety days, a comprehensive after-action review will be produced in classified and unclassified versions, he explained.
Exercise personnel included role players, observers/controllers and players.
Observers/controllers observed the players and noted positive and negative actions which would be the foundation of the after-action report, Kershner said. Players are always experts — the people who actually do the jobs that are focused on in the exercise — so during the exercise they were allowed to work freely.

Setting the stage
In the exercise, Kershner said, "the scenario really sets the stage for actions required within the whole-of government response framework." He added, "That goes to consequence management, the immediate actions that would require the recapture and recovery of U.S. assets, and the deployment of these types of teams and organizations and agencies throughout the United States."

U.S. may support nuke conference proposal challenging Israel's nuclear program

Source: http://www.homelandsecuritynewswire.com/dr20150522-u-s-may-support-nuke-conference-proposal-challenging-israel-s-nuclear-program

May 22 – **Israeli officials expressed their concerns that the Nuclear Nonproliferation Treaty Review Conference, which ends today in New York after month-long deliberations, will approve decisions which would pose a major challenge to Israel's unacknowledged nuclear weapons program. Arab states have already tried, in previous Review Conferences, to push for resolutions calling for making the Middle East a WMD-free zone, in effect, requiring Israel, the only nuclear-armed state in the region, to disarm.**

On the agenda of this year's Review Conference has been a proposal by Arab states to convene a regional conference on making the Middle East a nuclear weapons-free zone.
Bloomberg View reports that early on in the Review Conference, Egypt submitted a proposal for a regional conference on making the Middle East a nuclear-free zone – mandating that this conference be convene with or without Israel as a participant. The Egyptian proposal also called for making Israel's nuclear program the main focus of the regional conference.

Israel's position, supported by the United States and other countries, is that the nuclear arms issue should be dealt with as only one element of the regional security context, which also includes terrorism and the spread of missile technology. Another Israeli condition is that the regional conference's agenda must be agreed on by all the participants in the conference.

Late last week Spain took it upon itself to bridge the differences between Israel and Egypt, and after consulting with both sides, presented a compromise proposal which said that if no consensus on the regional conference's agenda is reached before December 2015, the UN secretary general will be empowered to decide whether to convene the conference, and on what terms.

Israel sees the Spanish proposal as too close to the Egyptian proposal, since it holds out the possibility that the regional conference would convened, and its agenda determined, even if there is no consensus among the participants.

A senior Israeli official, who spoke on the condition of anonymity because he was discussing sensitive diplomatic issues, told *Bloomberg View* that "The adoption of such a resolution [the Spanish proposal] would contradict a U.S. commitment made to Israel as publicly stated in 2010 by President Obama and then National Security Adviser James Jones."

Until the 2010 Review Conference – these conferences meet every five years – the United States supported Israel's position without much quibbling. In 2010, however, there appeared to be differences emerging between Israel's and the U.S. approach to regional nuclear disarmament.

Israeli officials said they worried that the gap between Israel's and the U.S. position was growing.

Thomas Countryman, the U.S. assistant secretary of state for international security and nonproliferation, has been in Israel since Tuesday, engaged in intensive talks with high-level officials from Israel's Foreign Ministry, the National Security Council, and the Israel Atomic Energy Commission.

Countryman is still in Israel, and no agreement satisfactory to Israel has yet been reached.

A senior Israeli government official Wednesday told *Bloomberg View* that "Israel is increasingly concerned that the United States is not going to prevent the NPT review conference currently meeting in New York from adopting a resolution on the Middle East that would jeopardize Israel's national security."

A senior Israeli official told *Haaretz* that Israel fears a "rerun" of what happened at the last NPT Review Conference, in 2010. Five years ago Egypt was successful in persuading the United States to include a section in the Conference's concluding statement which referred to Israel's nuclear capabilities and urged it to open all its nuclear facilities to UN inspections.

The 2010 statement also called for convening, within two years, a regional conference to discuss ways to make the Middle East an area free of weapons of mass destruction.

Israel's then-new prime minister, Benjamin Netanyahu (he came to power in 2009) did not bother to hide his anger with President Barack Obama, who came to power in January 2009 and who made his first major foreign policy speech in Prague, on 5 April 2009, outlining his vision of a world free of nuclear weapons.

Israeli sources were quoted in newspaper stories accusing the Obama administration of violating agreements the Nixon administration reached with Israel in the fall of 1969 which dealt with the nuclear issue. These sources said that the September 1969 understandings had guided U.S. policy on Israel's nuclear program for four decades, until Obama, in 2010, reneged on the 1969 U.S. commitments to Israel.

Netanyahu demanded clarifications and "compensation" from Washington for what he saw as a U.S. violation of its commitments, and he appeared to have received both during a meeting with Obama in the White House in July 2010, during which Obama pledged that there would be no change in American policy on Israel's nuclear program and that Washington would not seek to undermine Israel's policy of ambiguity over its nuclear arms.

After the meeting with Netanyahu, Obama said the U.S. supported the Middle East zone free of weapons of mass destruction, but he added: "Our view is that a comprehensive and durable peace in the region and full compliance by all regional states with their arms control and nonproliferation obligations are essential precursors for its establishment." Obama also said, "We strongly oppose efforts to single out Israel, and will oppose actions that jeopardize Israel's national security."

The senior Israeli official told *Haaretz* that Israel is worried that as was the case in 2010, Washington's eagerness to include in the Conference's concluding statement a reference to making the Middle East a WMD-free zone would push the United States to make concessions to Egypt which would undermine what Israel regard as essential security interests.

Bernadette Meehan, a spokesman for the U.S. National Security Council, said, though, that the United States was aware of Israel's concerns and that the United States would work to ensure that the final statement satisfies both U.S. and Israeli interests.

"Both the United States and Israel support the creation of a WMD-free zone in the Middle East," said Meehan. "We are working closely with our Israeli partners to advance our mutual interests, including preserving the NPT."

"This Administration and this President do not break commitments to our Israeli partners," she said.

EDITOR'S COMMENT: Nuclear Nonproliferation Treaty Review Conference, bla, bla, bla… The solution is simple: either ALL countries should have (if afforded) nukes or NONO should have them! Israel has long realized that in this life there are no friends; just circumstancial partners. Israel will not abandon its nuclear capabilities as long as it feels threaten. We can have either nuclear peace or just peace! It is up to us to decide what is best for the survival of both people and planet Earth.

Can I buy a nuclear weapon?

Source: http://i-hls.com/2015/05/saudi-arabia-wants-to-buy-pakistani-nuclear-weapons

Saudi Arabia intends to buy an "off the shelf" nuclear weapon from Pakistan, according to US officials quoted in The Sunday Times.

The report comes amid ongoing negotiations between Iran and other world powers over its nuclear programme, and a potential thawing of relations between the US and Iran.

Saudi Arabia is wary of a potential deal on Iran's nuclear programme and Prince Turki bin Faisal, the former Saudi intelligence chief, has warned that it could pave the way for nuclear proliferation in the region.

The Sunday Times report suggests that Saudi Arabia has already taken the decision to acquire a nuclear device from its ally Pakistan.
The report quotes an anonymous US defence official as saying: "There has been a longstanding agreement in place with the Pakistanis [over nuclear weapons] and the House of Saud has now made the strategic decision to move forward."
Saudi Arabia is believed to have helped fund Pakistan's nuclear programme, which began back in the 1970s. Pakistan tested its first nuclear device in 1998.
Pakistani officials deny allowing Saudi Arabia access to the country's nuclear technology.
Negotiators have yet to reach a deal on Iran's nuclear programme, but if they do it could leave Iran's 5,000 centrifuges and much of its research programme in place.
The Gulf States warn that any deal that leaves open the possibility Iran could eventually enrich uranium to weapons grade would promote a nuclear arms race in the region.
Barack Obama, the US president, has attempted to ally those fears, holding discussions with the US's Gulf allies at Camp David last week.

EMP – the threat is real, very real

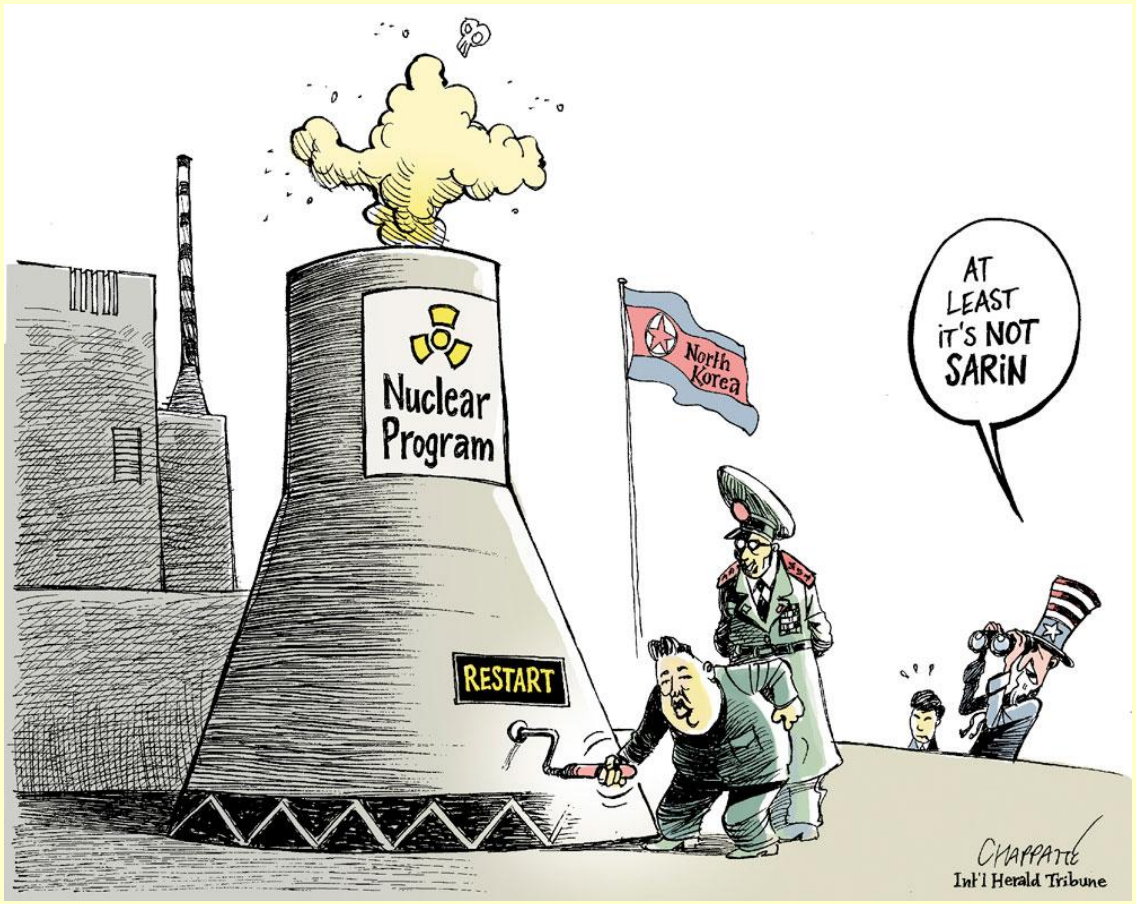
Source: http://i-hls.com/2015/05/emp-the-threat-is-real-very-real/

An EMP strike, most likely from the detonation of a nuclear weapon in space, would destroy unprotected military and civilian electronics nationwide, blacking out the electric grid and other critical infrastructure for months or years. The staggering human cost of such a catastrophic attack is not difficult to imagine.

Cheyenne Mountain According to the Wall Street Journal, the Pentagon was wise to move NORAD communications back into Cheyenne Mountain and to take measures elsewhere to survive an EMP attack. But how are the American people to survive?

In the event of a year long nationwide blackout, tens of millions of Americans would perish from starvation and societal chaos, according to members of the Congressional EMP Commission, which published its last unclassified report in 2008.
The U.S newspaper says that President Obama has not acted on the EMP Commission's draft executive order to protect national infrastructure that is essential to provide for the common defense. Hardening the national electric grid would cost a few billion dollars, a trivial amount compared with the loss of electricity and lives following an EMP attack. The U.S. also should deploy one of its existing transportable radars in the Philippines to help the ground-based interceptors at California's Vandenberg Air Force defend the country against an attack from the south.

Congress also has failed to act on the plans of its own EMP commission to protect the electric grid and other civilian infrastructure that depends on a viable electric grid—such as communications, transportation, banking—that are essential to the economy. In recent years, the GRID Act, the Shield Act, and the Critical Infrastructure Protection Act have gained bipartisan and even unanimous support in the House, yet they died in the Senate.



KeDetect XD4 & XD8

Source: http://www.ketech.com/index.php/products-solutions/detection/kedetect-xd4

The KeDetect XD4 is a compact and low cost portable kit for reliably detecting Ammonium Nitrate based home-made explosives. It was developed by KeTech in conjunction with the UK MoD to specifically provide a highly sensitive and accurate detection facility for the 'sugar' variant of explosive known as 'ANS'.

KeDetect XD8

The KeDetect XD8 was developed by KeTech in conjunction with the UK MoD and is designed to efficiently and safely detect the presence of explosives based on peroxides or chlorates, which are commonly used in IEDs

Smart IED-Jammer – A life saver

Source: http://i-hls.com/2013/05/smart-ied-jammer-provides-electronic-surveillance/#sthash.os2Z4EaZ.dpbs

Cassidian, the defence and security division of EADS, has developed a new-generation multifunctional jamming system that significantly enhances the protection of vehicles against radio-controlled improvised explosive devices (RCIEDs). Defense Update reports.

The new mobile jammer combines the smart jamming functionality with signals intelligence (also known as Electronic Support Measures – ESM), allowing detailed understanding of the threat, thus significantly improving mission planning and force protection.

According to the company, the multifunctional jammer analyses the signal spectrum around a vehicle and is thus in a position to jam the radio signals intended to trigger a roadside bomb in a targeted manner rather than by barraging noise over a wide spectrum, blocking friendly communications or operating over specific bands, leaving vulnerable gaps that could be exploited by insurgents.

Cassidian's multifunctional jammer features the new, ultra-fast Smart Responsive Jamming Technology to substantially enhance the level of protection. This system detects and classifies radio signals intended to ignite roadside bombs. It then transmits jamming signals in real-time, which are tailored exactly to the hostile frequency band. Thanks to the new digital receiver and signal processing technologies it is thus possible to achieve reaction times of well below a millisecond.

The new jammer also employs the SMARTscout extension, providing signal intelligence battlespace picture – a task that previously could only be accomplished by relatively complex systems which are difficult to deploy and consume a lot of energy. SMARTscout allows the user to deploy numerous sensors in theater, at relatively low cost, and to obtain an 'electronic order of battle' of radio communication threat situation in less time. This new capability assists the user in gaining force protection and the intelligence essential for planning of further operations.

"Lessons learnt in recent conflicts prove that the enemy often changes the type of radio transmission used for triggering signals in asymmetric scenarios," explains Elmar Compans, head of the Sensors & Electronic Warfare unit at Cassidian. "Continuous analysis of threats and the resulting adaptation of countermeasures are therefore indispensable. Using our SMARTscout system, both of these tasks can be done faster and with reduced effort."

4,300 people in more than fifteen countries killed in 504 suicide bombings in 2014

Source: http://www.homelandsecuritynewswire.com/dr20150501-4-300-people-in-more-than-fifteen-countries-killed-in-504-suicide-bombings-in-2014

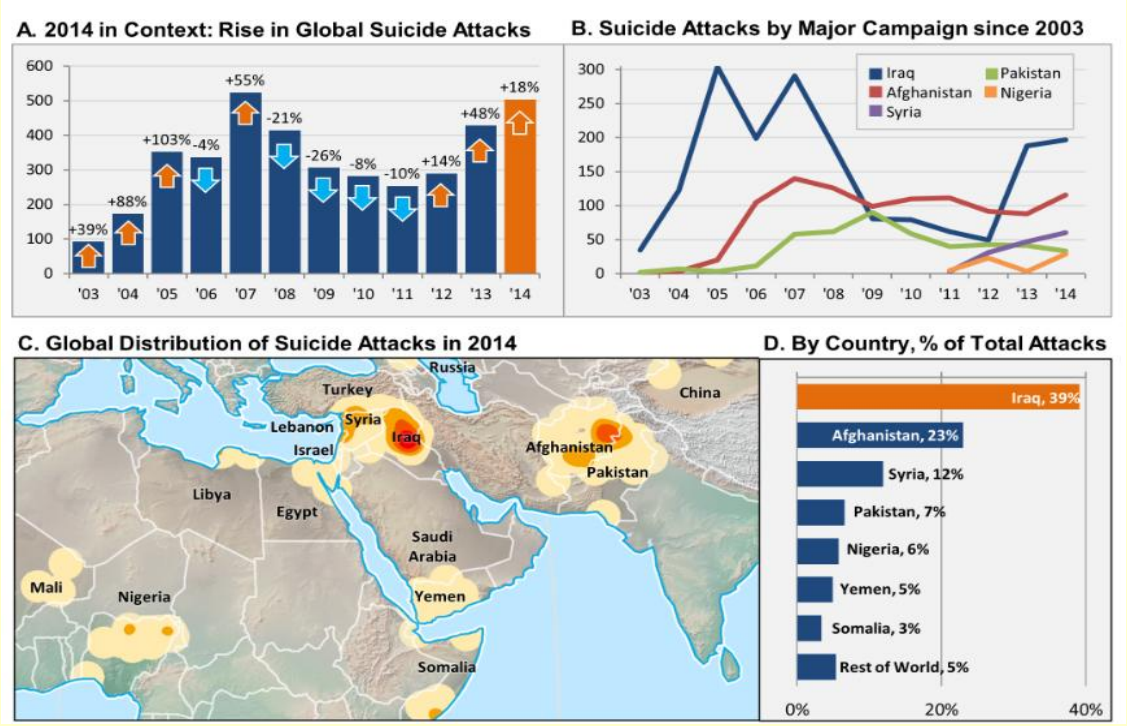
May 01 – **A new report on global trends in suicide terrorism shows that during 2014 more than 4,300 people in more than fifteen countries were killed in suicide bombings. Out of the fifteen countries, Afghanistan and Iraq led the world last year in suicide attacks with an increase in Iraq. The report shows that Iraq accounts for 40 percent of all such events in the world.** "If you're just following the news on a daily basis, you might have the idea that the entire world has suddenly been engulfed in terrorism and that somehow that was worse in 2014," said Robert Pape, Professor of Political Science and the founding faculty director of the Chicago Project on Security & Terrorism (CPOST), which published the report. Pape said, however, that the data show that the increase was limited to Iraq.

A University of Chicago release reports that the CPOST 2014 Suicide Attack Index is the first one-year summary of suicide attacks that occurred across the world. Pape and his team of CPOST researchers compiled the index and accompanying report. They showed that the total number of confirmed attacks reached 504 in 2014.

CPOST research director Keven Ruby, Ph.D. '12, said one surprise the report made clear is that the number of suicide attacks in Afghanistan has remained relatively constant for several years. "That's particularly worrisome from a U.S. policy perspective," said Ruby, "because the United States wants to withdraw militarily from Afghanistan, but there are no signs that the campaign by the Afghan Taliban is letting up."

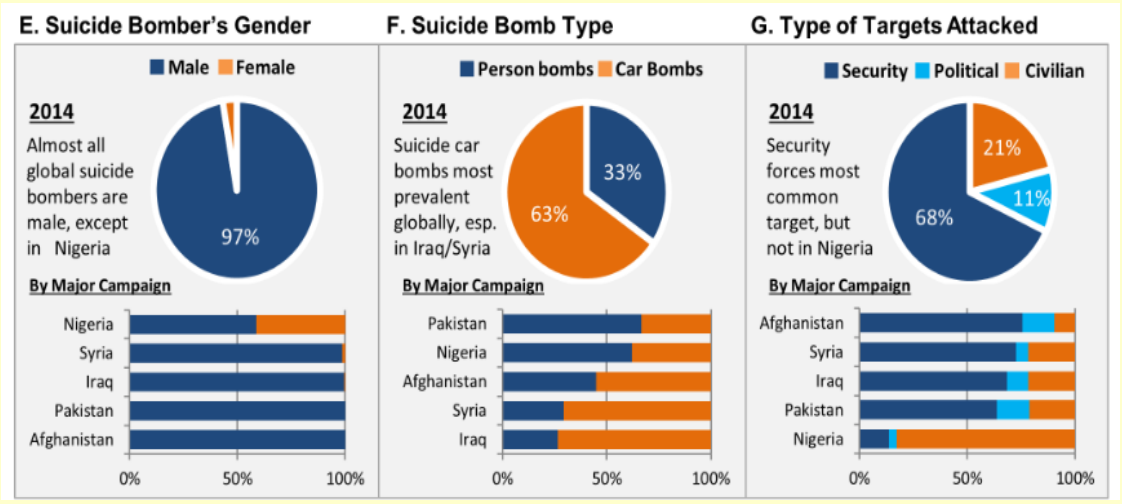
The CPOST index highlights key data on world hot spots for attacks and also shows that, with the exception of Nigeria, the majority of suicide bombers were males. The researchers also found that car bombs were the most prevalent weapons, and the targets were overwhelmingly security forces.

In 2004 Pape created CPOST, an international security affairs research institute at the University of Chicago. As its director, he heads a team of investigators, including several students, who track globally all suicide incidents. "We decided that we should do what nobody else is doing with these terrorism databases, and that is to put the information together on a single page to summarize what happened in the world of suicide attack last year," said Pape. "We're trying to set the standard for reporting this information."



Fourth-year and research associate McIntyre Skarzynski is among the team of students who carefully investigate each suicide attack by gathering as much data as possible from a variety of sources. "We will have at least two independent news sources, usually more, plus documents from the terrorist organizations and government reports," said Skarzynski.

"Each student has a different region of the world to track. We look at each attack to see whom the terrorists were attacking, how many people were killed, and where the attack was taking place. We're constantly checking each other's work to make sure the database is as accurate as possible," Skarzynski added.



"We're collecting information in the way a medical researcher might collect information on lung cancer," said Pape. "Let's call this the disease of suicide attack.

We're looking for specific risk factors for the deadliest threats we face from terrorism in the world."

Pape and his CPOST team hope the information from the suicide attack index and report will be helpful to policy makers, academic researchers and journalists to put the data into context.

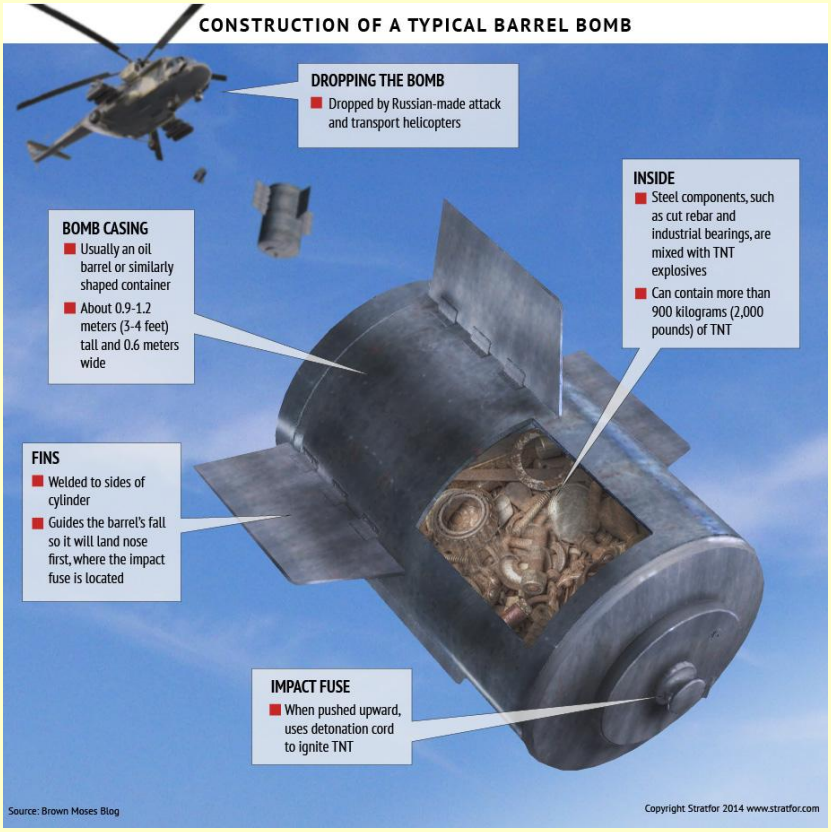
"We're doing this to save lives," said Pape. "We want to provide the best data in the world to develop better policies to save lives and to mitigate harm against bystander populations. If you have the wrong policy because you don't have good enough data, you can actually cause more harm than good."

— Read more in Suicide Attack Index: Global Trends in Suicide Terrorism in 2014 (CPOST, University of Chicago, April 2015)

Barrel Bombs Kill More Than 3,000 Civilians in Syria, Report Says

Source: http://www.terrorismwatch.org/2015/05/barrel-bombs-kill-more-than-3000.html

"I saw children without heads, body parts everywhere. It was how I imagine hell to be."



The Syrian army has dropped barrel bombs on schools, markets, hospitals and mosques throughout the northern city of Aleppo, killing more than 3,000 civilians since 2012, according to a new report.

The Amnesty International report finds that barrel bombs—an oil or fuel tank packed with shards of metal—have been dropped with growing frequency in recent months, forcing schools and hospitals to operate out of underground bunkers. Local activists recorded more than 85 barrel bomb attacks in the last month alone, according to the report.

"Widespread atrocities, in particular the vicious and unrelenting aerial bombardment of civilian neighborhoods by government forces, have made life for civilians in Aleppo increasingly unbearable, said Philip Luther, Director of Amnesty International's Middle East and North Africa program.

The report was based on eyewitness accounts from 78 former residents and 29 professionals, which were verified with video evidence of the devastation.

"I saw children without heads, body parts everywhere," said one local factory worker after an attack on al-Fardous neighborhood in 2014. "It was how I imagine hell to be."

Fluid Threats Indeed?

Source: http://i-hls.com/2015/05/fluid-threats-indeed

It's been eight years since police foiled a terrorist plot to detonate liquid explosives onboard airplanes headed from the United Kingdom to the United States, and since that time intelligence agencies have issued blanket airport security measures, including unprecedented restrictions on carrying liquids onto aircraft. But a lot has changed in those eight years, and technology and policy may have finally started to catch up with – and even stay ahead of – these threats.

For the first time since the foiled bombing, airport restrictions on liquids will be scaled back in Europe. The European Union (EU) has issued policy updates, gradually lifting regulations on carry-on liquids. By 2016, there will be no restrictions whatsoever. Instead, liquids will be tested at airport security checkpoints using cutting-edge explosives detection technology.

That's not to say airports are lightening up on security. Instead, security regulations are becoming more targeted to thwart emerging threats. Earlier this year, for example, **U.S.-bound passengers flying from Europe were required to power on all electronic devices to show that they weren't packed with explosives.**

Staying a step ahead of terrorism threats, especially those involving explosives, takes more than just detection technology. Experts emphasize the importance of a layered security approach that would theoretically stop a terrorist before a bomb is even in play.

Liquids, aerosols, and gels (LAGs) have been some of the most heavily-regulated items at airports worldwide. Next month, European airports will lift restrictions on the type and quantity of LAGs. In 2014, airports in Europe allowed larger quantities of baby foods and medications to pass through security checkpoints, and next month – pending the EU's continued support – clear liquids in clear bottles will be allowed on airplanes.

This change in policy is largely thanks to the development of explosives detection technology that will enable airports to quickly and accurately test liquids for explosives components, explains Pablo Prado, CEO of detection tool manufacturer One Resonance Sensors. **This type of explosives detection system screens bottles for dangerous**

chemicals within seconds, regardless of the opacity or composition of the bottle. Detectors like One Resonance's MobiLab BLS use MRI-based technology, which tests the liquid without opening the bottle.

According to *Security Management*, security shouldn't begin and end at the checkpoints, says Matthew Hager, senior intelligence manager at iJET. There have been instances of attacks occurring outside of the terminals, like the December 2013 shooting of a Philippine mayor and his family at a Manila airport. He's also seen an emergence of online instructions and YouTube videos focusing on building weapons or incendiary devices past security checkpoints in terminals using items found in duty-free shops.

Training the future canine force

Source: http://www.homelandsecuritynewswire.com/dr20150506-training-the-future-canine-force

Canines have proven to be expert bomb detectors for U.S. troops in Iraq and Afghanistan. With combat operations winding down, however, the Office of Naval Research's (ONR) Expeditionary Canine Sciences program says it is taking **a fresh look at how dogs are trained to identify different explosive devices — and their roles in future conflicts.**

"We don't know what challenges the battlefield of the future will present," said Chief of Naval

Research Rear Adm. Mat Winter. "Our canine warfighters must be as well trained as their human counterparts. It's critical that we learn as much as we can about how canines process

scents and how long they retain scent memory."

Researchers hope to streamline and enhance canines' training so they can work with any Navy or Marine Corps dog handler, not just one. Another goal is to get the dogs to the point where they can even work without a handler's leash.

In previous years, research and training focused primarily on developing physically strong dogs that could withstand the harsh climate, terrain and stress of combat. ONR's new research focuses on cracking the code of olfactory and cognitive optimization — essentially, how dogs recognize and remember odors, and for how long and to what degree.

For example, different combustible elements are used to make improvised explosive devices (IEDs). Researchers want to find out if bomb-detecting dogs can expand their recognition of odors within these diverse elements and in what ratios.

"Before, dogs were trained on one dominant odor to identify explosive devices," said Dr. Joong Kim, who oversees the canine program. "In this research, we want to expose them to a variety of elements and odors. Also, it's not known whether dogs forget odors over time, so our tests will see how long dogs can remember smells before requiring retraining."

ONR-sponsored tests are already underway in places like Maryland's Blossom Point Research Facility. There, researchers from the Naval Research Laboratory, as well as from the Explosive Ordnance Disposal Technology Division at Naval Surface Warfare Center Indian Head, work with U.S. Army dog handlers to test canines using **Mixed-Odor Delivery Devices** (MODDs) — small, cube-shaped boxes containing vials of substances used to make IEDs.

Each MODD holds two to four vials, presenting varying scent mixtures for the dogs to detect. The canines also sniff out explosives hidden in abandoned vehicles and underneath tin cans and wooden boxes.

In addition to challenging dogs' noses, ONR-sponsored research is studying their minds. **Canines' brains are evaluated using functional MRI machines (fMRIs) to determine how well they respond to various forms of motivation — snack treats, verbal praise, or physical affection such as petting.** While traditional MRI machines generate images to map out brain structure, fMRIs measure brain activity by detecting changes in blood flow.

Kim envisions ONR's Expeditionary Canine

Sciences program going beyond just military needs, encompassing law enforcement and homeland security missions. ONR is currently developing an interagency program with the Department of Homeland Security and the U.S. Army Research Office to coordinate scientific research that will benefit both

military and public safety functions.
"Dogs are and will continue to be a key part of our future expeditionary forces," said Kim. "They are mobile, smart and resilient, and can help warfighters through a host of battlefield situations."
ONR notes that under its Expeditionary Canine Sciences program, it supports researchers at academic institutions, government agencies, and companies studying canine cognition, training, stress and genetics. The program aligns with the recently released Naval Science and Technology Strategy, which emphasizes mobility and adaptability within irregular warfare as key components of warfighter performance.

The device that will protect your vehicle from "Sticky bombs"

Source: http://i-hls.com/2015/05/anti-devices-system-protects-your-vehicle/

So called 'Sticky bombs' are becoming a global threat and are commonly used by terror groups, local mafia and other para-military organizations. The security market is ready now more than ever for any viable solution.

An Israeli company has endeavored to feature what they refer to as 'The Advanced Car Protection'. Currently under development these days, it will detect any hidden device placed under the parked car and will issue an alert in real time. The system will also prevent easy access to the chassis area of the car by deploying a physical shield around the car. The core technology, already in development, is patent pending.

Placing a 'sticky bomb' under a car is typically done while the car is parked, either a civilian or even a military vehicle, while standing at a crowded place. Once placed, the bomb can be triggered manually or automatically, as well as via direct connection such as wire, infrared or Bluetooth – as well as via remote connection (cellular). There is no need to eliminate the car alarm or try to physically break into the car.
Therefore, the bomb can be in "silent" mode before it is triggered and will be hard to detect even when one looks under the car to check. The same is true for tracking devices that are even smaller in size and therefore harder to detect by a physical check of the chassis.
The system, developed by ABCD MAX, features a holistic approach that combines electronic sensors and physical protection. **The patented physical barrier prevents unauthorized access to the vehicle by sealing the gap between the vehicle and the ground while smart sensors cover the area underneath the vehicle, preventing penetration of any foreign objects. This approach allows 360-degree chassis protection of any car, both armored as well as not armored.**
ABCD MAX's application will provide alert to smartphone/ any computer about any attempt to lay an object under the vehicle. The end user can control the system by any smartphone or computer.

Chemring Technology Solutions Launches World's First Interchangeable Handheld IED Detector for both Wire and Metal

Source: http://www.hstoday.us/single-article/chemring-technology-solutions-launches-world-s-first-interchangeable-handheld-ied-detector-for-both-wire-and-metal/25b4abec1feae89d1a756b6c7b5a20c1.html

Chemring Technology Solutions launched GroundHunter MHDS, the world's first hand-held IED detector with interchangeable sensor heads for wire and metal detection.

GroundHunter MHDS (Multi-head Detection System) supports multiple sensor heads to enable search teams to respond quickly to changing scenarios, while the common user interface significantly reduces training burden. The lightweight system has a compact folding design, and allows multiple heads to be carried by a single operator for rapid reconfiguration.

Currently offering two sensor heads, the **CWD100** and **MD100,** GroundHunter MHDS has a future-proof design that will be compatible with future sensor heads. As technologies become available, GroundHunter MHDS will have the ability to address new threats.

The CWD100 command wire detector head identifies command wires that are over 20 metres in length, independent of their orientation. Incorporating its own transmitter and receiver, the CWD100 eliminates the requirement for supporting infrastructure. This reduces the total cost of ownership compared with traditional command wire detection products. Using pulsed induction techniques, the MD100 head detects both ferrous and non-ferrous metals.

Ian Redwood, Product Manager at Chemring Technology Solutions, said: "For the last forty years, we have continuously introduced market firsts and world-leading products to our military customers. Our pedigree of developing exceptional sensors and systems has enabled us to create GroundHunter MHDS, which delivers multiple functions to help military teams react faster and more flexibly to the threats they find themselves facing. GroundHunter MHDS provides a weight and power saving compared to carrying two detectors, as well as being easy to pack and carry."

Most Businesses Use Network Protection from the 90s

Source: http://www.infosecurity-magazine.com/news//most-businesses-use-network-1/?utm_campaign=NetworkProtectionfromthe90s&utm_source=E-Newsletter28%2F04&utm_medium=Email

More than 90% of companies are still using outdated technologies as their primary source of security for network access control—and 45% of them have not increased their security budgets to modernize, despite recent high-profile breaches.

That's the word from a new survey from Cryptzone and TechValidate, which uncovered that outdated approaches to security are rife. Most importantly, there is a decided lack of advanced solutions to limit the carte blanche access granted to employees and third parties under older network security models.

A vast majority (91%) of respondents said that VPNs are still the main form of security for controlling network access, despite the fact that VPN technology was created almost 20 years ago.

A slight majority (51%) noted that their access control technology was greater than three years old, and 11% said it was more than 10 years old.

Host IPS, next-gen firewalls, identity management solutions and vulnerability assessment are only being used by between 24-30% of the organizations for the purpose of access control. Exactly half said that their network access/firewall rules were static, and only 21% of companies rely on attribute-based controls to secure access. Most rely on authentication (93%) and session authorization (46%).

Overall, more than half of companies (52%) have not reviewed their access policies in over a year, and 42% of companies can't or don't automatically enforce security policies.

"It's remarkable that many organizations are still utilizing network security technologies developed in the nineties—a time when the Internet was still in its infancy," said Kurt Mueffelmann, president and CEO for Cryptzone, in a statement. "The cyber-attacks we have seen over the last few years, have demonstrated that it's far too easy for hackers to steal user credentials, and then use those credentials to traverse the enterprise network in search of the most valuable data. Organizations need to accept that outdated access control technologies are not working against today's sophisticated adversaries.

There's also a big gap between concerns and reality when it comes to threats. The survey revealed that malicious external user actions (hacking) were perceived as the greatest security risk to an organization (66%), followed closely by user mistakes/accidents (56%). But, upon reviewing the threats that had caused the most actual harm or damage to organizations in the last 12 months, 61% noted user mistakes/accidents, and only 46% noted malicious external user actions. So in other words, insider threats caused the most actual harm or damage to information security, not outside threats.

"The default position should be to make your infrastructure invisible, and then grant access on a case-by-case basis, only after user identity, posture and context have been validated," Meuffelmann said. "Organizations must stop giving out the keys to the kingdom when it comes to privileged user, third party and employee access."

Social media analysis suggests links between Baltimore and Ferguson violence

By Catherine Herridge

Source: http://www.foxnews.com/tech/2015/04/28/social-media-analysis-suggests-links-between-baltimore-and-ferguson-violence/

An analysis of social media traffic in downtown Baltimore Monday has unearthed striking connections to the protests in Ferguson, Mo. last year, according to a leading data mining firm that shared its findings exclusively with Fox News.

The firm, which asked to remain anonymous because of its government work, **found between 20 and 50 social media accounts in Baltimore that were also tied to the peak period of violence in Ferguson. While**

further analysis is being conducted on the data, it suggests the presence of "professional protesters" or anarchists

taking advantage of Freddie Gray's death to incite more violence.

Gray, 25, died April 18, a week after being injured while in police custody. A wave of violence erupted in Baltimore following his funeral Monday.

One account, which also tracked the recent union protests in New York City as well as other disturbances, tweeted photos of Gray's funeral and used language that seemed to anticipate violence in Baltimore.

The discovery that some social media accounts were tied to cities 825 miles apart was described to Fox News as "surprising." While it is possible to spoof accounts and make it appear as if someone is in one location when they are really in another, the data mining firm told Fox News that it can't fully explain the numbers.

The use of social media to fuel violence in Baltimore has already been highlighted by law enforcement. On Monday, police said an online call was issued for a "purge" at 3 p.m. ET, starting at Mondawmin Mall and ending in the downtown area. That type of threat is based on a movie called "The Purge," the plot of which involves rampant lawlessness.

The Washington Times also reported Monday that law enforcement intelligence officials issued a warning after someone sent a text urging people to "kill all white police officers" in reaction to Gray's death. The text has fueled fears that the violence in Baltimore could spread nationally, according to safety memos obtained by The Washington Times.

Baltimore's mayor, Stephanie Rawlings-Blake, announced a 10 p.m.-5a.m. curfew would be imposed beginning Tuesday.

***Catherine Herridge** is an award-winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London-based correspondent.*

Here's What a Cyber Warfare Arsenal Might Look Like

Source: http://www.scientificamerican.com/article/here-s-what-a-cyber-warfare-arsenal-might-look-like/

The Pentagon has made clear in recent weeks that cyber warfare is no longer just a futuristic threat—it is now a real one. U.S. government agency and industry computer systems are already embroiled in a number of nasty cyber warfare campaigns against attackers based in China, North Korea, Russia and elsewhere. As a counterpoint, hackers with ties to Russia have been accused of stealing a number of Pres. Barack Obama's e-mails, although the White House has not formally blamed placed any blame at the Kremlin's doorstep. The Obama administration did, however, call out North Korea for ordering last year's cyber attack on Sony Pictures Entertainment.

The battle has begun. "External actors probe and scan [U.S. Department of Defense (DoD)] networks for vulnerabilities millions of times each day, and over 100 foreign intelligence agencies continually attempt to infiltrate DoD networks," Eric Rosenbach, assistant secretary for homeland defense and global security, testified in April before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities. "Unfortunately, some incursions—by both state and nonstate entities—have succeeded."

After years of debate as to how the fog of war will extend to the

Internet, Obama last month signed an executive order declaring cyber attacks launched from abroad against U.S. targets a "national emergency" and levying sanctions against those responsible. Penalties include freezing the U.S. assets of cyber attackers and those aiding them as well as preventing U.S. residents from conducting financial transactions with those targeted by the executive order.

Deterrence of this type can only go so far, of course, which is why the DoD last month issued an updated version of its cyber strategy for engaging its adversaries online. The plan outlines Defense's efforts to shore up government networks, systems and information as well as those run by U.S. companies.

If cyber attacks continue to increase at the current rate, they could destabilize already tense world situations, says O. Sami Saydjari, a former Pentagon cyber expert who now runs a consultancy called the Cyber Defense Agency. "Nations must begin to create real consequences for malicious action in cyberspace because they are leading, in aggregate, to serious damage, and there is potential for much larger damage than we have seen so far," he adds.

A major part of the DoD's cyber strategy is to bolster the Pentagon's "cyber mission force," which the department began forming in 2013 to carry out its operations in cyberspace. Although the unit will not be fully operational before 2018 the unit is expected to have nearly 6,200 military, civilian and contractors—divided into 13 teams—working across various military departments and defense agencies to "hunt down online intruders," Defense Secretary Ashton Carter said last month during a lecture delivered at Stanford University.

The strategy does not go into detail about which digital weapons the cyber mission force will deploy to fight its campaigns. That information can instead be gleaned from the malicious software—"malware"—already rampant on the Internet as well as military technologies designed to disrupt digital communications. The Stuxnet worm that sabotaged Iran's Natanz uranium enrichment plant in November 2007 is an early example of cyber war weaponry. No one has officially claimed ownership of Stuxnet although much speculation points to the U.S. and Israel as its authors. A related piece of strategic malware known as Flame is subtler, stealthily gathering information and transmitting it via Bluetooth while avoiding detection.

The components of cyber warfare are the very same components as warfare using guns and explosives, only much faster, Saydjari says. An attacker would seek to damage a critical infrastructure such as power, telecommunications or banking by damaging the computer systems that control those infrastructures. "The instrument of creating that damage is generally some form of malicious software that is inserted into such systems by a variety of means including hacking into the system by taking advantage of some known but as yet unpatched or as yet undiscovered vulnerability," he adds.

China recently admitted that it has both military and civilian teams of programmers developing digital weapons, and documents disclosed by National Security Agency whistle-blower Edward Snowden indicate China has developed malware to attack U.S. Defense Department computers and even steal sensitive information about the F-35 Lightning II fighter plane that Lockheed Martin is developing for the U.S. Air Force. "All technically savvy countries are developing both offensive and defensive capabilities to prepare for the potential of cyber conflict both by itself and as one aspect of broader conflicts including kinetic warfare, which involves bombs and bullets," Saydjari says. "The goal of many such countries is to be able to exercise complete dominance and control over any part of cyberspace, anywhere and anytime it serves their national interests."

The Air Force Research Laboratory is soliciting projects that could furnish cyber deception capabilities for use by commanders to "provide false information, confuse, delay or otherwise impede cyber attackers to the benefit of friendly forces." Another aspect of cyber warfare could be the use of cyber electromagnetic activities to "seize, retain and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum," according to a U.S. Army report on the subject. Electromagnetic attacks have already struck in South Korea where more than 500 aircraft flying in and out of that country's Incheon and Gimpo airports reported GPS failures in 2010, *IEEE Spectrum* reported in 2014. The source of the electromagnetic fields was traced to the North Korean city of

Kaesong, about 50 kilometers north of Incheon. Cyber war itself may be difficult to define but cyber treaties pose an even bigger challenge. "In some sense it is a bit like asking bank robbers in the old wild West to negotiate a non–bank-robbing treaty," Saydjari says. "Many countries are benefiting from the lack of rules. Many countries are exploring this new arena of warfare and do not quite understand it well enough to agree to stop exploring it."

Even more importantly, he adds, it is very difficult to attribute responsibility to actions within cyberspace because of its complexity, "so imposing consequences to treaty violation would be problematic."

Rising Cyber Attacks Costing Health System $6 Billion Annually

Source: http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually?linkId=14050233

A rise in cyber attacks against doctors and hospitals is costing the U.S. health-care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records, security researchers say.

Criminal attacks against health-care providers have more than doubled in the past five years, with the average data breach costing a hospital $2.1 million, according to a study today from the Ponemon Institute, a security research and consulting firm. Nearly 90 percent of health-care providers were hit by breaches in the past two years, half of them criminal in nature, the report found.

While intrusions like ones exposing millions of consumers at health insurer Anthem Inc. and hospital operator Community Health Systems Inc. have increased risk awareness, most of their peers are still unprepared for sophisticated data attacks, security experts have said.

"The health-care industry is being hunted and hacked by the elite financial criminal syndicates that had been targeting large financial institutions until they realized health-care databases are more valuable," said Tom Kellermann, chief cybersecurity officer at Trend Micro Inc., who wasn't involved in the study.

Medical records, which often contain Social Security numbers, insurance IDs, addresses and medical details, sell for as much as 20 times the price of a stolen credit-card number, according to Dell SecureWorks, a unit of Dell Inc.

Free Insurance

Thieves can use that information to take out a loan or open up a line of credit in the victim's name, or for medical identity theft, where the victim's insurance ID is used by an impostor seeking free medical care.

About half of health-care organizations surveyed by Ponemon said they didn't have sufficient technology to prevent or quickly detect a breach, or the personnel with the necessary technical expertise.

"The organizations are getting better, but it is a slow-moving train," said Larry Ponemon, chairman of the Ponemon Institute. He said many firms are moving from paper-based to automated systems, a transition that makes them "very vulnerable to criminal attacks."

Last year, health records on 88.4 million people were breached as a result of theft or hacking -- about twice as many as in 2010, according to a database kept by the Department of Health and Human Services, which requires organizations to report breaches involving more than 500 patients.

Dark Web

The numbers this year are already in excess of last year's, after hackers accessed almost 80 million records from Anthem and 11 million from the health insurer Premera Blue Cross.

Data is resold on private forums that specialize in selling stolen credit cards or Social Security numbers, or on the dark web, where users' identities are hidden and transactions are done anonymously in Bitcoins, said Patrick Peterson, chief executive

officer of data security firm Agari Data Inc.
He said he has seen thieves selling thousands of records containing information on people who've been diagnosed with HIV or have liver damage from alcohol use, among other conditions. He said he suspects the cyber security world only discovers a fraction of the theft going on -- "the tip of the iceberg."

Researchers hack a teleoperated surgical robot, revealing security flaws

Source: http://www.homelandsecuritynewswire.com/dr20150515-researchers-hack-a-teleoperated-surgical-robot-revealing-security-flaws

To make cars as safe as possible, we crash them into walls to pinpoint weaknesses and better protect people who use them.
This is the idea behind a series of experiments conducted by a University of Washington engineering team who hacked a next generation teleoperated surgical robot — one used only for research purposes — to test how easily a malicious attack could hijack remotely controlled operations in the future and to make those systems more secure.
Real-world teleoperated robots, which are controlled by a human who may be in another physical location, are expected to become more commonplace as the technology evolves. They are ideal for situations which are dangerous for people: fighting fires in chemical plants, diffusing explosive devices or extricating earthquake victims from collapsed buildings.

Outside of a handful of experimental surgeries conducted remotely, doctors typically use surgical robots today to operate on a patient in the same room using a secure, hardwired connection. But telerobots may one day routinely provide medical treatment in underdeveloped rural areas, battlefield scenarios, Ebola wards or catastrophic disasters happening half a world away.
A UW release reports that in two recent papers, UW BioRobotics Lab researchers demonstrated that next generation teleoperated robots using nonprivate networks — which may be the only option in disasters or in remote locations — can be easily disrupted or derailed by common forms of cyberattacks. Incorporating security measures to foil those attacks, the authors argue, will be critical to their safe adoption and use.
"We want to make the next generation of telerobots resilient to some of the threats we've detected without putting an operator or patient or any other person in the physical world in danger," said lead author Tamara Bonaci, a UW doctoral candidate in electrical engineering.
To expose vulnerabilities, the UW team mounted common types of cyberattacks as study participants used a teleoperated surgical robot developed at the UW for research purposes to move rubber blocks between pegs on a pegboard.

Raven II

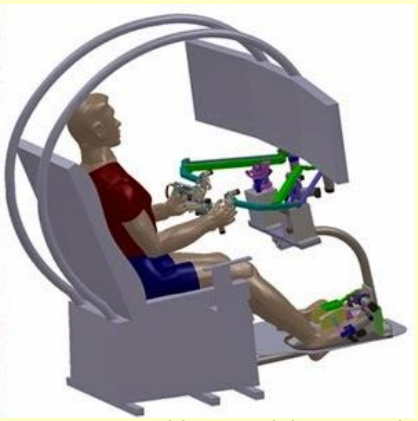
By mounting "man in the middle" attacks, which alter the commands flowing between the operator and robot, the team was able to maliciously disrupt a wide range of the robot's functions — making it hard to grasp objects with the robot's arms — and even to completely override command inputs. During denial-of-service attacks, in which the attacking machine flooded the system with useless data, the

robots became jerky and harder to use.

In some cases, the human operators were eventually able to compensate for those disruptions, given the relatively simple task of moving blocks. In situations where precise movements can mean the difference between life and death — such as surgery or a search and rescue extrication — these types of cyberattacks could have more serious consequences, the researchers believe.

With a single packet of bad data, for instance, the team was able to maliciously trigger the robot's emergency stop mechanism, rendering it useless.

The tests were conducted with the Raven II, an open source teleoperated robotic system



developed by UW electrical engineering professor Blake Hannaford and former UW professor Jacob Rosen, along with their students. Raven II, currently manufactured and sold by Seattle-based Applied Dexterity Inc., a UW spin-out, is a next generation teleoperated robotic system designed to support research in advanced techniques of robotic-assisted surgery. The system is not currently in clinical use and is not approved by the FDA.

The surgical robots that are FDA-approved for clinical use today, which typically allow a surgeon to remove tumors, repair heart valves or perform other procedures in a less invasive way, use a different communication channel and typically do not rely on publicly available networks, which would make the cyberattacks the UW team tested much harder to mount.

But if teleoperated robots will be used in locations with no secure alternative to networks or other communication channels that are easy to hack, it's important to begin designing and incorporating additional security features now, the researchers argue.

"If there's been a disaster, the network has probably been damaged too. So you might have to fly a drone and put a router on it and send signals up to it," said Howard Chizeck, UW professor of electrical engineering and co-director of the UW BioRobotics Lab.

"In an ideal world, you'd always have a private network and everything could be controlled, but that's not always going to be the case. We need to design for and test additional security measures now, before the next generation of telerobots are deployed."

Encrypting data packets that flow between the robot and human operator would help prevent certain types of cyberattacks. But it is not effective against denial-of-service attacks that bog down the system with extraneous data. With video, encryption also runs the risk of causing unacceptable delays in delicate operations.

The release notes that the UW team is also developing the concept of "operator signatures," which leverage the ways in which a particular surgeon or other teleoperator interacts with a robot to create a unique biometric signature.

By tracking the forces and torques that a particular operator applies to the console instruments and his or her interactions with the robot's tools, the researchers have developed a novel way to validate that person's identity and authenticate that the operator is the person he or she claims to be.

Moreover, monitoring those actions and reactions during a telerobotic procedure could give early warning that someone else has hijacked that process.

"Just as everyone signs something a little bit differently and you can identify people from the way they write different letters, different surgeons move the robotic system differently," Chizeck said. "This would allow us to detect and raise the alarm if

all of a sudden someone who doesn't seem to be operator A is maliciously controlling or interfering with the procedure."

Co-authors on the three telerobotic security papers include UW electrical engineering graduate students Junjie Yan and Jeffrey Herron, Tadayoshi Kohno of the UW computer science and engineering department, former UW computer science and engineering undergraduate Tariq Yusuf, Ryan Calo of the UW School of Law, and law student Aaron Alva.

ISIS preps for cyber war

Source: http://thehill.com/policy/cybersecurity/242280-isis-preps-for-cyber-war

May 17 – Islamic terrorists are stoking alarm with threats of an all-out cyber crusade against the United States, and experts say the warnings should be taken seriously.

Hackers claiming affiliation with the Islamic State in Iraq and Syria (ISIS) released a video Monday vowing an "electronic war" against the United States and Europe and claiming access to "American leadership" online.

"Praise to Allah, today we extend on the land and in the Internet," a faceless, hooded figure said in Arabic. "We send this message to America and Europe: We are the hackers of the Islamic State and the electronic war has not yet begun."

The video received ridicule online for its poor phrasing and the group's apparent inability to make good on its cyber threat this week.

But as hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends, experts said.

"It's only really a matter of time till we start seeing terrorist organizations using cyberattack techniques in a more expanded way," said John Cohen, a former counterterrorism coordinator at the Department of Homeland Security.

"The concern is that, as an organization like ISIS acquires more resources financially, they will be able to hire the talent they need or outsource to criminal organizations," Cohen added. "I think they're probably moving in that direction anyway."

Military officials agree. NSA Director Adm. Michael Rogers this week called the pending shift "a great concern and something that we pay lots of attention to."

"At what point do they decide they need to move from viewing the Internet as a source of recruitment … [to] viewing it as a potential weapon system?" Rogers asked.

While ISIS has been widely recognized for its social media prowess, the growing computer science talent of its recruits has mostly gone unnoticed.

"A number of individuals that have recently joined the movement of ISIS were folks that studied computer science in British schools and European universities," said Tom Kellermann, chief cybersecurity officer at security firm Trend Micro, who said ISIS's cyber capabilities are "advancing dramatically."

Even the man reportedly responsible for a number of the brutal ISIS beheadings, dubbed "Jihadi John" by his captives, has a computer science degree, Kellermann said.

The burgeoning online threat posed by Islamic extremists was part of the motivation for a new security pact announced Thursday between the White House and Gulf states.

In addition to securing infrastructure and providing cyber training, U.S. officials will also work with partner states to expand joint exercises that involve the potential for cyber warfare.

Part of the danger of the ISIS threat is the group's ability to marshal attacks from its sympathizers, generating a diffuse and unconnected network that is hard to track.

Kellermann said the video threats this week were "a call to arms more than anything," meant to incite individuals to act on their own.

"It has actually added a new dimension to the terrorist threat that our counterterrorism approach is not intended or designed to pick up on," Cohen said.

So far, supporters have focused on distributed denial-of-service attacks, spear phishing campaigns and hijacking legitimate websites to push malware, creating what are known as "watering holes."

"For example, if you go to an ISIS website and download their videos, you better recognize most of those websites are watering holes," Kellermann said. "[They are] basically trying to attack you while you're watching that video."

Experts think radical hackers are likely to expand this tactic to mainstream websites and powerful companies' websites as a way to gather information on targets.

"They're beginning to conduct more and more counterintelligence," Kellermann said.

The ISIS's use of the Internet has been described as unprecedented for a terrorist group, and lawmakers are growing increasingly concerned about U.S. attempts to counter its rhetoric online.

Sen. Cory Booker (D-N.J.) recently criticized U.S.-led online campaigns against radicalization as "laughable," saying he was "stunned" by the efforts' lack of sophistication.

Jen Weedon, threat intelligence manager at security researcher FireEye, said these concerns are understandable.

"Part of the reason why there's a belief that these emissaries are so savvy is because there's a sense of people not feeling that they're' in control of the message," she said.

Most of ISIS's current online power lies in its messaging, experts say, and not in its ability to hack real computer networks. But a handful of high-profile intrusions point toward its aspirations as a hacking group.

Almost every month of 2015 has been punctuated by some online attack by ISIS affiliates or sympathizers.

The so-called Cyber Caliphate took over the Twitter and YouTube accounts for the U.S. Central Command in January and the Twitter account for *Newsweek* magazine in February.

Then, the next month, the so-called Islamic State Hacking Division posted the personal details of 100 U.S. military personnel supposedly involved in attacks on ISIS in Iraq and Syria.

"Kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking they are safe," the group urged supporters.

In April, a French TV station was knocked offline in perhaps the best example of terrorists' abilities.

"It seemed to be of a broader scale than we had seen previously," Weedon said. "There were a number of facets to that attack, and they also took the station offline for quite awhile. That seemed to me to be of a different magnitude."

Some worry the next step is inevitable within the year.

Kellermann has noticed an uptick in ISIS activity on the "cyber arms bazaar," the massive underground dark Web market run out of Eastern Europe that traffics in almost every form of cyber sabotage imaginable.

"By the end of 2015," Kellermann said, "we're going to hear about significant attacks that were pulled off by sympathizers of ISIS."

Safety Resources for Ambulances Released by DHS S&T

Source: http://www.hstoday.us/single-article/safety-resources-for-ambulances-released-by-dhs-s-t/86d2c50fa4f1031e3a6356e87a1474bb.html

Two ambulance safety resources for emergency medical services (EMS) leaders, professionals and organizations nationwide the aim of which is to reduce the injury and fatality rate of EMS personnel have been released by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T).

According to data from the National Highway and Traffic Safety Administration (NHTSA), the fatality rate of EMS professionals is three times greater than the average in any other occupation.

"In the rush to deliver care and get a patient to the hospital, first responders often place their own safety on the line," said DHS Deputy Under Secretary for Science and Technology Dr. Robert Griffin. "By developing and releasing these resources, we can address key design concerns and training needs to ensure patients and EMS professionals are transported safely.

The first of the two resources, the *Ambulance Patient Compartment Human Factors Design Guidebook*, recommends improved physical design standards. The second resource, the *Research Study of Ambulance Operations and Best Practice Considerations for Emergency Medical Services Personnel*, addresses operational procedures and practices while operating an ambulance.

"To develop design guidelines, S&T coordinated with the National Institute for Occupational Safety and Health (NIOSH) and the National Institute of Standards and Technology (NIST) to observe EMS professionals in the back of ambulances, specifically looking at the ergonomics of the patient compartment," S&T said in its announcement. "They worked with EMS providers to determine the safest position for the caregiver and the patient. Additionally, the multi-agency team looked at the safety of the individual aspects of the vehicle in the event of a crash, and developed recommendations for EMS provider and patient restraints, cots and equipment mountings."

Pulling from several existing EMS resources and data, S&T and its partners developed the best practices to give localities a consolidated resource that can inform standard operating procedures and processes that many EMS organizations are lacking.

S&T, NIST and NIOSH also plan to make these resources available to ambulance accreditation bodies such as the National Fire Protection Association and the Commission on Accreditation of Ambulance Services.

"Ultimately," S&T said, "the application of these resources at a user level and within guidelines will ensure that EMS response is safer from a design and practices standpoint."

How to Make a Safe Room within an Existing Structure

Source: http://construction.about.com/od/Construction-Design/fl/How-to-Make-a-Safe-Room-Within-an-Existing-Structure.htm?r=9F

A safe room can be very expensive to build and even more challenging to design when there is no room available. Sometimes the only option is to retrofit an existing space providing that safe area within the structure.

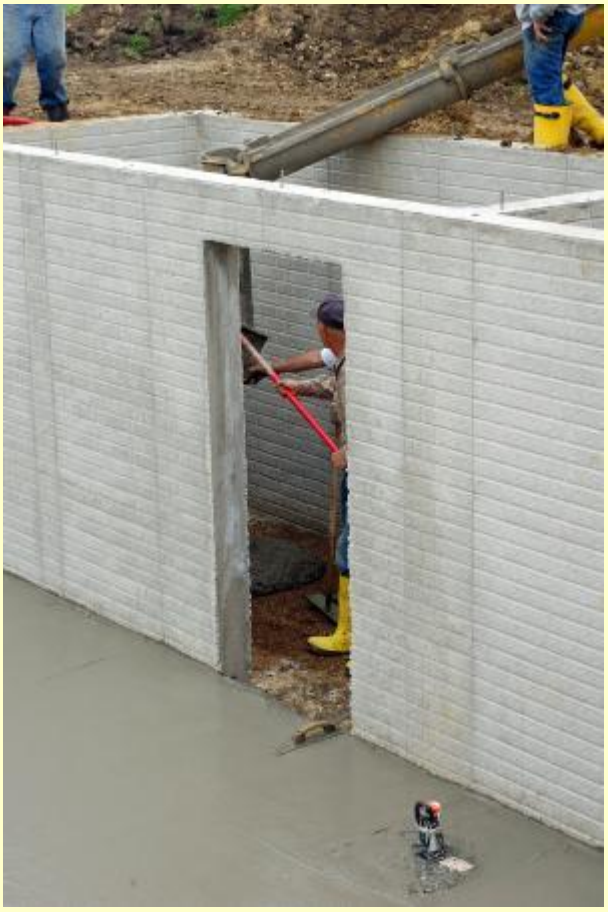
Best Areas for a Safe Room

Considering a traditional structure, corridors are always considered as the safest areas of the structures, because roof heights and they are normally free of obstructions.

However, ti might be challenging to storm proof a hallway because it might contain many doors and openings that shall be prepared to become air tight. Other areas that can be considered as potential safe rooms are offices, workrooms and lounges but they might be ale to withstand the impact of a 15-lb design missile at 100 mph.

How to Retrofit Areas as Safe Rooms

The following plan shall be put into effect to retrofit certain areas so they can be considered as safe-rooms.



- Replace existing doors, including door hardware vulnerable to fail after a missile has impacted them or susceptible to fail under tornado force winds with metal doors.
- Wall sections or glazing unable to withstand tornado winds or missile impacts shall be replaced with wall sections that meet code criteria, **ICC 500-2014: ICC/NSSA Standard for the Design and Construction of Storm Shelters.**
- Use or install metal doors, impact-resistant glazing or shutter systems that meet building code standards.
- Walls can be modified or recessed to protect existing doors from the direct impact of flying debris,

Safe Room Retrofitting Mistakes

When you are trying to retrofit an area to bring up to storm resistant standards, you need to avoid these pitfalls:

- Check that the budget is enough to complete the project
- Double check walls and openings, as these might always be the weakest points and sometimes the protection might not be good enough.
- Do not retrofit a door or window if the wall is not able to withstand wind load or flying debris.

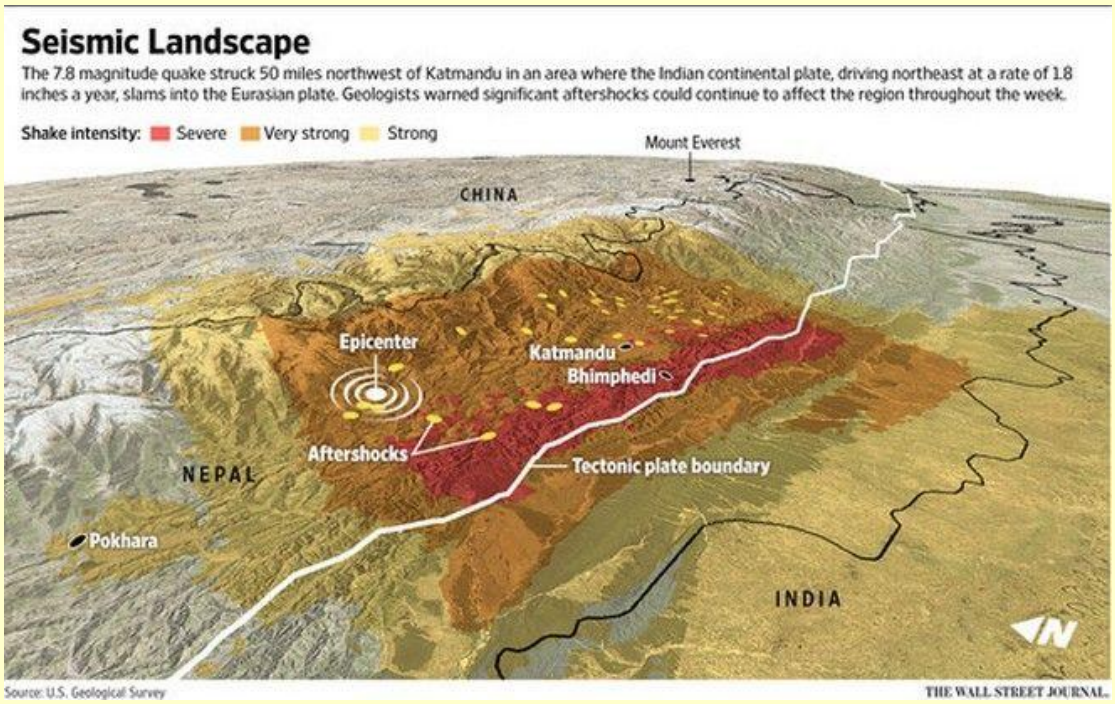
- Check that the roof is not design to act together as a whole. Roof can be retrofitted in a specific area to provide adequate protection.
- Unable to protect equipment installed at the roof such as vents, skylights and others.
- Areas that are unable to withstand wind pressure such as load-bearing and non-load-bearing walls
- Not using shutter systems and doors rated to meet FEMA 320 and 361.
- A system that encourages using manually installed shutter might fail as time will not be sufficient to have them properly installed.
- Not securing a door with at least six points of connection. Ideally a good system must have three hinges and three latching mechanisms
- Door frames constructed of inappropriate thickness. Door frames should be constructed of at least 6-gauge metal and adequately secured to the walls to prevent the complete failure of the door/frame assemblies

- Never consider to use a mechanical room as a safe room area unless it is life threatening situation
- Always try to avoid storage areas that are small in size when compared to the amount of persons using the safe room.
- Not verifying that all material and building components meet **ICC 500-2014: ICC/NSSA Standard for the Design and Construction of Storm Shelters or more restrictive code regulation.**

Nepal shows its vulnerability after devastating earthquake

By Simon Redfern

Source: http://www.homelandsecuritynewswire.com/dr20150427-nepal-shows-its-vulnerability-after-devastating-earthquake



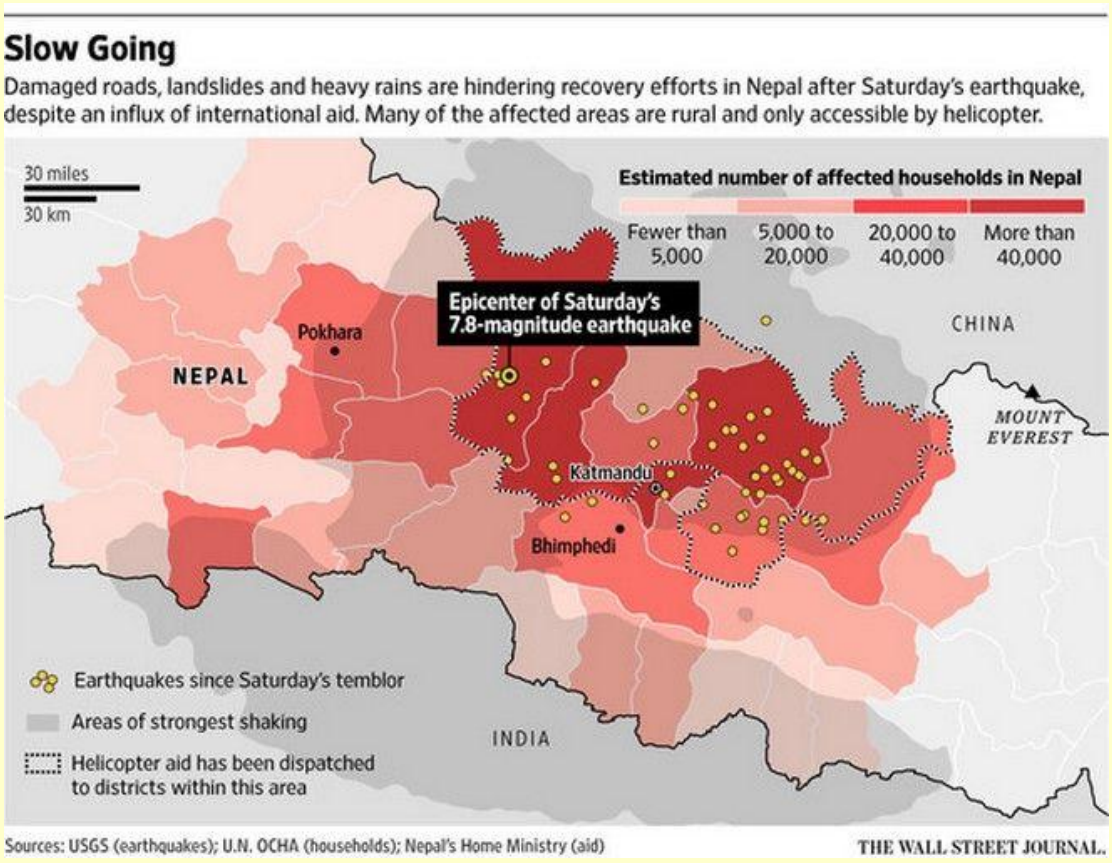
Apr 27 – For some time scientists have realized that the Kathmandu valley is one of the most dangerous places in the world, in terms of earthquake risk. And now a combination of high seismic activity at the front of the Tibetan plateau, poor building standards, and haphazard urbanization have come together with fatal consequences.

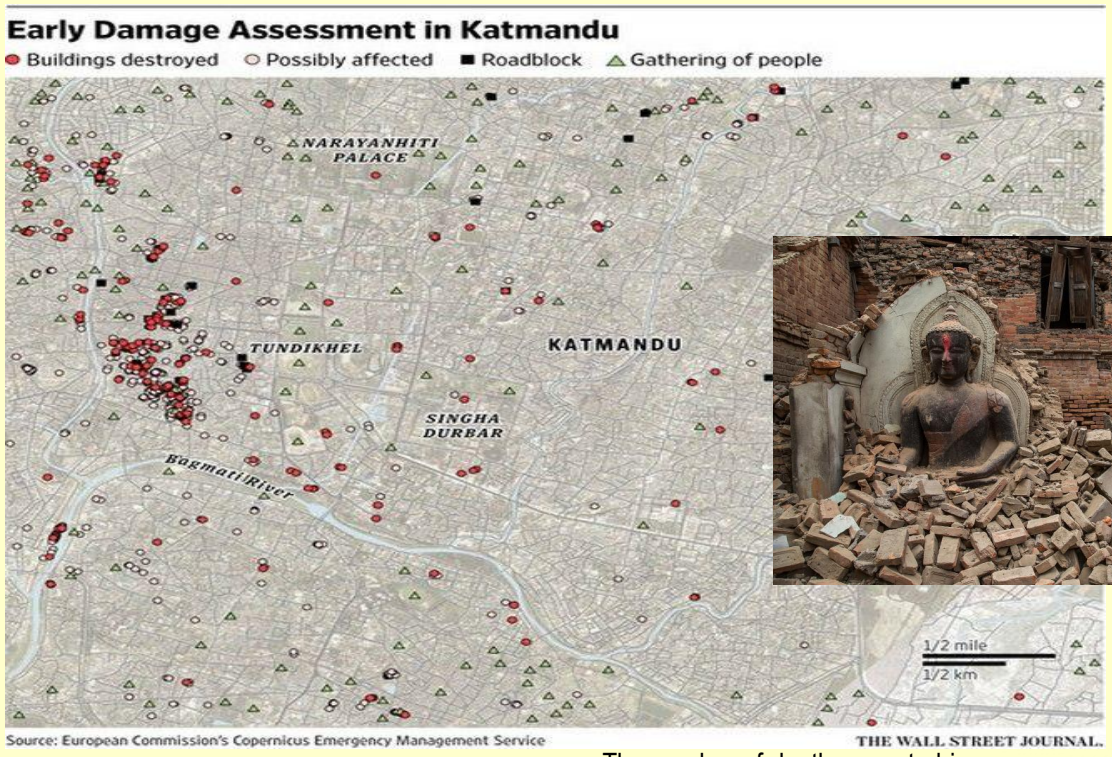
The magnitude 7.9 earthquake that hit Nepal hit just before noon, local time, on Saturday around forty-eight miles north west of Kathmandu. The Indian tectonic plate is driving beneath the Eurasian plate at an average rate of forty-five millimeter per year along a front that defines the edge of the Tibetan plateau. This force created the Himalayas, and Nepal lies slap bang along that front. The quake was shallow, estimated at twelve kilometers depth, and devastating as the Indian crust thrust beneath Tibet one more time.

Historic buildings in the center of Kathmandu have been reduced to rubble. Brick masonry dwellings have collapsed under clouds of dust. Weakened buildings will now be vulnerable to aftershocks, which continue to rattle Nepal through the day. Multiple aftershocks above magnitude 4 hit in the six hours following the earthquake.

Away from the populated Kathmandu valley, in the heights of the Himalaya, climbers on Everest tweeted reports of damage to base camp, and fatal avalanches on the flanks of the mountain. The steep valleys and precipitous dwellings of the more populated areas are vulnerable to landslides. Now is the time for us all to consider how we can help those most in need, in practical ways.

Although one cannot predict the day or the hour, the scenario that we see on our TV screens had been thought through many times already, with one particularly prescient article written almost two years ago to the day. The likely impacts of the quake can be readily estimated, and in any case will soon be reported directly from the surroundings.





The number of deaths reported is only, tragically, going to increase, with the U.S. Geological Survey putting estimates of fatalities in

the range of thousands to tens of thousands.
Just one week ago my geophysicist colleagues returned to the United Kingdom from a meeting in Kathmandu, Nepal, as part of the Earthquakes Without Frontiers research project. The focus was earthquake risk reduction and hazard awareness in Nepal. The risks have been recognized for some time, but I don't suppose any of the participants expected their work to be thrown into the spotlight so soon.
Professor James Jackson, of Cambridge University and one of the leaders of the Earthquakes Without Frontiers project, talked with me on his return from Kathmandu last weekend. He described tall, thin houses, with extra stories built up on top, explaining how they arise from the Nepalese tradition of sharing inherited property between siblings, with houses split vertically between them.
The only way to build is upwards. In a seismic area, it's a recipe for disaster, and one can't help but wonder what this phenomenon has wrought on families in Kathmandu.

***Simon Redfern** is Professor in Earth Sciences at University of Cambridge.*

Emergency Managers Debate the Need for Background Checks for Volunteers

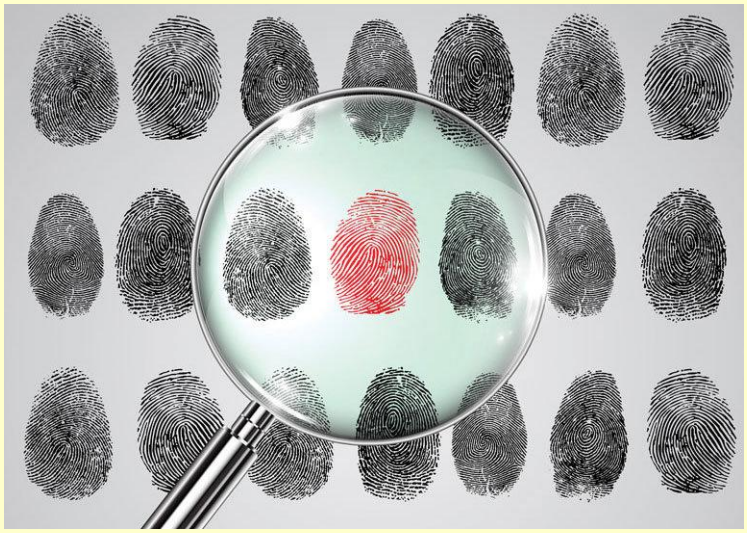
Source: http://www.emergencymgmt.com/training/Emergency-Managers-Debate-Background-Checks-for-Volunteers.html

It ought to go without saying that a volunteer firefighter isn't going to perpetrate a sex crime or rob a house when he's supposed to be dousing the flames. Apparently it isn't that obvious.
Last year New York Gov. Andrew Cuomo signed a law requiring background checks to ensure volunteer firefighters weren't carrying sex offense convictions. It's up to individual fire companies to decide whether a prospective volunteer is fit to serve, in spite of a past sex offense, but everyone gets screened.
In Rush County, Ind., volunteers for Community Emergency Response Teams (CERTs) must submit to an even broader check, one that encompasses all past criminal history.
At first blush it might seem counterintuitive to run background checks on volunteers. These people have stepped up to help; they certainly appear to be of goodwill.
Yet advocates of background checks cite a number of reasons why a CERT or other response organization should dig into the history of potential volunteers. The emergency management community seems to be heeding these calls: Around the nation, volunteers at a range of levels are having their histories poked and prodded before they're allowed to join the team.

The phrase heard most often in regard to background checks is "vulnerable populations." When people are in crisis they may succumb more easily to predators, a premise that applies especially to children, the old and the infirm. When responders and rescuers come into contact with these populations, the argument goes, emergency managers need to be sure that these Samaritans can shoulder the task responsibly.
"The upside to a background check is that you have confidence in the people you are working with, you can feel comfortable sending them out in the community under your own banner," said Bruce Fitzgerald, director of the Maine Emergency Management Agency. "If a CERT is associated with the emergency management office, you want to have that confidence in the people you are putting out there."
In Rush County, Emergency Management Agency Director Charles Kemker suggests that background checks may help an agency to fortify its legal defense. If a volunteer's bad actions should ever land on its doorstep in the form of some legal liability, "who is going to be held accountable for them?" he said. A background check may show the agency had done its due diligence to ensure the public good, perhaps absolving the agency of some culpability.
Background checks could also help to ensure public trust. When people see a first responder with a CERT credential, they likely presume this person is "safe,"

someone they can rely on in a crisis. For example, children are taught to look for the person in uniform. An inspection of a volunteer's past can help ensure that trust is well founded.

These arguments have proven compelling in public life, not just among emergency response organizations. In Howard County, Md., even the Recreation and Parks Department runs



investigations on everyone from coaches and instructors to sports advisory board members. Adoption at this level suggests a high degree of confidence in the background check as a meaningful safeguard.

But it won't be a perfect precaution. For example, many bad actors don't have criminal records. In fact, some in the emergency community see a range of reasons to oppose the background check.

The process costs money. The funds don't usually come out of the CERT budget, but someone has to pay for these background checks, whether it be the local police department or some other entity. Checks take time too, potentially slowing the intake process at a moment when volunteers are needed.

In addition, the prospect of a background check could scare away potential volunteers. Some might not want their personal history examined or may fear the details in the report will become public knowledge.

"With several hundred volunteers, to date, we have not performed background checks," said Demetrius Kastros, a Monterey, Calif., CERT instructor. "Background checks are usually conducted by the law enforcement agency of a jurisdiction, and they usually have enough constraints on their time without doing background checks on the 35 students in a CERT class."

In any case, he suggests, the very nature of an emergency likely would limit the kind of harm a potential criminal might perpetrate. "CERT members operate in teams and are not working with overly expensive or sensitive equipment, where there are concerns about loss of materials," Kastros said.

Interestingly the business of vetting volunteers extends beyond the emergency management community. While CERTs tend to rely on state and local law enforcement to fund background checks, a growing niche industry has sprung up to conduct this work for others in the nonprofit community. Organizations such as First Advantage, AccuSource and True Hire's subsidiary Background Checks for Volunteers all offer to help the nonprofit community conduct investigations for a fee.

Clearly strong cases exist for and against the use of background checks in emergency response. To see how these arguments play out in practice, it helps to look at a few specific situations.

The 400 active volunteers in the Austin, Texas, CERT represent a broad swath of the local population. Their ages, professions and ethnicities all may vary. But these green-vested responders all have one thing in common: clean criminal records.

To become a CERT volunteer, it's not enough to attend one of the twice-yearly, eight-session classes, or to join the monthly meetings for continuing education and training. To earn the ID emblazoned with city and CERT logos, volunteers must submit to the background check.

The police department runs the check and picks up the tab for any associated costs. Individuals are matched against the Texas penal code for past violations, and their fingerprints are run against an FBI database. It's the same level of scrutiny as is applied to any city employee, said Jacob Dirr, a spokesman for the Austin Office of Homeland

Security and Emergency Management.
"There is the potential for our volunteers to come into contact with children or vulnerable populations, and we want to ensure that in those instances we are doing our due diligence," he said.
While some may be concerned that such checks will scare off potential volunteers, Dirr said he has never known that to be the case. Nor has the check impeded what some say is a vital aspect of emergency response: That is, the spontaneous volunteer. Such individuals have been a crucial component in many emergency operations, such as the 2014 Oso mudslide in Washington state, where hundreds of volunteers helped mitigate a landslide that killed more than 40 people.
Austin makes sure CERT's background checks do not slow any emergency response. To do this it relies on a memorandum of understanding with the American Red Cross, which typically will lead the intake of volunteers during a major disaster. The CERT will put these people to work, even without the usual investigation. "If we are in an instance where we have spontaneous volunteers, nine times out of 10 we are going to be doing that with the American Red Cross, and they have their own very efficient ways of checking people before they are accepted as Red Cross volunteers," Dirr said.

Not everyone agrees with this way of thinking. Sometimes the organization of a community's emergency response mechanisms will actually mitigate against the need for a background check.
Among the 3,000 CERT volunteers in Palm Beach County, Fla., not one has even been subjected to investigation. Primarily the job of the public safety department is to collect a $50,000 state grant and then to pass it through to fund training at the local state college, said Vince Bonvento, an assistant county administrator and also director of the Public Safety Department.
Volunteers get trained and certified, but they also get badges stating they are not county employees or even sanctioned volunteers. "If they were volunteers for the county we would be responsible for their actions," Bonvento explained. That's not a weight the county wants to bear — not when most volunteers spend their time patrolling retirement communities.

To take responsibility for these helpers, the county would probably want to run background checks, and that raises a range of tough questions. "What are going to be the criteria you are going to use to deny someone a CERT certification? There are various levels of misdemeanor; there are these different levels of checks. All of that would have to be defined," Bonvento said. "If there is cost involved, do you pass that on to the volunteers? Will it be allowable to take it out of the grant?"
Answers to these and other questions may be forthcoming, as Florida's inspector general recommended recently that background checks be made mandatory for emergency volunteers. That would suit Bonvento just fine, as long as the state is willing to take on responsibility for the effort. "If it is going to be done it needs to be done by the state of Florida," he said. "They need to come to the counties, and they need to give us direction."

Even when checks are run, a dubious score doesn't mean automatic rejection, at least not in Rush County. Most investigations, for example, will delve into credit history: A person with financial troubles may be more apt to abuse trust. But Kemker doesn't look at those scores.
"There are a lot of people having financial hard times right now," he said. "We are not going to exclude someone based on that."
Even criminal blips may be overlooked. "We have had some that have been questionable, where maybe the people they run with have an extensive history with law enforcement and they are just 'known associates,'" Kemker said. "We sit with them, we discuss it and we give them a chance."
The returns on that effort can be mixed. "We have had a couple of them that have been straight with us, who have been willing to make a change and have become better citizens. Then we've had others who we find out they are still associating with those people, or they are making racial slurs or sexual innuendos on Facebook."
So Kemker runs the check, but he relies most heavily on interviews between candidates and present volunteers. "They sometimes tend to get a better description of what the people will be like, bringing out things that would not normally show up on a background check

as far as their attitude and their actions."
In some states, investigations into the criminal histories of emergency volunteers remain something of a mixed bag.
In Maine, where there is no statewide oversight of volunteer programs, counties manage their own CERTs, Fitzgerald said, and it is hit and miss as to which choose to run background checks.
Fitzgerald knows of cases in which a volunteer's checkered past has caused planners to shift direction or even decline assistance. "I have heard of instances where a background check turned up something that might be concerning, and we have either had to change the role of that volunteer and think about where we might use their skills, or else say thanks but no thanks."
While counties are free to choose the level of scrutiny they wish to apply, Fitzgerald's bottom line is pragmatic: Unless there is some compelling reason not to, let's get those people into the pipeline. "If there is a need in a community and you have a group of people who want to get training, you want to take advantage of that," he said. "It's hard enough to find people who are willing to volunteer and do this kind of work."

Adam Stone *is a contributing writer for* Emergency Management *magazine. Stone writes on business and technology from Annapolis, Md. He also contributes to* Government Technology *magazine.*

EDITOR'S COMMENT: Although volunteering is a noble gestrure towards society, we live into dubious times, so: **definetly background checks!**

Disaster Preparedness & Response Require Having Faith

By Raphael M. Barishansky & Audrey Mazurek

With people regularly attending services each week at faith-based organizations around the world, these organizations must have plans in place to provide safe egress of large crowds of attendees from their buildings on a regular basis. Much can be learned from and implemented into such organizations to provide greater community resilience.

The world of emergency response is ever expanding with governmental responsibilities to communities increasing on an almost daily basis. However, whether the emergency is naturally occurring or human-caused, there are times when the governmental agencies that are set up to provide help to communities will be overwhelmed. It is during times like this when citizenry, through established volunteer-based groups such as the Community Emergency Response Team (CERT) and the Medical Reserve Corps (MRC), swing into action to act as an adjunct to local, state, regional, territorial, tribal, and federal government response agencies.

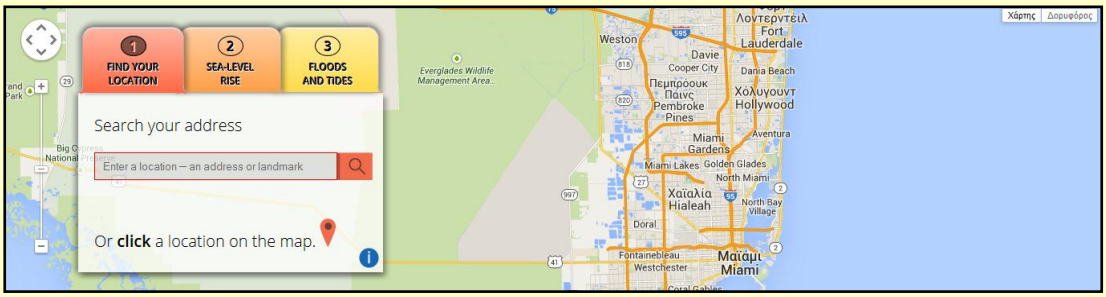
Source: http://www.domesticpreparedness.com/pub/docs/DPJApril15.pdf (p.16)

Raphael M. Barishansky*, MPH, MS, CPM is director of the Connecticut Department of Public Health's Office of Emergency Medical Services (OEMS). Before establishing himself in this position, he served as chief of public health emergency preparedness for the Prince George's County (Maryland) Health Department.*
Audrey Mazurek *is a deputy program manager with ICF International, specializing in public health and healthcare preparedness. Previously as a technical specialist for ICF, she served as a public health preparedness planner for the Prince George's County and Montgomery County (Maryland) Health Departments. Prior to this position, she was an analyst at the Homeland Security Studies and Analysis Institute (HSSAI), and program manager at the National Association of County and City Health*

Officials (NACCHO). Ms. Mazurek is also the managing director for TSGStrategies, LLC.

Web app helps Miami residents visualize how sea level rise affects their homes

Source: http://www.homelandsecuritynewswire.com/dr20150430-web-app-helps-miami-residents-visualize-how-sea-level-rise-affects-their-homes



Apr 30 – Florida International University's School of Journalism and Mass Communication in conjunction with Geographic Information Systems (GIS) Center have developed a web app, known as the Sea Level Rise Toolbox, which helps Miami-Dade residents visualize the possible impact of rising seas in South Florida on their neighborhoods.

An FIU release reports that the Web app, using elevation data from the Google Elevation Service, and based on sea level rise calculations created by Peter Harlem, a scientist at FIU's Geographic Information Systems (GIS) Center, is an interactive sea-level rise viewer where users can enter an address to visualize how up to a 6-foot rise in sea level may affect Miami-Dade County neighborhoods.

"Our goal with our app is to inform residents of South Florida about the potential impact of sea level rise where they live," said Susan Jacobson, assistant professor of journalism at FIU and the web app project manager. "We want to help our fellow Floridians understand sea level rise and how it may affect their community."

The Sea Level Rise Toolbox will also include a database of flood reports from both government and citizen sources in South Florida. Miami-Dade County recently launched an open data portal that includes flood reports, which will be included in the flood database.

"The flood report database will help residents identify the incidence of what the National Oceanic and Atmospheric Administration calls 'nuisance flooding,' a phenomenon that is increasingly common as sea levels rise," Jacobson said.

The Web app is free and was officially launched at BarCamp Miami on 28 March.

The Web app was developed under SJMC's Eyes on the Rise, a project funded by the Online News Association.

NOAA study finds marshes, reefs, beaches can enhance coastal resilience

Source: http://www.noaanews.noaa.gov/stories2015/20150429-noaa-study-finds-marshes-reefs-beaches-can-enhance-coastal-resilience.html

The resilience of U.S. coastal communities to storms, flooding, erosion and other threats can be strengthened when they are protected by natural infrastructure such as marshes, reefs, and beaches, or with hybrid approaches, such as a "living shoreline" — a combination of natural habitat and built infrastructure, according to a new NOAA study.

The study, published in *Environmental Science and Policy*, assesses reports and peer-reviewed studies on the strengths and weaknesses of using built infrastructure, such as seawalls or dikes, natural infrastructure, or approaches which combine both. The study focuses on how these approaches help coastal

communities reduce their risk of flooding and erosion, as well as additional benefits, and the tradeoffs when decision makers choose one type over another.

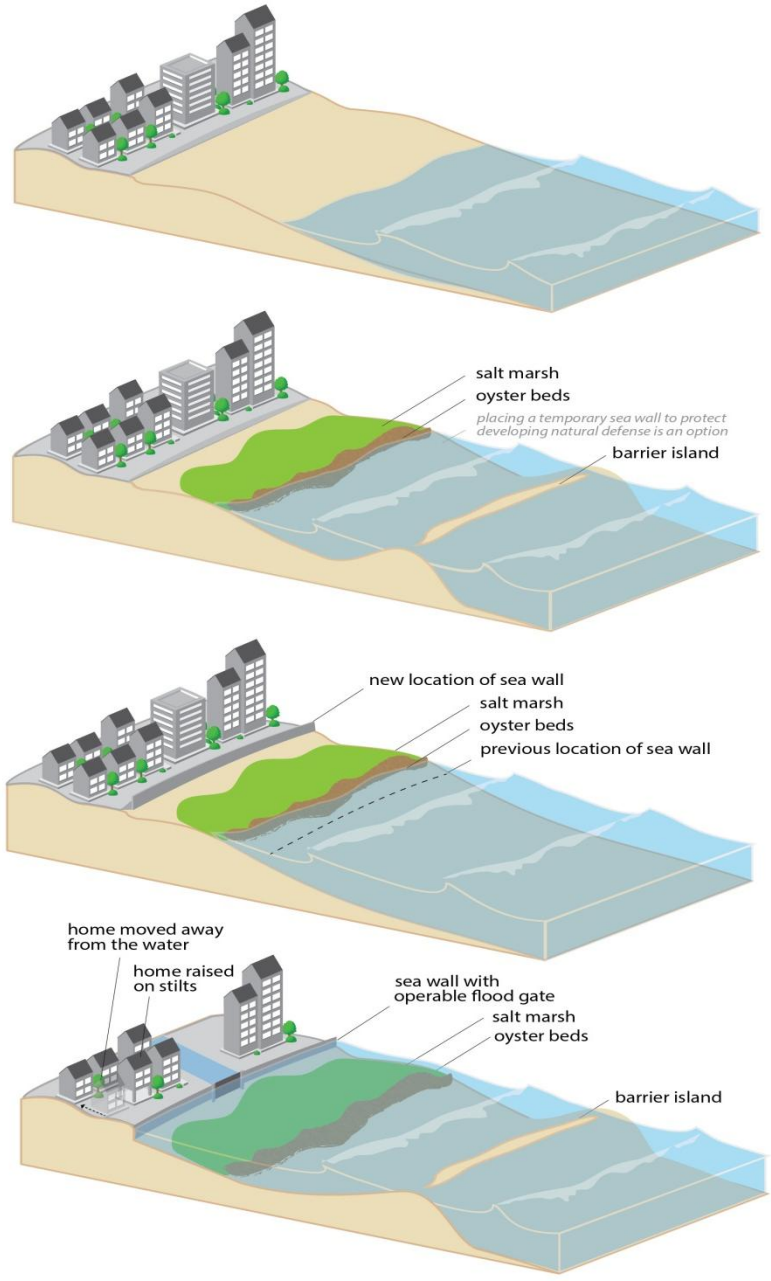
adviser. "Natural and hybrid systems can also improve water quality, provide habitat for many important species, and mitigate carbon going into our atmosphere."

Minimal Defense
Many communities have developed right along the ocean with only minimal natural defenses from a small strip of beach between them and the ocean.

Natural
Natural habitats that can provide storm and coastal flooding protection include salt marsh, oyster and coral reefs, mangroves, seagrasses, dunes, and barrier islands. A combination of natural habitats can be used to provide more protection, as seen in this figure. Communities could restore or create a barrier island, followed by oyster reefs and salt marsh. Temporary infrastructure (such as a removable sea wall) can protect natural infrastructure as it gets established.

Managed Realignment
Natural infrastructure can be used to protect built infrastructure in order to help the built infrastructure have a longer lifetime and to provide more storm protection benefits. In managed realignment, communities are moving sea walls farther away from the ocean edge, closer to the community and allowing natural infrastructure to recruit between the ocean edge and the sea wall.

Hybrid
In the hybrid approach, specific built infrastructure, such as removable sea walls or openable flood gates (as shown here) are installed simultaneously with restored or created natural infrastructure, such as salt marsh and oyster reefs. Other options include moving houses away from the water and/or raising them on stilts. The natural infrastructure provides key storm protection benefits for small to medium storms and then when a large storm is expected, the built infrastructure is used for additional protection.



"When making coastal protection decisions, it's important to recognize that built infrastructure only provides benefits when storms are approaching, but natural and hybrid systems provide additional benefits, including opportunities for fishing and recreation, all the time," said Ariana Sutton-Grier, Ph.D., the study's lead author, member of the research faculty at University of Maryland and NOAA's National Ocean Service ecosystem science

Examples of coastal defenses including natural infrastructure, managed realignment, and hybrid approaches. (Credit: NOAA).

Threats like coastal erosion, storms and flooding can reshape the shoreline and threaten coastal property. With approximately 350,000 houses, business, bridges and other structures

located within 500 feet of the nation's shoreline, erosion is a problem many U.S. coastal communities are addressing.

Coastal flooding caused by extreme weather events and sea level rise is of growing global concern. As noted in this study, in 2012 there were 11 weather and climate billion-dollar

disaster events across the United States, including superstorm Sandy, causing 377 deaths and more than $110 billion in damages. While only two of those were coastal events, Sandy alone was responsible for nearly sixty percent of the damages, at $65 billion (the other, Hurricane Isaac, caused $3 billion in damage). Nationally, these made 2012 the second costliest year on record for weather disasters. Only 2005, which incurred $160 billion in damages due in part to four devastating coastal hurricanes, saw more.

"Coastal resiliency and disaster risk reduction have become a national priority, and healthy coastal ecosystems play an important role in building resilient communities," said Holly Bamford, Ph.D., acting assistant secretary of commerce for conservation and management at NOAA, and co-author of the study. "We know that sea levels are rising and that coastal communities are becoming more vulnerable to extreme weather- and climate-related events. Now is the time to invest in protection to secure our coasts, but we need to make those investments wisely and with a full understanding of the costs and benefits of different approaches."

The study points out that there is still a need for built approaches in some locations. However, natural or hybrid approaches can be used in many cases.

Some natural ecosystems can maintain themselves, recovering after storm events and reducing the cost of upkeep. Natural habitats such as coral reefs, marshes and dunes can act as buffers for waves, storms and floods. Natural ecosystems also can, in many cases, keep pace with sea level rise, while built infrastructure does not adapt to changing conditions.

"There is a lot of potential innovation with hybrid approaches," said Katya Wowk, Ph.D., NOAA senior social scientist, and the third co-author of the study. "Hybrid approaches, using both built and natural infrastructure, often provide more cost-effective flood risk reduction options and alternatives for communities when there is not enough space to use natural coastal protection alone."

Hybrid approaches, such as combining some habitat restoration with openable flood gates or removable flood walls, provide benefits while also providing more storm and erosion protection than natural approaches alone. The study highlights hybrid approaches in the New York City metro area and in Seoul, South Korea, to deal with their monsoon flooding events.

"One of the challenging aspects is that these approaches are very new, so we are still learning what works best in which situations and under what circumstances," said Wowk.

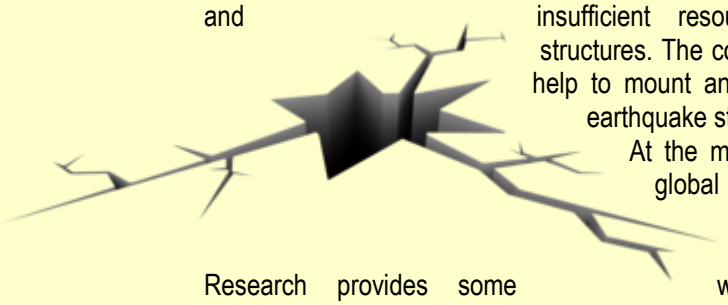
The authors suggest that every location where hybrid and natural

approaches are being implemented provide opportunities for monitoring so we can learn as much as possible about each approach, including longer-term cost effectiveness.
"There is no 'one size fits all' solution when it comes to what is best for a community in providing coastal protection from flooding," said Bamford. "We all have to work to innovate, test, monitor, and develop a better suite of options that includes more natural and hybrid infrastructure alternatives for providing coastal protection to communities around the world."
NOAA's mission is to understand and predict changes in the Earth's environment, from the depths of the ocean to the surface of the sun, and to conserve and manage our coastal and marine resources.

What works and doesn't in disaster health response

By Richard Bissell and Thomas Kirsch
Source: http://www.homelandsecuritynewswire.com/dr20150501-what-works-and-doesn-t-in-disaster-health-response

May 01 – On Saturday, 24 April 2015, a major (Magnitude 7.8) earthquake hit Nepal shortly after midday. Long-expected by seismologists, this large earthquake has left many of the older structures in this mountainous and economically challenged country of thirty-one million inhabitants in ruins. It has also released avalanches affecting mountaineers from all over the world.
As is the case of many mountain communities in developing countries throughout the world, Nepal is vulnerable to a trifecta of risk: a seismologically active landscape, slide and avalanche prone hillsides, and insufficient resources to construct modern earthquake-resistant structures. The country's poverty also means that it will require outside help to mount an effective response to the widespread needs of an earthquake stricken population.



At the moment, the most important question is how can the global community best respond? What can and what should international relief teams be prepared to do when responding to such an event?
Research provides some well-documented evidence that many international health-oriented responses are poorly targeted and may be influenced by objectives that play well on the home front rather than what's needed on the ground. Let's look at this from the perspective of the still-unfolding Nepal earthquake response.

Assess damage and determine immediate needs
The first function in the response to any emergency, whether it is a multi-vehicle crash on the local interstate, or a massive earthquake in the Himalayas, is to conduct an immediate situation assessment.
The most important aspect of this process is called the "needs assessment," which uses an initial damage assessment to predict what kinds of rescue, health, food and shelter needs exist at that time, as well as what will likely be needed going forward in the near- and midterm. As the needs are established, then the appropriate response can be directed to meet those needs.
International and United Nations-based organizations with previous experience in these kinds of assessments, and armed with the latest satellite imaging technology to estimate damage across the affected country, can provide assistance to local officials in setting response priorities.

Search and rescue needs to happen immediately
Earthquakes cause buildings to collapse, trapping people and causing massive amounts of injury. This was the case in the 2010 Haiti earthquake and now in Nepal. Fallen buildings make immediate search and rescue efforts critical to saving lives.
Unfortunately the nature of crush injuries necessitates rapid rescues and limits the amount of "saves" that external search and rescue (SAR) teams can accomplish. Crush syndrome, which occurs when blood circulation to a limb is cut off by heavy debris, can lead to kidney failure even if the victim is

successfully extricated. And crush injuries can also lead to severe, and sometimes fatal, blood loss. In both cases, rapid extrication is necessary to save lives.

Decades ago, disaster epidemiologist Erik Noji and others demonstrated that up to 90 percent of successful rescue extrications after earthquakes are done by family members and local bystanders. People trapped under rubble are likely to die quickly without immediate rescue. We can't expect much success from teams that arrive on-site 48, 72, or even 96 hours after the earthquake. Based on previous history, it is unlikely that the U.S. SAR teams deployed to Nepal (some seventy-two hours post-earthquake) will save many people.

Past history has shown that international SAR teams rarely save many lives at the cost of millions of dollars that might have been better employed in other relief and treatment functions, such as water purification, emergency food supplies, and medications to replace those lost in the rubble.

What kind of health response is needed most?

Then the question is: what kind of health response would better target the needs of the Nepalese? Urgent trauma care is critical in the first days and even the first week, and well-trained and provisioned teams from the region that can set up in days can make a difference.

These teams would be capable of providing necessary amputations and surgical repairs. It is important, however, that such surgical teams not use technologies that are beyond local capacity to deal with once the international teams have left. Working closely with local medical practitioners is key.

Much of the injury-related care does not need surgical intervention, and can be provided in clinics and mobile health settings. This might include care for broken bones, cuts, and superficial injuries. The extent to which outside help is needed is not a function of how fast international teams can respond, but rather how the well the country or region is prepared before the earthquake.

For example, our research shows that Chile was well-prepared to provide injury-related and primary care after the huge Concepción earthquake (Magnitude 8.8) in 2010, because that nation had a string of earthquake resistant primary care clinics and hospitals. The lesson here is that international response teams need to know the resilience status of local health care facilities before embarking on a response.

Infectious disease risks

In some cases, earthquakes may directly or indirectly lead to increases in infectious diseases. Earthquakes can damage or destroy sanitation systems. They tend to disrupt the local environment and how people live, leading to changes in the behavior of both humans and disease vectors, such as mosquitos.

For example, there was a rise in malaria in Costa Rica after the 1991 Limón earthquake. We found that this was due to several factors. People were sleeping outside, thus increasing their mosquito exposure, and regular mosquito- and malaria-control programs were delayed until bridges could be rebuilt.

Nepal has a long history of both intestinal bacterial or parasitic diseases and malaria. The earthquake has destroyed or damaged buildings throughout the country. Powerful aftershocks have made people understandably reluctant to return indoors, which means that many are sleeping outside. A concerted public health effort with international assistance may go a long way toward mitigating an earthquake-related upsurge in these kinds of diseases by prioritizing the provision of mosquito netting, temporary shelter, and clean potable water.

There will be more Nepals and Haitis in our future earthquake experience. Back in the early 1980s Dr. Claude de Ville de Goyet noted that certain kinds of disaster health relief seem to be perpetuated because "they photograph well." But we should shift the focus to things that actually work rather than what plays well on the news.

Looking forward to our next international earthquake responses, let us take into account what we have learned from past experiences, and, in coordination with our local hosts, provide the kinds of health assistance that are most likely to meet the needs of the people affected.

Richard Bissell *is Professor of Emergency Health Services at University of Maryland, Baltimore County.*

Thomas Kirsch *is Associate Professor and Director, Center for Refugee and Disaster Response at Johns Hopkins Medicine.*

Managing Emergencies

By Thomas Helmer

Source: http://csa-crisis.com/csa-today/managing-emergencies-part-one-preventing-and-preparing-for-emergencies/

Keeping in mind that different business sectors may require different response types, the overarching priority of any emergency response is to manage the People aspects first, then the impact on the Environment, followed by protecting Assets and last but not least, protecting Reputation. Often referred to as the P-E-A-R model, this is a good place to start.

PREVENTING AND PREPARING FOR EMERGENCIES

When tasked with setting up an emergency management system for your company, the following steps will ensure that you have used a proven best-practice methodology and can implement it effectively.

1. Identifying Hazards and Effects

A hazard can be described as a threat posing situation. This thread can be to life, health, assets, or the environment. Most hazards are dormant or potential, with only a theoretical risk of harm; however, once a hazard materialises, it can easily create an emergency situation. A hazardous situation that has come to pass is called an incident. Hazard and possibility interact together to create risk.

Hazards must be controlled effectively to reduce the risk of creating adverse effects. Therefore, each organisation needs to identify its hazards and effects. The process, called the Hazards and Effects Management Process (HEMP), was pioneered in the Oil and Gas sector, but is equally relevant to other industries and is the first step to determine the potential exposure a company must be prepared for.

Together with a multi-disciplinary team, start the process by listing all the potential hazards imaginable and then sort them in logical categories. For example –

- Pressurised Gases and Liquids
- Chemical substance (storage, handling, use)
- Dynamic Situations (e.g. Trucks, Cranes, Rotating Equipment)
- Differences in Height (e.g. working at height, objects overhead, slopes)
- Ergonomic (e.g. workspace, human machine interface)
- Biological (e.g. animals, insects, plants, bacteria)
- Security (e.g. civil unrest, terrorism, crime)
- Natural Environment (e.g. weather, flooding, earthquakes)
- Environmental Aspects (e.g. use of water, discharges, emissions)
- Etc.

Consider the hazards that have lead to incidents in the past in your company, but also in similar industries. Once the list is more or less complete, begin to identify where these hazards are in the organisation's operations, sites and facilities, make an inventory and describe what the effect(s) could be if control is lost.

Then list the current controls for each of the identified hazards and rate their effectiveness.

Results from this process must be documented in a Hazard and Effects Register and reviewed and updated annually. Best practice advocates that this Hazard and Effect Register should be externally audited every two years as a minimum.

TYPICAL ORGANISATIONAL PITFALLS

- The organisation has not developed or is not aware of the existence of a Hazard and Effects Register.
- The Hazard and Effects Register is out of date, incomplete, or not accessible.

2. Determining and Mitigating Risk

Each organisation must consider the risks they need to manage. Typically a Company Risk Register is used and updated monthly as part of financial controls.

Many companies choose to use a structured risk matrix to plot the severity of impact and likelihood of occurrence and to rate risks (low, medium, high, critical) and prioritise mitigation plans accordingly. ISO 31000:2009 guidelines that were developed for the Oil and Gas Industry can serve as a good starting point if nothing is in place yet.

When managing major risks affecting People, Environment and Assets, the high-level business risk management process (documented in the Company Risk register) is often insufficient to cover further associated risks. A deeper and more detailed risk assessment process is warranted for this purpose. Often structured to follow business functions or departments such as HSE (Health, Safety and Environment), Security and Reputation among others, these detailed risk registers are designed to catalogue specific risks with assigned owners and controls and where needed corresponding mitigating actions.

For both the high level Company Risk Register and the detailed risk registers, the following applies:

- Each risk must have a designated owner who shall be held accountable to manage that risk.
- Each identified barrier must have a designated owner who shall be held accountable to verify the effectiveness of the barrier at least annually.
- Each identified improvement opportunity must have a designated owner who shall be held accountable to scope the improvement.
- Opportunities must be ranked/prioritised annually.
- A sufficient number of opportunities must be selected for execution in the yearly business plan.
- The management team, acting as company risk committee, must review the high level risk register at least quarterly and consider whether priorities need to be changed.

Following this systematic methodology to identify risk enables your organisation to mitigate the risks to As Low As Reasonably Practicable (the ALARP principle) and also to develop the kind of response organisation and capability required in the unlikely event of a significant emergency occurring.

Results from this process must be documented in a Corporate/Site-specific Risk Register and updated annually which typically should be audited at least every two years by third party.

TYPICAL ORGANISATIONAL PITFALLS

- Risk registers are created by people with too little experience in what can go wrong.
- The organisation has not developed or is not aware of the existence of the Corporate/Site-specific Risk Register.
- Detailed Risk Registers are out-of-date, incomplete, and/or not accessible.
- Risk review meetings are not held and/or not treated seriously.
- Mitigation plans are not executed.

3. Developing the Emergency Response Organisation, Procedures and Practice

Following is a step-by-step approach to developing a robust Emergency Response Organisation:

- Define how the response organisation should be structured to manage the listed potential emergencies that could occur.
- Define what skills-sets are needed in what location.
- Nominate staff to be members of your Emergency Response Team. Ensure back-ups are also designated.
- Train the teams and practice regularly (minimum twice a year)
- Identify which external resources need to be mobilised and/or informed.
- Develop mutual aid contracts with other companies/agencies in areas where your own organisation lacks the capability to respond effectively. E.g. call centres, Oil Spill Response, Fire Fighting, rescue and evacuation, medical and psychological support.
- List all stakeholders involved that could be involved, collect their contact details and keep them up-to-date.

Results from this process must be documented in an Emergency Management Manual that must be updated annually. Most companies audit the results from the above process at least every two years.

TYPICAL ORGANISATIONAL PITFALLS

- Documents are out of date, incomplete, and/or not accessible.
- Staff nominated for Emergency Response duties are not trained
- Emergency drills and exercises are not conducted and/or do not develop skills of the nominated staff.
- Insufficient resources are nominated to provide 24/7 cover if needed.

MANAGING EMERGENCIES

When tasked with managing emergencies in your company, the following steps will need to be in place to ensure that you have deployed proven best practice:

1. Alert and Raise the Alarm
2. Evacuate People
3. Account for People
4. Mobilise your Emergency Response Team and Resources
5. Manage the Integrated Response Resources
6. Manage Stakeholders and Public Response

To develop an effective emergency management capability, organisations must first define the three main levels of response and then establish clear escalation criteria from one to the next. So let's begin by reviewing some definitions:

1. Incident - An incident is a non-routine event needing immediate attention that can be managed by the regular organisation at the premises.
Examples in incidents are non reportable/non-lost time minor events, minor vehicle accidents, short interruption to utilities and near misses. In such cases, the organisation can manage the situation with its own resources.

2. Emergency – An emergency is a sudden disruption of routine operations or a threat that causes injury/lost time to people, serious damage to property and/or products and/or non-achievement of business objectives. The situation requires assistance from external resources such as public emergency services, e.g. ambulances, fire brigade, etc.
Examples of emergencies are serious injuries hazardous material spills, fires, explosions, gas leaks or prolonged loss of utilities that would have a major impact on the ability to conduct normal business.

3. Crisis – A crisis occurs when an issue or emergency is out of control and begins to adversely affect the company's ability to achieve its objectives, threatens its reputation and can impact its license to operate. Outside forces (often led by the media's insistent demands for answers) can overwhelm management's ability to cope. Note that emergencies can escalate into a crisis, but a crisis can also occur without starting as an emergency first.
Possible triggers for a crisis can include fatalities, civil disturbances, third party hostile actions, epidemics, serious spills, fires, explosions, natural disasters, but also commercial events and even rumours.

1. Alert and Raise The Alarm

When an emergency is discovered, it is critical that all people (staff, contractors and visitors) on your premises be alerted as quickly as possible and respond in a controlled fashion.

The key objective of safety briefings is to ensure that anyone on site receives and understand fundamental safety information about your premises. This includes how to raise an alarm upon discovering an emergency, the different types of alarm (sounds and visuals) and the immediate instructions to follow with details such as layout, escape routes and assembly points. Therefore it is necessary to establish a watertight system that provides safety briefs to staff, contractors and visitors when they arrive at your location(s).

Everyone must understand that the alarm must be raised as soon as the emergency is discovered, before anything else and definitely before attempting to contain the emergency. Once the alarm is raised, staff must go to their designated assembly point as quickly as possible taking the shortest route, and should never get involved in the emergency.
Call-points to raise the alarm must be clearly visible from a distance and available at strategic locations, e.g. near staircases and exits.
People must respond to the alarm immediately and NOT wait for instructions.
On September 11 when the Twin Towers in New York were struck by airplanes, many of those who started walking down the stairs immediately upon hearing the alarm managed to leave the building and survived. Including a number that were working above the impact zone.
More and more companies opt for a short video with a simple quiz at the end. Some provide the option for visitors to watch the video on-line before arriving on location. Such methods facilitate good record keeping.
Alarm and public address systems must be tested at least monthly. The response of people must be tested at least quarterly.

TYPICAL ORGANISATIONAL PITFALLS

- People did not receive a safety briefing upon arrival nor a refresher.
- Alarm call points may meet legislative requirements, but may not be situated at obvious locations, are hard to find or obscured.
- People do not respond to an alarm and "wait for instructions" before moving to their designated assembly points.

2. Evacuate People

In the event of an emergency, getting people away from the site is of paramount importance. A disorganised evacuation can result in confusion, injury, and property damage. When developing your evacuation plan, it is necessary to consider the following:

- Determine which emergencies would require an evacuation;
- Determine in which emergencies it may be better to shelter-in-place;
- Establish a clear chain of command and designate the employee(s) in your business authorised to order an evacuation and/or shut down;
- Develop specific evacuation procedures, including routes and exits;
- Develop procedures for assisting visitors and employees to evacuate, particularly those with disabilities or who do not speak your language;
- Designate, if necessary, employees who will need to remain after the alarm has been raised to shut down critical operations or perform other duties before evacuating;
- Verify that you have sufficient trained first-aiders on each floor/area;
- Verify the need for provision of appropriate smoke hoods or respirators.

Designated Assembly Points, both inside and outside your premises, must be clearly signposted. These areas must provide sufficient space to accommodate the maximum number of people expected. Inside locations are often called refuges. Outside locations are often a parking lot or an open area away from busy streets, up-wind from prevailing wind conditions and located far enough away from the premises so that they do not restrict access for emergency response resources. Identify alternative locations should the primary area not be available.
An evacuation exercise must be held at least annually and more frequently at high-risk facilities, where a monthly or even a weekly drill may be prudent.

TYPICAL ORGANISATIONAL PITFALLS

- Floor wardens are not trained or not available during an emergency.
- Exits may be locked to avoid uncontrolled access and pilferage.
- Assembly Point locations may obstruct emergency response services access, e.g. car parks around the premises.

3. Account for People

To complete an evacuation, it is critical to confirm as quickly as possible that everyone has vacated the premises. This is to avoid committing rescuers to the emergency site to conduct search and rescue for someone who is not there.

In each area of the premises, e.g. a floor in a building or factory hall, groups of no more than 100, shall have a dedicated Assembly Point Checker (APC) taking charge of those gathered at the designated Assembly Point. Floor wardens report the result of their efforts to sweep the area before evacuation to the APC, including details about areas not checked and the reasons.

Accounting for people when they are standing outside the premises can be a daunting task unless it is well organised and practiced. Focus on getting a head count first and who is not accounted for next.

There should also be procedures to follow when people need to be redirected to a location further away and transport must be mobilised.

Many companies expect the security services to print out a list of all persons present in the building when the alarm goes off for use during the head count. Today, most premises use electronic security access systems to account for who is present in the building during normal conditions. Regrettably, this is not always used in an emergency situation. Some high-risk sites use Radio Frequency Identification (RFID) technology to establish the roll-call, which speeds up the process with accurate data.

TYPICAL ORGANISATIONAL PITFALLS

- Premises with security access systems often open the exit doors/gates to let all people out as quickly as possible thereby losing the ability to verify who is left inside.
- Some people may take the opportunity to go home instead of going to their assembly point and therefore may end up being counted as missing.

4. Mobilise Emergency Response

When an alarm is raised the appropriate emergency response resources must be mobilised whether the emergency is confirmed or not. This avoids wasting precious time and allows emergency response resources to practice their readiness even when it is a false alarm.

The person in charge at the emergency site, often called the On-site/On-scene Commander (OSC), is responsible to mobilise the appropriate resources without delay based on an assessment of what support may be required to deal with the emergency. **Prudent over-reaction** is considered best practice. E.g. valuable time is lost if the OSC waits to find out if a fire cannot be extinguished with hand-held units.

The OSC will also mobilise the Emergency Management Team at a location away from the emergency.

Aligned with the three levels outlined above – Incident, Emergency, Crisis – a three-tiered response model is advocated:

1. On Scene Commander (OSC) – Manages the Operational Response

- Is the most competent person at or near the emergency.
- Monitors the situation and leads the response on site.
- Rescues any persons on site and provides first-aid.
- Controls the emergency on site to prevent escalation.

2. Emergency Management Team (EMT) – Manages the Tactical Response

- Is lead by the Emergency Management Team Leader (EMTL)
- Maintains contact with the OSC.
- Establishes the head count and identify missing persons.
- Identifies and mobilises additional resources. e.g. police, fire brigades, ambulances, hospitals.
- Manages the interfaces between different resource providers and local stakeholders.

- Informs the Crisis Management Team.

3. Crisis Management Team (CMT) – Manages Strategic Response

- Is lead by the Crisis Management Team Leader (CMTL)
- Protects the company's reputation.
- Manages primary business and the broader implications of the crisis
- Manages interface with higher levels in the organisation, including the company board, shareholders, etc.
- Manages national and regional stakeholders, including media.

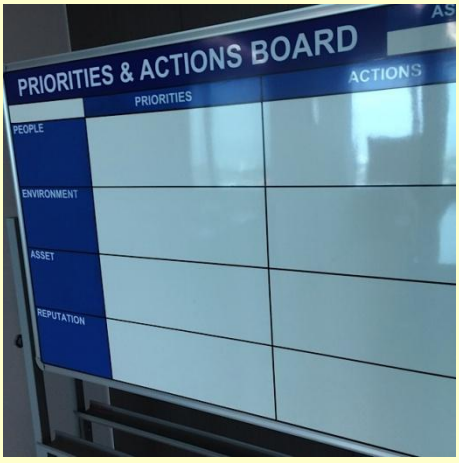
To manage the various aspects of an emergency effectively, it is essential that all staff nominated with Emergency Response duties be trained and practice regularly using a range of possible scenarios.
Depending on the size and complexity of the organisation it may be necessary to provide dedicated and equipped EMT and CMT facilities that are specifically designed for that purpose.
It is best practice that external resources (emergency services, fire department, etc.) be familiar with the premises and its hazards. Therefore, it is prudent and advised to conduct site visits for them at least annually and take them through a number of possible scenarios.
Safety Material Data Sheets (SMDS) for all hazardous materials on site must be readily available for all to use. E.g. a set of up-to-date data sheet must be held at the entrance gates. Plot plans must be maintained to identify where these materials are stored and in which quantity.

TYPICAL ORGANISATIONAL PITFALLS

- Those designated for Emergency Response duties are inadequately trained and do not practice often enough to be effective when it matters.
- The Emergency Management Team congregates too close to the emergency to manage the emergency effectively.
- Organisations are reticent to call out external resources in case it turns out to be a false alarm or a minor incident.

5. Manage Integrated Response Resources

When an emergency calls for resources from a variety of providers, e.g. security staff, volunteer fire fighters, first aiders, stretcher bearers, police, external fire brigades, ambulances, hospitals, etc., they must be well-coordinated to be effective. To avoid congestion on your site, it is essential to have detailed deployment plans upfront and share them with the various providers.



To coordinate multiple resource providers on one emergency site, the Emergency Management Team Leader and his team must keep track of who and what is mobilised using detailed tracking logs and who is where, marking plot plans for the team to keep a detailed overview. The EMTL must call regular time-outs to ensure that all team members are aligned, calibrate priorities and assess resources.
It is also necessary to consider what is needed should an emergency prolong, e.g. food and beverage, a rest and relief, and the availability of consumables e.g. firewater and fuel for trucks, tenders and buses.
When the premises are located in an urban or city environment, local emergency response authorities may take over command and control of the situation. In such cases it is critical that they understand your business and its risks, and that you are able to support them with detailed information such as layouts and the presence of any hazardous materials.

TYPICAL ORGANISATIONAL PITFALLS

- Local emergency response may be inadequately prepared for the risks found on your premises thereby posing unacceptable risks to their people and resources.

- Too much equipment is mobilised hampering the response activities.

6. Manage Stakeholders and Public Response

Stakeholders may be impacted or may perceive to be impacted by the emergency. In either case, acknowledging their needs and engaging them are essential to prevent the emergency from escalating into a company crisis.

The Emergency Management Team Leader (EMTL) is responsible to manage stakeholders, such as emergency response services, neighbours, staff and their families, local authorities, that may be impacted by the emergency and/or have bearing on the effectiveness of the emergency response efforts. The EMTL must assess what potential effects the emergency has on each of these stakeholders and what can be done to mitigate these.

In its strategic role, the Crisis Management Team (CMT) is responsible to manage a different set of stakeholders including regulators, the media and social media, politicians, shareholders, NGOs, and any other stakeholder group beyond the boundaries of the emergency response.

Both teams must learn how to manage their respective stakeholders groups during training, and practice stakeholder-mapping skills during exercises.

TYPICAL ORGANISATIONAL PITFALLS

- Stakeholders are missed or ignored.
- Stakeholder management is initiated too late or too slowly.
- The company is focused on managing the emergency alone.

Managing emergencies effectively depends greatly on the ability to engage external stakeholders early, to deploy internal and external resources optimally and to follow procedures as well as on ensuring teams are well-trained and practiced, and on conducting regular preparedness audits.

LEARNING FROM EMERGENCIES

When tasked with managing emergencies in your company, the following steps will need to be in place to ensure that you have deployed proven best practice:

1. Incident Reporting and Investigation
2. Learning from Third-party Incidents
3. Root Cause Analysis
4. After Action Reviews
5. Training and Exercises

1. Incident Reporting and Investigation

Each organisation must determine up front which types of incidents are reportable to the Authorities and/or Classification Society and what information must be provided. Typically, all accidents affecting members of the public, work related fatalities, major injuries, over seven-day lost time incidents, some occupational diseases, explosions, environmental spills and certain dangerous occurrences, are reportable. And requirements vary from country to country.

Companies do well by learning as much a possible from incidents happening in their own organisation as well as from incidents in the industry.

As soon as an emergency is under control, an investigation team with sufficient skills and sponsored by a company Director must be assigned to obtain the root cause of the incident.

Many companies have a policy in place stipulating that all incidents, violations and near misses must be investigated and have the associated procedures in place specifying how the investigation must be conducted and reported. An investigation must cover all aspects of an incident from its trigger point, contributing aspects and escalation events. It must identify the root cause(s) and provide recommendations to prevent and/or mitigate similar incidents from occurring in the future.

Recommendations must be SMART: **S**pecific, **M**easurable, **A**chievable, **R**ealistic and **T**ime-based. These recommendations may include improvements to policies, standards, procedures, training, hardware, engineering controls, personal protective equipment and/or training of employees and contractors. The investigation report must include all relevant information and a history of the events.

TYPICAL ORGANISATIONAL PITFALLS

- Insufficient skills and time are allocated to conduct a proper incident investigation.
- Time pressure to resume operations cause critical information to be lost.
- Recommendations are not tracked, executed nor completed.

2. Learning from Third-party Incidents

Highly effective organisations experience fewer and fewer incidents themselves and do well by learning from third-party incidents to identify further improvement areas.

Every day the news is riddled with events and triggers that can help assess an organisation's ability to respond to similar situations, e.g. floods, earthquakes, electrical outages, explosions, fires, etc. Some of those events are useful to trigger internal discussion with leadership teams, or within the HSSE (Health Safety Security and Environment function to assess the organisation's ability to respond should that event occur. These questions can be used to kick-off the discussion:

1. Could an event like this happen to us?
2. Where would it have the biggest impact?
3. Are we confident that we would be able to deal with it effectively?
4. Which aspects need verification/testing?

However, significant incidents in a similar industry must trigger a much more thorough response. Assign a team-leader to lead the investigation and collect as much details of the event as possible as if the incident had happened in your organisation. Implement the learning from this investigation.

TYPICAL ORGANISATIONAL PITFALLS

- External events are not used to check internal response capabilities.
- External incidents are not used to verify the organisations' controls and response capabilities.

3. Root Cause Analysis

A root-cause is a condition or trigger that leads to the undesirable outcome or generates an escalation of further cause and effects leading to the incident. Often an incident occurs when a number of aspects happen at the same time or in short succession creating a causal chain of events in which each one could have been avoided by a simple intervention.

Establishing the root-cause is therefore not always as easy as it seems.

A variety of techniques have been developed across different industry to help seek out the root cause as efficiently as possible.

The fastest method is asking "Why" at least five times to a cross disciplinary team of experts. The first question can be: "Why did this incident happen? Elements of the answer are then used to develop the next "Why" question until a good understanding of what root causes were at play is established.

Specialist facilitators are sometimes needed in the event of a very complex incident.

TYPICAL ORGANISATIONAL PITFALLS

- Investigators jump to conclusions and miss finding the root-cause and therefore fail to address the underlying issues.
- Investigators focus on one root cause and miss the complementary causes that lead to the incident or caused it to escalate.

4. After Action Review

Over and above conducting the incident investigation, a thorough review of the response to the incident from the initial alarm until stand-down must be undertaken with all response providers.

Often it is best to use the After Action Review (AAR) methodology to assess

the effectiveness of the incident response. As a minimum it must address the effectiveness of:

- Raising the alarm
- Assembling, Evacuating and Accounting for people
- Mobilising Emergency Response services
- Mitigating the risk of escalation
- Demobilising of Emergency Response services
- Clearing up the site
- Resuming normal activities

The AAR was developed and effectively deployed by the US army during the "Desert Storm" campaign in the Middle East and is now widely used across industries to assess/debrief and event, incident or other major occurrences.

In a typical AAR, the following guiding questions are used:

- What did we set out to do?
- What did we actually do?
- What could we have done better?
- What did we learn?
- Who are we going to tell?

TYPICAL ORGANISATIONAL PITFALLS

- Organisations revert to normal operations as quickly as possible and do not take the time to assess whether the response to the incident was timely and adequate, and whether corrective measures are required.

5. Training and Exercises

An organisation must have sufficient skills in-house or have access to those skills through contracts with service providers to cover the following aspects of Managing Emergencies:

- Floor wardens
- Assembly Checkers
- First Aiders
- Stretcher bearers
- Incident Commanders
- Emergency Response
- Next-of-kin Responders
- Incident Investigation Team Leader
- After Action Review Team Leader

Without refreshers and regular practice, skills erode over time. Therefore, for each skill, it is essential to define if refreshers are required and at which frequency. It is also critical to verify annually that sufficient people have been nominated for each skill to provide adequate cover.

Just having a quick fire drill every month, is not sufficient. Each organisation must develop a catalogue of scenarios that serves as the basis for practical exercises. Research shows that companies that practice their top scenarios every now and then are better prepared than those that do not. Develop an annual calendar of exercises that cover Health, Safety, Environmental and Security based scenarios. Combine this with a related theme of the month and provide sufficient material for discussions at safety meetings. This is a way to keep major risks top of mind for staff and contractors. Conduct at least one major exercise every year involving the mobilisation of Emergency Response resources. Check that all critical resources have had an opportunity to practice at least once every year.

Each exercise must be carefully prepared to ensure that all critical steps are covered. A trigger event must be selected to allow the exercise to begin with something tangible and follow on with additional injects that provide sufficient realism and pressure. Facilitate the exercise to ensure that the learning objectives are achieved.
Conduct a post exercise After-Action-Review to gather any learning and share these with the appropriate parties for follow-up and closeout.

TYPICAL ORGANISATIONAL PITFALLS

- Companies conduct quick drills every month without using the opportunity to practice a variety of relevant and specific scenario.
- Companies never practice the mobilisation of their Emergency Response resources.

Thomas Helmer *is Senior Director with CS&A International Risk, crisis and Business Continuity Management, a specialist firm working globally with multi-national clients across industry sectors. Prior to CS&A, Thomas had a long and distinguished career in the oil and gas industry with particular expertise in HSE and extensive experience as an emergency coordinator.*

References

- ***ISO 31000:2009,*** *Risk management – Principles and guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.*
- ***ISO 17776:2000,*** *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment.*
- ***ISO 22320:2011,*** *Societal security – Emergency management – Requirements for incident response, designed to minimise the impact of disasters, terrorist attacks and other major incidents it will help save lives, mitigate harm and damage and ensure continuity of basic services such as health, rescue services, water and food supplies, and electricity and fuel delivery.*
- ***BS 11200:2014*** *Crisis Management. Guidance and good practice. A capability to manage crises is one aspect of a more resilient organisation. Resilience requires effective crisis management, which needs to be understood, developed, applied and validated in the context of a range of risk related disciplines. These include risk, business continuity and security management.*

Do You Know Your Emergency Training Legal Obligations?

Source: http://www.hstoday.us/single-article/do-you-know-your-emergency-training-legal-obligations/551cb287935543bc35bd5edb03d4281d.html

"Way too many executives/administrators think that they're not required by law to train all employees for emergencies in their workplace. Wrong! Every employer in America is required by law to train all employees, without exception," cautions Bo Mitchell, a veteran certified emergency manager and president of 911 Consulting.
Wilton, Connecticut Police Commissioner for 16 years, Mitchell retired in February 2001 to found 911 Consulting which creates emergency, disaster recovery and business continuity plans, training and exercises for organizations like GE, Hyatt Hotels, MasterCard and universities.
As emergency planning takes on greater importance, and visibility, Mitchell has prepared a *10 Commandments of Workplace Emergency Training* report.
"While great emergency plans are a smart thing, training is everything," Mitchell stated in the short manual, warning that, "If we don't get the words off the paper and into employees' heads, we have failed operationally, morally and legally."

"Understanding the obligation of employers regarding training is critical," he said, noting that the 10 commandments of workplace emergency training he's outlined are "required by law for every employer in the US without exception for emergency action and fire prevention plans."

"To experts in workplace safety and security, the ten commandments of workplace emergency training are self-evident truths," Mitchell said, "But, these experts also recognize that most senior managers in corporations, campuses and medical facilities are ignorant of even their core management responsibilities for personnel safety in the workplace. In fact, many employers' inside and outside lawyers are ignorant of these responsibilities."

Consequently, he said, "Workplace and worker law is a specialty unknown to most. But, once through this door, the documentation regarding the 10 commandments is voluminous. This controlling documentation is manifested in federal, state and local statutes, regulations, codes and court decisions; plus administrative interpretations on part of authorities having jurisdiction—from your local fire marshal to Occupational Safety and Health Administration (OSHA) regulators in Washington, DC."

And OSHA isn't a town in Wisconsin, he said. "These regulations apply to corporations, campuses, medical facilities, non-profits, employers of any size or business model, federal agencies and, in most cases, state and local agencies. 29 CFR 1910.38 and 1910.39 cover Emergency Action Plans (EAP) and Fire Prevention Plans (FPP), both required by federal law of every employer without exception. EAPs and FPPs are required in addition to what the state and local codes may require."

10 Commandments of Emergency Training

The 10 Commandments of Emergency Training are the 10 fundamental rules of conducting emergency training that every organization needs to follow. What are they?

1. All U.S. employers without exception shall create and train Emergency Action and Fire Prevention Plans.
2. All U.S. employers shall create and train employees as their emergency team. Training shall be annual at least.
3. Training all other employees is required by law.
4. Training Shall Be Annual at Least.
5. Training shall be at hire on day-one including full-time, temporary and contract workers.
6. Training shall occur in a classroom by a "qualified" trainer—qualified by dint of experience and/or training. On-screen training shall not substitute for classroom training.
7. Training Shall Occur if the Plan Changes or If the People in the Plan Change.
8. Training shall be for all hazards.
9. All emergency planning and training shall be site specific. No plagiarizing. No landlord plan can substitute for tenant's responsibilities under law.
10. The CEO is the responsible party civilly, personally and criminally.

Dubai muscle car ambulances are not only smart but fast

Source: http://www.thenational.ae/uae/health/dubai-muscle-car-ambulances-are-not-only-smart-but-fast

You've seen the ever-expanding fleet of police supercars. Now, it seems ambulances are getting in on the act, with rescue vehicles that are sure to get to the scene at speed.

Smart ambulances loaded up with the latest healthcare technology are delivering life-saving treatment fast via a fleet of muscle cars and specially modified emergency vehicles in Dubai.

The fleet of cars, bikes and trucks were on display at Digital Health Live at Dubai World Trade Centre alongside the latest innovations in health care. A Dodge Challenger, Ford Mustang and Lotus Evora equipped with everything needed to offer first aid on the ground are the latest additions to the Dubai Ambulance Service. A Harley-Davidson motorcycle is also equipped with first-aid equipment to help fight through traffic to attend a crash scene.

Hareb Yenish is a fast-responding paramedic who drives one of the muscle cars for Dubai Ambulance Service.

"The idea is that the public will see them and be confident we are capable of arriving at the scene to help patients quickly."

"The cars have everything they need to treat patients at the scene before an ambulance arrives," he said.

Solar panels help power carbon fibre smart ambulances on the road, each with wide-ranging diagnostic equipment to pass on patient information quickly to waiting hospital doctors.

Other advancements in Dubai's fast-response unit include antibacterial non-slip flooring and more headroom inside the rear of ambulances big enough for two paramedics and a driver. A mobile unit is also able to be deployed to a crisis site to help manage large-scale casualties, with full X-ray and ultrasound facilities on board.

Off-road 4x4s that carry bicycles are also part of the fleet and are designed to treat patients in need of care in the desert, or rugged, hard-to-reach areas. Sara Al Haddad, a paramedic for four years, said constant training helped staff keep on top of the latest innovations to help save more lives.

"The medical buses can also be used as field hospitals, so we are well equipped to deal with any crisis situation that may arise," she said. "We don't take more than 15 minutes with patients."

Improved structure firefighting glove commercially available

Source: http://www.homelandsecuritynewswire.com/dr20150507-improved-structure-firefighting-glove-commercially-available

When responding to structural fires, firefighters wear protective gloves known as "structure gloves" to shield their hands from burns and other injuries. Because structure gloves can be bulky and limit dexterity, firefighters often need to remove the gloves to complete routine tasks, such as handling operating tools or using communications equipment. Without gloves, firefighters' hands are at a higher risk of injury.

In addition to dexterity issues, existing structure gloves can be difficult to put on when wet and offer limited heat protection. In the field, these gloves can be very impractical and slow response time.

The Department of Homeland Security Science and Technology Directorate (S&T) partnered with NanoSonic, Inc. and Shelby Glove to construct a new, improved structure glove that will provide the full range of protection firefighters need. This next-generation glove provides firefighters with enhanced dexterity, water repellency and fire resistance.

NanoSonic has developed a durable material called **HybridSil** —a Kevlar-based fabric that is both heat and water resistant. HybridSil can withstand punctures and lacerations that current structure gloves may not. S&T is working with NanoSonic to ensure the final glove meets all identified first responder requirements, standards and certifications.

The glove was tested against National Fire Protection Administration (NFPA) standards regarding safety and heat resistance in April 2014 and met all current requirements.

By improving the structure glove's technology and materials, S&T says it ensured firefighters can perform their duties while fully protected. The new material and design allows fire-fighters to make more precise movements without having to remove their gloves. The improved form and fit and water repellant-features ensure they provide the protection fire-fighters need.

The project underwent multiple stages of research and testing to ensure the durability of the selected materials in operational field conditions.

To make certain the glove truly met the needs of firefighters, S&T sent each prototype to be tested by fire departments across the nation. Testers used the glove in a series of exercises designed to replicate real life scenarios. Firefighters used the gloves as rigorously during testing as they would in the field. Each iteration featured improvements based on firefighters comments. The current version of the glove was assessed in spring 2014 and evaluated against five categories: ease of donning and doffing, proper fit, puncture resistance, dexterity and thermal protection and heat dissipation.

After gathering feedback from responders through several rounds of testing, the final specifications for the glove were captured. The finished product features three layers of HybridSil material.

The other day S&T announced that after two years of development, field testing, and subsequent improvements, the new improved structure glove has completed testing and received National Fire Protection Administration (NFPA) certification. **The glove is now commercially available for firefighters use from Shelby Specialty Glove.**

DHS Successfully Transitions Search and Rescue Tool That Pinpoints Buried Victims

Release Date: May 7, 2015

Source: http://www.dhs.gov/science-and-technology/news/2015/05/07/dhs-transitions-finder

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T), in partnership with the National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory, announced today the transition of the final prototype of the **Finding Individuals for Disaster and Emergency Response (FINDER)** technology to the commercial market. FINDER is a radar technology designed to detect heartbeats of victims trapped in wreckage. Two commercial partners have been licensed to manufacture the device: R4 Inc. of Eatontown, N.J. and SpecOps Group Inc. of Sarasota, Fla.

Earlier today, S&T and NASA demonstrated its newest capabilities at the Virginia Task Force One (VA-TF1) Training Facility in Lorton, Va., finding "survivors" in a simulated disaster. This is thanks to the new locator feature, which can help pinpoint the location of the victim to within about five feet – depending on the type of rubble. This key change saves rescuers time, increasing chances for locating survivors.

The technology proved successful during its first real-world operational use when it was deployed to Nepal following the April 25 earthquake to support international search and rescue efforts in the country. David Lewis, president of one of S&T's commercial partners, R4 Inc., arrived in Nepal with two prototype FINDER devices on April 29 to assist in the rescue efforts. He joined a contingent of international rescuers from China, the Netherlands, Belgium and members of the Nepali Army in Northern Nepal. Using FINDER, they were able to detect two heartbeats beneath each of two different collapsed structures, allowing the rescue workers to find and save the men. The four men had been trapped beneath the

rubble for days in the hard-hit village of Chautara.

"I stopped at every decimated village and used

FINDER there," Lewis explained of his actions in Nepal, crediting the Nepali people with providing invaluable support. "On two separate occasions, FINDER found two heartbeats. Family members were desperate to find trapped people. I am just happy we could be there with FINDER; I am very privileged to be part of the team and effort."

FINDER's human-finding abilities were demonstrated through multiple test searches over the past two years with urban search and rescue (US&R) teams in Virginia, Oklahoma, Indiana, New Jersey, Georgia, California, and Illinois.

"The latest operational assessments demonstrated FINDER was successful in locating a VATF-1 member buried in 30 feet of mixed concrete, rebar, and gravel rubble from a distance of over 30 feet," said John Price, S&T program manager for FINDER. "This capability will complement the current Urban Search and Rescue tools such as canines, listening devices, and video cameras to detect the presence of living victims in rubble."

"There is no one magic tool that can find everyone. We use FINDER as one of our tools: canines, Delsar listening devices, cameras," explained VATF-1Captain Randy Bittinger. "FINDER is the only tool that can identify an unconscious, unresponsive individual just by their heartbeat. We don't have any other tool like it. I want any tool that will help us find any people anywhere in the world."

In disaster scenarios, such as earthquakes and tornadoes, the wreckage is made up of twisted and shattered materials. Radar signals bounce back so signals are complex.

"Because the victim's hearts are beating, that signal changes a very small amount," said Jim Lux, JPL's FINDER task manager. "So what FINDER can do, is look for those very small changes, determine if they're from a human heartbeat and it they are, a message will display for the user indicating there is somebody in there."

S&T and R4 Inc. are also evaluating FINDER for additional search and rescue applications such as detecting people in burning buildings.

Operation RENAISSANCE 15-1 : CAF contribution to humanitarian relief efforts in Nepal

Source: http://www.forces.gc.ca/en/operations-abroad/nepal.page

As part of a Government of Canada response, the Canadian Armed Forces (CAF) are contributing personnel to an assessment team led by Foreign Affairs, Trade and Development (DFATD) to support Nepal following an earthquake that hit the country on 25 April 2015.

As part of a Government of Canada response, the Canadian Armed Forces (CAF) are contributing personnel to an assessment team led by Foreign Affairs, Trade and Development (DFATD) to support Nepal following an earthquake that hit the country on 25 April 2015.

Elements of the Disaster Assistance Response Team (DART) have deployed and continue to assess how Canada might best respond to the disaster.

Humanitarian Assistance Efforts

The DFATD-led Interdepartmental Strategic Support Team (ISST) is comprised of three experts from DFATD and three officers from the Department of National Defence (DND), including the DART Commander.

The Humanitarian Assessment Reconnaissance Team (HART) is working alongside the ISST with local government representatives and Non-Government Organizations (NGOs) to establish the immediate needs and integrate with ongoing relief efforts. The HART is also establishing a base of operations and prepared for the arrival of other deployed elements of the DART.

On 29 April, a CC-177 Globemaster III and its air crew arrived in Kathmandu carrying 31 CAF personnel and 11 additional aircrew personnel including:

- Members of HART;
- Engineers;
- Medical personnel; and
- One member of the Red Cross.

On 30 April, a second CC-177 Globemaster III arrived in Kathmandu carrying 51 elements of DART personnel including:

- Medical personnel;
- Civil-military cooperation personnel;
- Air movement specialists;
- Signalers; and
- Support personnel.

The CC-177 Globemaster III aircraft have also transported the following relief supplies:

- Water and rations;
- Engineering equipment;
- Communications equipment;
- Camp equipment;
- All-terrain vehicles;
- Ambulances;
- A cargo vehicle;
- Forklifts;
- Self-sustainment equipment; and
- Red Cross humanitarian air equipment.

Mission context

On 25 April 2015, a 7.8 magnitude earthquake hit Nepal's capital, Kathmandu, causing significant damages. A major aftershock struck Nepal and India on 26 April and triggered more avalanches in the Himalayan Mountains.

The earthquake caused significant loss of life, a large number of injuries, as well as destruction of property, leaving thousands of people requiring humanitarian support.

- 26 April 2015 – the Government of Canada announced five million dollars in humanitarian assistance funding and prepared to deploy elements of the DART.
- 26 April 2015 – the first C-177 Globemaster III transporting elements of the DART and relief supplies departed from Trenton
- 28 April - the DFATD-led ISST arrived in Kathmandu.
- 28 April - a second C-177 Globemaster III transporting 51 CAF personnel deployed from 8 Wing in Trenton.
- 29 April 2015 – the first elements of the DART and relief supplies arrived in Kathmandu.
- 30 April 2015 – the first elements of the DART conducted a reconnaissance in the vicinity of Bidur, north of Kathmandu.
- 30 April 2015 – the second CC-177 Globemaster III transporting other elements of the DART arrived in Kathmandu.

- 1 May 2015 – the second CC-177 Globemaster III transported 18 passengers from Canada and other nations to New Delhi, in support of the DFATD-led evacuation efforts.
- On 2 May, 2015, the Government of Canada announced a phased deployment of the DART into Nepal. This approach will allow the CAF to adjust the capabilities and composition of the DART based on needs on the ground.
- On 4 May, DART established the Forward Operating Base (FOB) in SUMITRA, Nepal.

Contingency Plan RENAISSANCE

Contingency Plan (CONPLAN) RENAISSANCE is the Canadian Armed Forces' plan for rapid deployment to the scene of a disaster overseas, as directed by the Government of Canada. It provides direction to the CAF in the event of a decision by the Government of Canada to respond to a request from another nation for help.

The plan delivers a rapid CAF response that is flexible enough to make an immediate positive impact at the scene of the disaster, and to continue helping people as the situation develops.

The Government of Canada's response to natural disasters abroad is coordinated by DFATD in close partnership with core departments and agencies, including the Department of National Defence and the Privy Council Office (PCO).

Interdepartmental Strategic Support Team

The role of the ISST is to meet with local and international representatives to assess the needs on the ground and to identify potential follow-on response options to the Government of Canada.

Disaster Assistance Response Team

The Disaster Assistance Response Team (DART) is a military organization ready to deploy quickly to conduct emergency relief operations. It is one component of Canada's toolkit to respond to natural disasters abroad.

Before the DART is fully deployed, an advance party is sent to prepare for the arrival of the main body and DART capabilities which could deploy at a later date.

The DART is a self-sufficient, scalable military capability ready to deploy quickly to conduct emergency relief operations for up to 40 days.

Its main elements include the DART headquarters, a logistics platoon, an engineer troop, a medical platoon and a defence and security platoon. DART equipment, stores, and supplies are stored at 8 Wing Trenton and are maintained for immediate deployment by a small supporting staff.

The DART is not designed to provide first response services, such as search and rescue or emergency trauma care. Instead, it can be useful where the capabilities of local governments and humanitarian agencies to provide primary health care and potable water are overstretched.

The DART serves three critical needs in emergencies:

- water purification;
- primary medical care; and
- engineering help.

Elements of the Disaster Assistance Response Team (DART) have deployed and continue to assess how Canada might best respond to the disaster.

Latest News

As of May 8, 2015, approximately 135 members of the Canadian Armed Forces are deployed in Nepal.

Located in Kathmandu, the geomatics team continues to produce maps which are an essential tool in the conduct of relief operations.

Based on assessments conducted in recent days, the Charikot region has been identified as the area of focus for DART resources and capabilities. Elements of the DART have since established the Forward Operating Base (FOB) in SUMITRA along the Friendship Highway, which includes a medical capability. From there, coordination and liaison elements are being pushed forward from the camp into the Charikot region to assist and enable local initiatives and facilitate the operation of Non-Government Organizations (NGOs) in the

region. In the vicinity of Camp SUMITRA, DART medical staff is treating villagers, while the Engineering team is providing road clearance support along the Friendship Highway.

EDITOR'S COMMENT: Perhaps the unfortunate event in Nepal is an indicator that the disaster response is a military operation and plans whould be changed – worldwide. State response might be sufficient for small/medium scale disasters but not for catastrophic incidents in large scale. The military has the structure, modus operandi and means to successfully undertake the mission. Of course now there is close cooperation between these two entities but stll the military works under the civilian umbrella and this is not enough for a fast and successful outcome.

The Game of Drones

By Dr. Alexandros E. Soulahakis

Source: Original article

Drones, Unmanned Aerial Vehicles (UAV) & Unmanned Aircraft Systems (UAS) nowadays are becoming very popular. They offer a number of advantages while they introduce new capabilities to all industries. It is a fact that drones are being used for pleasure, [1], [2], filming HD scenes, transferring packages, but they can also be used for sending medical devices, monitoring gas pipes, surveying oil platforms or other scenarios

While the Sendai Framework was agreed at the third world conference on Disaster Risk Reduction 14-18 March 2015 (Sendai), Miyagi, Japan [3], more cities are adopting the new ISO 37120. The later aims to measure the performance of city services and quality of life using 100 indicators. Today UNISDR is promoting the most exiting campaign ever about urban resiliency [4].

At the same time random disasters continue to occur globally as its unpredictable characteristics cannot be easily forecasted. Many lives were lost during recent disasters but also many people survived. During a hazardous event, the first hours after the beginning of the incident are the most important for rescuing lives. The possibility of saving victims alive in most cases is decreasing as time passes. This is why it is important to empower the first responders with the "know-how" of the new standard and also give them new intuitive technology to help them on the field at the time of the incident. ***So what if the first responders could be transformed to superheroes, so they could use their "super vision", to observe the surrounding environment?*** Have you ever watched a movie in which a "familiar" bird/eagle/crow flies away and transfer its vision to its master? "Yes but this is supernatural and you are talking about a movie Alex". Well maybe not. Not all superheroes have superpowers. Batman for example uses no superpowers. He does all the tricks by using high tech gadgets, critical mind and his human powers. So my point is that we can transform responders (from heroes) to superheroes by using the technology on their favour. We can help responders to get the full picture of a disaster, react faster and implement DRR to their routings through the current technology.

The safety of resilient cities and their immediate responders in the distant future will be depended on sensors, wearables and drones. It is a fact that we, humans understand our world mostly through vision. We visualize and react. So how can we use our flying tech to serve sustainability, resilience, DRR and help responders?

- **A drone can fly**

  The greatest advantage of a drone is that it can fly above any location and stream the video of the suffering area. This is an awesome characteristic, which helps people judge/visualize what the magnitude of the hazard is and how much force will be needed to ensure fast recovery. Additionally promoting awareness will motivate civilians to use their drones to volunteer for DRR.

- **A drone can respond faster**
  It is obvious that a drone can travel faster than a running human. That means it can cover an area a lot faster than humans and pinpoint possible issues.
- **A drone cannot die**
  We would never let a human to scout into the source of danger if we knew that there is a chance of death. What about sending a drone in there. Worst-case scenario is to loose a few thousand dollars, not a human life.
- **A drone can fit**
  In many cases a helicopter cannot fly through the city buildings and obstacles as this raises many different risks. Very often we are in the need of observing what is happening inside a structure and the only way to get there is to go through holes. A drone has the perfect size to do the dirty work without risking a responder's or a trained dog's life. Moreover using that method we free up one more unit to help in other tasks.
- **A drone is fearless**
  Will fly high, low, inside, through fire, in radiated areas, without any hesitation. Fear is literally not an option for drones.
- **A drone can fly alone**
  Recent technological achievement introduces autonomous drone technology that can survey areas without the pilot's real time interaction. Responder can set the waypoints through software and the drone will fly following the flight path. The best part of it is that the drone will come back to base to get recharged and can fly again when it is ready.
- **A drone can "give sight beyond sight"**
  During my studies in UK, I have seen robots that "watch" laser welding and measure the quality of the welding in real-time. A different DSP project involved Artificial Intelligence to monitor the live HD camera feed and recognise objects, (human, barrel, car or other). Police uses this technology on helicopters to follow people during a night incident. So why not use it on the drones? We will be able to see from above in low light conditions. Autonomous drones can use their DSP to focus camera on fire and automatically hover or park in a place, from which it will transmit live feed of the incident.
- **A drone has feelings**
  Not really, but it can sense. We can install sensors for temperature, GPS-location, humidity, radiation, movement, sound detectors, beacons, sonars and many more. This could give valuable measurements and also detect humans are in danger within a hazardous area or fire starting. NASA today can detect a human's heartbeat using the Finding Individuals for Disaster and Emergency Response (FINDER) [5] (read also article in p.73). Maybe it is time to release a "dron-e-fied" version of it.
- **A drone can broadcast**
  During massive disasters drones could be placed in strategic position to form an ad-hoc WI-FI network for supporting interconnections between places suffering an outage. Furthermore they could be deployed on demand to support other public events.
- **The "drone" runner**
  Major energy companies nowadays use UAV's commercially (FAA has granted permission to BP) to improve their operations on the field while they manage to improve the safety risk in a cost effective way. They fly it into a 40x60 mile area, using a battery, which lasts for two hours supporting their everyday operations [6].
- **A Drone goes to Hollywood**
  It is a fact that 4k slow motion videos are impressive. High frame rate cameras could also give clues or visual evidence of expositions, and help us understand the causes of a disaster.
- **Drones can carry things**
  Commercially usage of a drone can deliver a package. It can also carry medical equipment like defibrillator [7], medicines [8] while flying at 60 miles per hour (100km/hr).
- **Drones offer mobility**
  They can be easily transferred everywhere. Their size is the key, as they are small and effective. Most of them can be easily controlled as they have mechanisms, which allows automatic hovering and friendly navigation controls. It may be a good idea that

drones could become standard equipment, for all responding vehicles in the distant future.

- **Drones are hungry.**
  The scenarios mentioned above are existing technologies and can be further expanded by minimizing the tech components in such way they can be installed on a drone. Current research for new battery technologies and solar panels can "feed" "hungry" electrical/electronic components. New batteries offer greater capacities, which mean longer flights.

Concluding this article, we may all agree that drones will benefit DRR and empower the responders. It is possible to further minimize the response time and help responders get prepared, even while they get transferred inside the dangerous zone. Imagine the possibilities of connecting autonomous drones with wearables to an incident management system and monitor our megacities. This is a great change to promote preparedness and let technology increase city resilience and empowers the responders.

References

1. http://www.theguardian.com/technology/2015/may/04/unmanned-aerial-vehicles-giving-drones-a-good-name
2. http://www.dronestagr.am
3. http://www.wcdrr.org/preparatory/post2015
4. http://www.unisdr.org/campaign/resilientcities/
5. http://news.nationalgeographic.com/2015/05/150507-nasa-finder-nepal-earthquake-survivors-rescue-technology/?utm_source=Facebook&utm_medium=Social&utm_content=link_fb20150507news-quakesurvivorheartbeats&utm_campaign=Content&sf9042777=1
6. https://www.youtube.com/watch?v=05t-dg6nFpE
7. http://www.dailymail.co.uk/sciencetech/article-2811851/The-ambulance-drone-save-life-Flying-defibrillator-reach-speeds-60mph.html#v-3864289608001
8. http://www.dailymail.co.uk/sciencetech/article-2768128/Send-DRONE-doctors-Parcelcopter-fly-medicine-urgent-goods-remote-German-island.html

Dr. Alexandros E. Soulahakis is *Associate Consultant at Resilience Guard GmbH (Zurich, Switzerland). He is a self-driven engineer with strong technical background and hands-on ability to work in fast paced environments, such as maritime and hospitality industries. Deep understanding of telecommunication systems, computer science and electrical/electronic engineering that allows innovative resolution of highly complex problem; ability to design and oversee the installation of telecommunications equipment and facilities, complex PBX scalable systems & VPN secure VoIP networks; experience with IT administration in real or simulated environments (storage, antivirus solutions, IDS/IPS).*

Homeland Security Committee Considers Turning Nation's Cellphones into Walkie-Talkies During Emergencies

Source: http://www.nextgov.com/emerging-tech/2015/05/homeland-security-committee-considers-turning-nations-cellphones-walkie-talkies-during-emergencies/112105/

Let's say it's 2016 and the government has a message to get out to the public -- ISIS is believed to be waging an attack on cellphone towers in the United States. How can the feds communicate that to a population of cord cutters when the towers are down?

That hypothetical scenario is one of the problems the government and tele-communications providers are grappling with, as they strategize how to maintain the integrity of emergency communications in an increasingly wireless world.

There are some solutions being floated around the Defense Department by the President's National Security Telecommunications Advisory Committee, a panel that compiles recommendations on critical national security and emergency preparedness issues.

"We need to think about in the digital environment how do we recreate the old national emergency broadcast and ask could we use cellphones, for example, differently?" Defense Chief Information Officer Terry

Halvorsen said at a committee meeting on Wednesday.

That smartphone may not be as inert as most would expect when towers go kaput.

"At the base level, electronics that people have in their pockets are radio transceivers and they can not only talk to cell towers, they can talk to each other," Bud Tribble, Apple vice president of software technology, told Halvorsen.

"Should we mesh these together" if towers are unavailable "to propagate a broadcast signal to replace the old civil defense broadcast?" Tribble posited, referring to a Cold War-era arrangement for discreetly repeating messages from one radio station to another across the country.

"It would be unimaginable 50 years ago to talk about a situation where every citizen has a UHF transceiver in their pocket, but that's what we have today and we should think out of the box in how to leverage that in emergency situations," he said.

The advisory council has long warned the government about the difficulty of pushing out Wi-Fi and broadband communications to the masses during disasters.

"A router placed at the edge of the network to connect various types of residential, cellular, satellite or enterprise clients to the core network may experience congestion at peak traffic times or during network events," panel members wrote in a 2008 report on National Security and Emergency Preparedness Internet Protocol-Based Traffic.

A federal government colleague of Halvorsen's from the Department of Homeland Security pointed out one hiccup with harnessing the distributed-cellular power of crowds to get out a message.

"In a world where everybody can broadcast, the ability to spoof, or fake, a government broadcast is obviously increased," said Andy Ozment, assistant secretary of the DHS Office of Cybersecurity and Communications.

Whereas now, "the likelihood that somebody will fake a government broadcast that overrides all the TV channels in the nation is relatively low; the likelihood that somebody will fake a government broadcast that appears on one stream of some commercial service is not as low at all," Ozment cautioned.

There have, in fact, been instances of hackers interrupting regular programming to issue false warnings.

In 2013, a Montana TV station broadcast was disrupted by news of a zombie apocalypse, *The Associated Press* reported at the time. Unauthorized users broke into the Emergency Alert System of KRTV and its CW channel. According to the *New York Daily News*, a computerized voice advised: the "bodies of the dead are rising from their graves. Follow the messages on screen that will be updated as information becomes available. Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous."

The government should make it harder for pranksters or terrorists to log into emergency communications systems, Tribble acknowledged.

"You don't want some teenager thinking -- 'Oh, this is Super Twitter,'" he said. "It comes down to who has the keys that authorize such a transmission so that kind of design has to be thought about up front to make sure that this is a secure mechanism. "

5 Elements of Proactive Situational Awareness

By Jim Bailey

Source: http://www.emergencymgmt.com/training/5-Elements-Proactive-Situational-Awareness.html

An old sports tenet says that you can't tell the players without a scorecard. It is equally true that you can't play the game without a playbook. Yet most emergency operations centers are doing just that.

EOCs all share one basic currency — information. At its core, an EOC is an information processing and dissemination mechanism that supports and

coordinates operations in the field. So how information is analyzed, processed and acted upon often means the difference between life and death. But there is a systemic problem.

All too often, emergency operations plans and EOC standard operating procedures state that the operations center will establish and maintain situational awareness and disseminate a common operating picture. Unfortunately no one ever tells you how to do that. Why does that matter? Because every single decision EOC responders make depends on accurate, complete and current situational awareness and a common operating picture, otherwise known as SA/COP. But several issues complicate the problem.

First, most hard-working, well meaning EOC responders work in the operations center part time. Most staff members only work in the EOC during activations which, depending on the jurisdiction, occur infrequently. Moreover, EOC staff often must skip training, as it competes directly with their day jobs. Add to that the perishability of the training, natural EOC staff turnover, no national EOC position credentialing program, and the tendency of emergency managers to rely on technology to solve their information management issues, and you have the recipe for anything but collaborative, effective operation. For all of these reasons, teaching practical SA/COP development is mission critical.

How to do that? President Dwight Eisenhower said, "Plans are useless, but planning is indispensable." Plan. Start by identifying your decision points for the top three threats your jurisdiction is at risk of facing. Know before an event where your decision points are and what information is needed to make those decisions.

It's no surprise that during an event, information pours into an EOC from every direction. If information requirements haven't been properly identified beforehand, collecting and assimilating all incoming data can be like trying to drink from a fire hose. Critical information can be missed, and less important information can take prominence. These are reasons why EOCs need to plan.

There are five elements at the crux of proactive SA/COP:

- Define your information requirements.
- Determine how to gather information.
- Decide who will analyze that information.
- Determine how that information will be shared.
- Choose the technology that will help communicate and manage the information.

It's that simple and that profound. And very few EOCs currently do this, let alone do it well. In sports, you can't tell the players without a scorecard. But in emergency management, when lives are on the line, you can't play the game well without proper training and an effective SA/COP system.

*Willdan Homeland Solutions president and CEO **James Bailey** is a retired Marine Corps intelligence officer with 13 years of emergency management planning, training and exercise consulting experience. Bailey created an SA/COP training course with Red Team Intelligence president and CEO Chris Bausch, also a retired Marine Corps intelligence officer with 13 years of emergency management planning, training and exercise consulting experience.*

Beyond the Chaos: 3 Stories of Those Under the Gun During Major Crises

By Jim McKay

Source: http://www.emergencymgmt.com/disaster/Beyond-the-Chaos-3-Stories-Major-Crises.html

The results of unexpected catastrophes — like the West, Texas, fertilizer plant explosion, the Oso, Wash., mudslide and the Oregon mall shooting — often yield a chaotic response effort but offer lessons learned.

In this feature, we look at three separate disasters through the lens of someone in command. All three of these emergencies were incredibly tragic and difficult or impossible to predict. Besides the tragedy, these emergency managers share lessons learned, some of which we discuss here.

Frank Patterson was one of the first responders on the scene of the West, Texas, fertilizer plant explosion and took command. He details how he navigated the chaos that night and what was learned.

We talked to John Pennington, director of the Snohomish County, Wash., Department of Emergency Management, whose eyes were forced to believe what he was seeing, and whose decisions helped guide the response and recovery efforts after a horrific mudslide.
Mark Spross directs the 911 center in Clackamas County, Ore. When a gunman opened fire in a local mall, it tied the county in knots. Much has changed — and improved — because of that day.

'You Need to Take Command'

Frank Patterson recalls the aftermath from the West, Texas, explosion.

The radio call on April 17, 2013, said "bombs going off, we need all the ambulances you've got."
Frank Patterson, Waco-McLennan County emergency management coordinator, was on his way, but he was thinking it was a propane tank explosion.
When Patterson arrived on scene, he learned of the fire at the West, Texas, fertilizer plant and ensuing explosion and that people were dead. He asked about a command post. The response was, "You need to take command."

Nearby there was a football field and a dirt field. Neighbors were already triaging victims in the dirt field. "It wasn't until I got into the neighborhood that I realized how bad it was," Patterson said. "People were coming at us injured, disheveled, some in wheelchairs, in the back of pickups."
He surveyed the area and saw doors blown off houses, windows blown out, collapsed houses. Debris was everywhere.
A call for mutual aid had already gone out and people were on the way. Patterson began setting up a command post at the dirt field. He asked a fire chief to take care of hazmat issues. He named a staging officer, a law enforcement person and a search and rescue person.
This emergency was a unique, no-notice event. There was no background on the situation, no warning. "None of us in command that night had any knowledge other than the plant was on fire," Patterson said. "We are recreating the incident command structure based on what's in front of us."
The call about a fire at the plant had gone out at 7:29 p.m., and fire personnel arrived at about 7:39. The place exploded at 7:51. "In that 12 minutes, they had to make a lot of decisions, like whether to evacuate. That's not a lot of time," said Patterson.
During that time, there was an ammonium nitrate explosion that killed 15 people, including 11 firefighters, and injured more than 200. It also damaged or destroyed more than 150 buildings.
Patterson called it a CNN event — a flood of people from every direction to add to an already-chaotic scene. "The first thing we had was people flooding in from every open road," he said. "Shutting down traffic became a priority, and it took 45 minutes to an hour to get our arms around that whole process."
The challenge of the spontaneous responders, combined with inherent interoperability issues, made the situation overwhelming. "We had to patch people together. Some people had 800-megahertz systems, others VHF or UHF within our own county. So we're patching and trying to convey that information, saying, 'Hey, this is the frequency we're going to operate on.'"
Over the years, the county has developed a system to patch all of that together. Patterson carries in his trunk a decade-old ACU-T Tactical Interconnect System. It's become routine to patch in disparate systems, and they've developed templates for each system. The patching became second nature for locals. "The issue here was, who was already on the scene, what were they operating off of and how do you talk to them if you don't know where they are?" Patterson said. "There were 30 channels."
The spontaneous responders kept coming and so did the wounded. Patterson had to stop the flow of responders and focus on the triaging process. He requested that the staging officer stop the traffic. "Just park

them somewhere," he said. "I just wanted them out of the way."
Twice he called for resources to stop coming. Making decisions in the command post became chaotic with the presence of all the responders who wanted to help or to know something was being done.
"We made a lot of good decisions early on when nobody knew where the command post was because we were able to create the objectives, establish some strategies and start lining up people for the tactics," Patterson recalled. "Once people realized where the decisions were being made, everybody wanted to be there."
He realized that the command post had to be isolated, and if it's not isolated, it needs to be controlled so that people can't just walk up it to or through it. "We were trying to work on strategies, objectives — and people would just walk up and say, 'Here I am.' You'd have to stop, deal with that, then get back to business. Later we realized we should have had law enforcement barricade us in there, put tape around us or something to keep people from wandering in."
Patterson finally requested a command trailer from which he would do briefings periodically, essentially yelling at the crowd. And that's how it went for the rest of the night until all 262 patients had been transported.
"Until then I couldn't even look up; the numbers were overwhelming," he said. "That was the toughest thing. They just didn't stop."
The injured were transported in ambulances, helicopters, even buses.
Another lesson learned.
"We plan ways of notifying hospitals with the expectation that it's all going to come from the hospital, but they're going to present in different ways and that might be the first notice you get. An [injured] person might show up in an SUV."
Social media was a problem and a lesson.
"We didn't use social media. It ate us up," Patterson said. "My wife, the next day, told me that if you're not paying attention to social media, you need to. You need to get control of it."
Information began circulating on social media about the number of dead and so forth. Reports were spreading of 60 to 70 dead and that plumes were moving toward Fort Worth 100 miles to the north. None of it was true.
Patterson said it's vital for rural communities to have a public information officer on scene who is the face of the incident. In this case, the local mayor is also the PIO and a volunteer fireman. Command staff played musical chairs being the PIO.
It's also important after the incident to have a PR person who becomes the voice of the command staff to blunt the criticism that will come.

Information Overload

Mark Spross, communications manager for Clackamas County 911 in Oregon City, Ore., said his 911 center changed the day of Dec. 11, 2012.

At about 3:30 that afternoon, his dispatch center lit up as calls poured in about an active shooter at the Town Center mall near Macy's.

The good news is that the sheriff's department is located less than two blocks away and was on the scene quickly. Unfortunately it was too late for two mall shoppers. Cindy Ann Yuille, a 54-year-old nurse, died as fellow shoppers tended to her wounds. Forty-five-year-old Steven Forsyth died at the scene as well. Fifteen-year-old Kristina Shevchenko was lucky that she survived the impacts of the killer's Bushmaster M4 Carbine rifle.
The word of an active shooter spread on social media and through other sources, and the call center was quickly overwhelmed. All 11 lines into the center were inundated.
The protocol in the center is to answer: "911, what's the location of your emergency?" and then go into specific questions. But every call was reporting an active shooter at the mall. It became impractical to

follow procedure amid such a furious onslaught, so dispatchers set the book aside and answered, "911, are you calling about the mall shooting?"

"There comes a point where you're so overwhelmed by incoming calls that you need to process them in and out as quickly as possible," Spross said.

Furthermore, every off-duty police officer in the area wanted to respond. Many of them called an already-overwhelmed 911 center. "We told them to follow your procedures and we disconnected," Spross said. "It turned out a lot of the departments didn't have procedures prior to this on what to do and they needed people to come in."

The shooting lasted just 22 minutes before the shooter turned the gun on himself, but everyone in the county — it seemed — got on their phone, knocking out service for hours. There were roughly 10,000 people in the mall that day, and as one officer put it as he arrived on scene, they were "on foot and bailing out like crazy."

Police and fire soon set up incident command posts, and the chaos continued well after the shooter was dead, mostly as a result of miscommunication or a total lack of communication.

Among the calls to the dispatch center were those from inside the shopping center, where employees had followed mall policy and pulled every nearby shopper into a store, closed the gate, hid and called 911. "Everything [mall employees] did saved lives that day," Spross said. "However, we didn't know that was their procedure, and knowing that would have been helpful so we could have said, 'As long as you're safe, don't call 911.' We want that information but maybe 10 minutes after the incident starts."

The EOC acted quickly and rerouted traffic, without the knowledge of 911 dispatch. It didn't occur to dispatch that it could be done so fast, Spross said. "If we'd have known, we would have requested it right away to make it easier for field responders to make traffic flow easier around there."

Spross praised police and fire for setting up the command posts quickly, but they too struggled with communication. The fire department was getting reports of additional injured patients. And the police officers, not realizing that their frequencies were in fact the source of the fire department's reports, were doubling back trying to find the additional injured people. "They recognize that they need to talk to each other faster and sooner, and have a joint command center," Spross said.

That day set in motion policy changes on several fronts.

"One thing we learned is that we really don't practice on a regular basis these high-stress events," he acknowledged. "We don't take it to the training room. Since then, we have done that. And staff understands they have a little more ability to work outside of the day-to-day structure."

They've also worked with mall management to incorporate the 911 center into mall training and policy. And the mall and sheriff's department have collaborated on communicating better, with the mall offering to pay for additional training for the department.

Another lesson according to Spross: "We learned we have to take better care of our staff in terms of mental health."

'We've Had a Mudslide'

John Pennington, director of the Snohomish County, Wash., Department of Emergency Management, remembers getting out of the shower at about 10:45 a.m. that day and seeing the light blinking on his BlackBerry. He remembers the uncertainty in the caller's voice.

"We've had a mudslide. Kind of scattered reports, but I think there's a house that's impacted or been pushed near the highway. I don't have a good feeling about this."

Early reports from the scene of the slide began to trickle in as first responders arrived. Then came reports of screams for help. There was no situational awareness for those on the scene, and conclusions from initial reports suggested a mudslide of 300 or 400 yards. The enormity of the incident started to take shape as air assets began plucking people out of the muck.

In February and March 2014, an unusual amount of rain had pelted Snohomish County. On March 22, a hill near the communities of Hazel and Oso gave way, pouring mud across the Stillaguamish River, suffocating an area of about a square mile and taking 43 lives with it.

"When I first got my eyes on the slide from a Black Hawk, I was mentally prepared because I had seen still photos and some video, but I was really focused on the

dominoes downstream," Pennington said.

Throughout that day and into the night, with no real situational awareness, it was difficult to measure the depth of the catastrophe, Pennington remembers. "There wasn't really a strong ability for situational awareness. Because of the air assets, we would get a good visual that would be downloaded into our EOC, but we weren't able to access any of that because we didn't want to interfere with the fact that they were plucking people off the dirt.

What we saw were spot checks of dirt."

Looking back now, Pennington said if he had it to do again, he'd deploy additional air assets from either the state patrol or the federal government to get more video.

There are always lessons after the fact.

More reports began to trickle in about people yelling for help and the smell of natural gas and the depth of the mud mixed with power lines and jagged metal. The muck was everywhere, and it had collected ingredients that were harmful to search and rescue. The stuff was the consistency of pudding, The Seattle Times wrote later.

Pennington was uncertain if the debris would hold or break free and head down the river. "You're talking 75 feet of mounds and water debris." He evacuated the area downstream via the Emergency Alert System and upstream methodically with voice to text.

"The tactical commanders on the ground and I were talking a lot," Pennington said. "It became problematic in that the debris was liquefied so much that any attempts to get on the pile were almost impossible and dangerous to the point where calls had to be made repeatedly to pull people back because of movement or just the complete uncertainty of what was happening."

The search went on for days. More than a dozen people were pulled alive from the muck by the many who put their lives on hold to help. Nine days after the slide, just 24 bodies, or parts of bodies, had been found. The mud was so treacherous that searchers had to tape themselves into raincoats and pants to keep it out. The search continued for weeks.

Volunteers and agencies had flocked to the area wanting to help.

"My experience [with] the federal government and the state prior to that really helped me to understand that large-scale incidents, especially localized, had the highest potential for mission creep and federal takeover," he said. "I knew what I was going to do."

Pennington knew he had to "own" the incident. He made it clear with FEMA, for whom he had managed a Type II Incident Management Team (IMT), that everyone would work within the local system they had built and were building on the fly. "They were respectful of that."

Pennington said the system in place worked because it was flexible, acting as more of a framework than a prescription. He was in the EOC for just three of the 37 days of the ordeal. The same went for his deputies and senior leadership.

"What we defaulted to was a system of emergency management in our EOC that would operate in times of crisis where we weren't here, and that worked beautifully. But we had to inject ourselves into some tactical decisions knowing they impacted the larger strategy."

It was a balance of tactical and strategic solutions that he hadn't favored philosophically but was forced to practice in this event. A framework versus something too prescriptive allows for bending when the unexpected happens.

"We had this wonderful debris management plan that was recognized nationally and had been exercised, but what we had not accounted for in the plan was human remains," said Pennington.

Another potential lesson involves the interface between the IMTs and the EOC. "What happens in an event like this one when you had huge IMT presence, but their

reporting wasn't to a county commission or council; instead they had to report to an aggressive, authoritative emergency operation center and emergency management function. Neither was prepared to work with the other," Pennington said.
In the end, he said they made it work but that Oso is a microcosm of what a localized catastrophic incident will look like and will include the potential for EOC/IMT functionality. It will require looking more deeply at reporting requirements and integration between the two.
And lastly he remembered the 200 or so crisis managers on scene helping out. The message? "None of us are immune to human emotion."

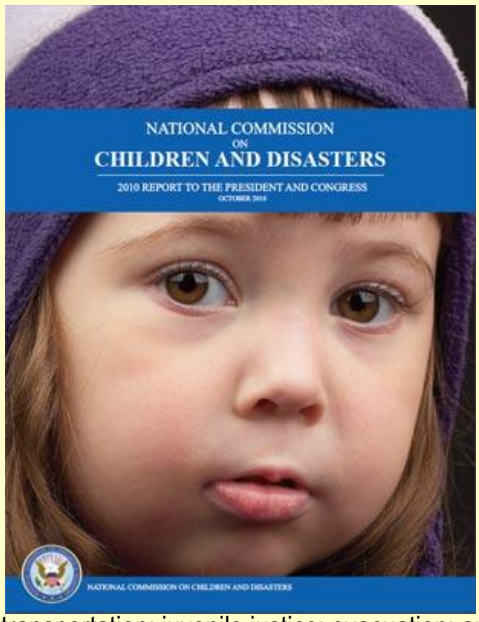
***Jim McKay** is the editor of* Emergency Management.

National Commission on Children and Disasters

2010 Report to the President and Congress

Source:http://cybercemetery.unt.edu/archive/nccd/20110426214356/http://www.acf.hhs.gov/ohsepr/nccdreport/index.html

The National Commission on Children and Disasters is an independent, bipartisan body established by Congress and the President to identify gaps in the Nation's disaster preparedness, response, and recovery for children and make recommendations to close the gaps. The commission was established under the Kids in Disasters Wellbeing, Safety, and Health Act of 2007.



In its October 2009 Interim Report, the Commission found serious deficiencies in the state of emergency preparedness for children. The 2010 Report to the President and Congress builds on the findings and recommendations in that Report.
The Commission examined and assessed the needs of children in relation to the preparation for, response to, and recovery from all hazards, including major disasters and emergencies. The Commission reports findings and recommendations relating to: child physical health, mental health, and trauma; child care in all settings; child welfare; elementary and secondary education; sheltering, temporary housing, and affordable housing; transportation; juvenile justice; evacuation; and relevant activities in emergency management.

▶ **You can access this very important report from source's URL.**

New Preparedness Game Targets Special Needs Children

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

As we approach the 10th anniversary of Hurricane Katrina, little progress has been made in preparing communities for better outcomes in disasters.
The 1,836 deaths in Katrina exposed an alarming lack of engagement by a large number of citizens on preparedness. Of those who perished in the tragic disaster, 22 percent were physically unable to evacuate, 14 percent

were physically disabled, 23 percent stayed in New Orleans to care for a physically disabled person, and 25 percent were suffering from a chronic disease. Despite the dangers of our reality, we are constantly witnessing an unacceptable lack of awareness when it comes to preparing our most valuable and vulnerable members of our society – our children and special needs citizens.

PrepBiz™ Gamification App Solution

PrepBiz™ 1.0 gamification app educates children, youth, adults and visually impaired individuals on best practice recommendation responses to disasters, hazards and active shooter incidents. Players must overcome challenges by choosing the safest course of action to avoid obstacles, hurdles and mishaps to reach safe points with pop up boxes alerting to common hazards and other information related to the incidents while remaining safe. PrepBiz™ 1.0 (VI) is an audio-only action/adventure game for mobile phones, tablets and computers where ears replace eyes thanks to a very innovative technology: binaural sound and players are guided only by 3D sound and live the adventure by controlling their Avatar with multi-point tactile gestures.

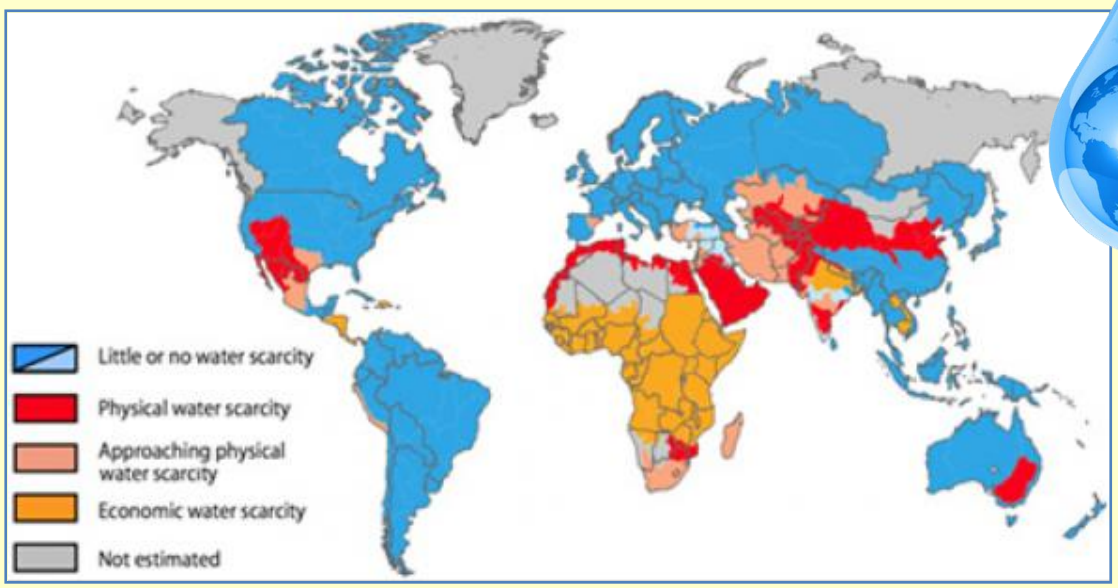
PrepWorld LLC, (www.prepworld.org) the parent company and designers of the PrepBiz™ gamification system and Project Starfish (www.pstarfish.org) have taken the challenge to explore not only if games could be effective in emergency preparedness, but how and why.

We feel videogames can be a great strategic partner to emergency preparedness and as such deserves fundamental investment of time, capital and attention from key stakeholders in both the public and private sector. The field needs more funding and research activities to grow this budding field.

The Middle East Runs out of Water

By Daniel Pipes

Source: http://www.meforum.org/5227/middle-east-no-water



A ranking Iranian political figure, Issa Kalantari, recently warned that past mistakes leave **Iran** with water supplies so insufficient that up to 70 percent, or 55 million out of 78 million Iranians, would be forced to abandon their native country for parts unknown.

Many facts buttress Kalantari's apocalyptic prediction: Once lauded in poetry, Lake Urmia, the Middle East's largest lake, has lost 95 percent of its water since 1996, going from 31 billion cubic meters to 1.5 billion. What the Seine is to Paris, the Zayanderud was to Isfahan – except the latter went bone-dry in 2010. Over two-thirds of Iran's cities and towns are "on the verge of a water crisis" that could result in drinking water shortages; already, thousands of villages depend on water tankers. Unprecedented dust storms disrupt economic activity and damage health.

Nor are Iranians alone in peril; many others in the arid Middle East may also be forced into unwanted, penurious, desperate exile. With a unique, magnificent exception, much of the Middle East is running out of water due to such maladies as population growth, short-sighted dictators, distorted economic incentives, and infrastructure-destroying warfare. Some specifics:

Egypt: Rising sea levels threaten not only to submerge the country's coastal cities (including Alexandria, population 4 million) but also to contaminate the Nile Delta aquifer, one of the world's largest groundwater reservoirs. The Ethiopian government finally woke to the hydraulic potential of the Blue Nile that originates in its country and is building massive dams that may severely reduce the flow of river water reaching Egypt (and Sudan).

Gaza: In what's called a "hydrological nightmare," seawater intrusion and the leakage of sewage has made 95 percent of the coastal aquifer unfit for human consumption.

Yemen: Oil remittances permit Yemenis to indulge more heavily than ever before in chewing *qat*, a leaf whose bushes absorb far more water than the food plants they replaced. Drinking water "is down to less than one quart per person per day" in many mountainous areas, reports water specialist Gerhard Lichtenthaeler. Specialist Ilan Wulfsohn writes that Sana'a "may become the first capital city in the world to run out of water."

Syria: The Syrian government wasted $15 billion on failed irrigation projects in 1988-2000. Between 2002 and 2008, nearly all the 420,000 illegal wells went dry, total water resources dropped by half, as did grain output, causing 250,000 farmers to abandon their land. By 2009, water problems had cost more than 800,000 jobs. By 2010, in the hinterland of Raqqa, now the Islamic State's capital, the *New York Times* reports, "Ancient irrigation systems have collapsed, underground water sources have run dry and hundreds of villages have been abandoned as

farmlands turn to cracked desert and grazing animals die off."

Iraq: Experts foresee the Euphrates River's waters soon halved (refer to Revelations 16:22 for those implications). Already in 2011, the Mosul Dam, Iraq's largest, shut down entirely due to insufficient flow. Sea water from the Persian Gulf has pushed up the Shatt al-Arab; the resulting briny water has destroyed fisheries, livestock, and crops. In northern Iraq, water shortages have led to the abandonment of villages, some now buried in sand, and a 95 percent decrease in barley and wheat farming. Date palms have diminished from 33 million to 9 million. Saddam Hussein drained the marshes of southern Iraq, at once destroying a wildlife ecology and depriving the Marsh Arabs of their livelihood.

Persian Gulf: Vast desalination efforts, ironically, have increased the salinity level of gulf sea water from 32,000 to 47,000 parts per million, threatening fauna and marine life.

Nearby **Pakistan** may be "a water-starved country" by 2022.

Israel provides the sole exception to this regional tale of woe. It too, as recently as the 1990s, suffered water shortages; but now, thanks to a combination of conservation, recycling, innovative agricultural techniques, and high-tech desalination, the country is awash in H_2O (Israel's Water Authority: "We have all the water we need"). I find particularly striking that Israel can desalinate about 17 liters of water for one U.S. penny; and that it recycles about five times more water than does second-ranked Spain.

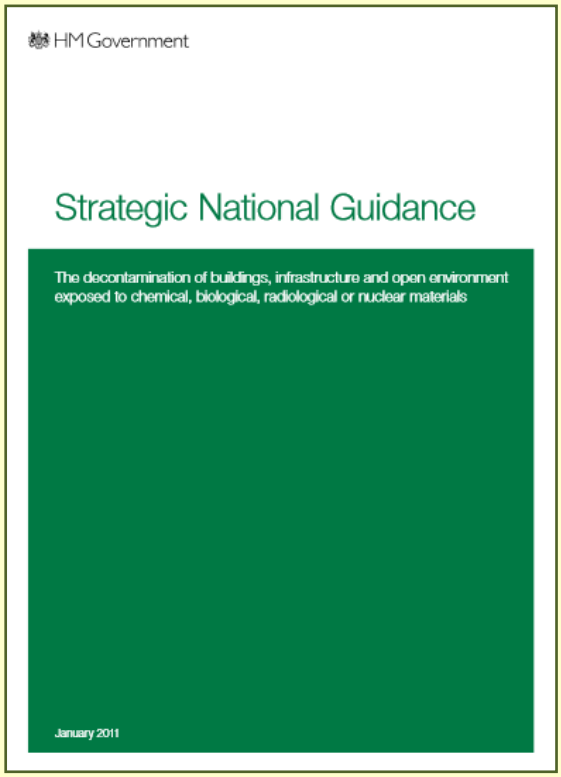
In other words, the looming drought-driven upheaval of populations – probably the very worst of the region's many profound problems – *can* be solved, with brainpower and political maturity. Desperate neighbors might think about ending their futile state of war with the world's hydraulic superpower and instead learn from it.

Daniel Pipes *is president of the Middle East Forum.*

Latest Strategic guidance on Building decontamination for CBRN

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

The guidance is part of sensible contingency and business continuity planning and does not mean that there is an increased risk of terrorist attack using CBRN materials. It gives basic information on the decontamination and remediation that may be required following a deliberate or accidental release in the UK as outlined below.



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.

Read the Strategic National Guidance at:
http://www.continuityforum.org/sites/default/files/images/403486_HMGov_StrategicNationalGuidance_acc.pdf