

May 2016

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders



www.cbrne-terrorism-newsletter.com

A look at the 1986 Chernobyl nuclear disaster in numbers

Source: <http://bigstory.ap.org/article/5ba7721c2b3d482eb87750b1bc882d05/look-1986-chernobyl-nuclear-disaster-numbers>

Apr 26 – Telling the story of Chernobyl in numbers 30 years later involves dauntingly large figures and others that are even more vexing because they're still unknown. A look at numbers that hint at the scope of the world's worst nuclear accident, the explosion and fire at the Chernobyl nuclear power plant on April 26, 1986:

— **More than 2 billion euros (\$2.25 billion):** The amount of money being spent by an internationally funded project to build a long-term shelter over the building containing Chernobyl's exploded reactor. Once the structure is in place, work will begin to remove the reactor and the lava-like radioactive waste.

— **4,762 square kilometers (1,838 square miles):** The amount of land around the plant that had to be abandoned because of heavy radiation and fallout, about half of it in Ukraine, where the plant is located, and the rest in Belarus. The area is approximately equal to the size of Rhode Island.

— **About 600,000 people:** Chernobyl's so-called "liquidators," those sent in to fight the fire and clean up the worst of the nuclear plant's contamination. They were all exposed to elevated radiation levels.

— **About 350,000 people:** Those evacuated from the explosion area in the early days after the accident, including all the 45,000 residents of the plant workers' city of Pripyat, or subsequently resettled by the government.

— **30 workers:** Plant employees who died in the explosion or from Acute Radiation Sickness within months.

— **9,000 to uncountable:** The eventual death toll from Chernobyl is subject to speculation and dispute. Even after the last person who was alive on the day of the explosion dies, other deaths may be attributable to Chernobyl because of the radiation fallout that has entered the food chain. The World Health Organization's cancer research arm suggests 9,000 people will die due to Chernobyl-related cancer and leukemia if the deaths follow a similar pattern to the Hiroshima and Nagasaki atomic bombings. The Greenpeace environmental group says the eventual Chernobyl death toll could be 90,000.

— **2 days:** The length of time until the world knew anything about the blast. Only after workers at a Swedish nuclear plant detected fallout and then analyzed where it could have come from did a picture of what had happened begin to form. The state-controlled Soviet

news media waited nearly three days to acknowledge anything had gone wrong, and even then downplayed its severity.



Radiological Terrorism – ‘Dirty Bombs’ and Beyond

By Uday Deshwal

Source: <http://thewire.in/2016/04/26/radiological-terrorism-dirty-bombs-and-beyond-31457/>

Apr 26 – In a pre-Nuclear Security Summit activity, the Nuclear Threat Initiative (NTI), a nonprofit, nonpartisan organisation working to reduce global threats from nuclear and other WMDs, released a [‘Radiological Progress Project Report’](#) on March 23. The report, while reviewing the progress made by 23 of the participating states (including Australia, Canada, Denmark, Germany, Italy, Japan, Kazakhstan, Republic of Korea, Turkey, UAE, UK, and the US) in their commitments, in accordance with the ‘2014 NSS Joint Statement on Enhancing Radiological Security’, aimed to raise “awareness and urgency to reduce the threat of the use of dangerous isotopes, develop a more effective system for securing radioactive sources, and replace the use of dangerous isotopes...” India was not party to this particular gift-basket from the previous summit.



However, in his visit to Washington for the 2016 Nuclear Security Summit, Prime Minister Narendra Modi announced several key initiatives taken by the government in the area of nuclear security and nonproliferation, and also confirmed that India would be “joining the three ‘gift-baskets’ for this summit in the priority areas of countering nuclear smuggling, nuclear security contact group in Vienna, and sharing of best practices through Centres of Excellence.” Additionally, he assured the “strengthening of the national detection architecture for nuclear and radioactive material, along with a plan of using vitrified forms of vulnerable radioisotopes such as cesium-137.”

Before 9/11, the use of radiation and its harmful effects was considered in at least two popular instances: General Douglas McArthur had suggested sowing “dangerous levels of radioactivity” along the Korean-Chinese border to prevent the Chinese from playing any further role on the ground in the Korean War; later, Saddam Hussein, in his efforts to acquire chemical, biological, radiological and nuclear (CBRN) capabilities, was believed to have experimented with the development of ways to disseminate radioactive material. In the aftermath of the events of 9/11 and al Qaeda’s subsequent announcement of their inclination toward using WMDs, a lot of attention was given to the possible use of so-called ‘dirty bombs’. However, as the threat from al Qaeda waned and with no reported activity on the use of the dirty bombs, so did the threat perception surrounding them.

But more recently, with the rise of the Islamic State (IS) and the increased level of terrorist activities in Europe, the discussion over the level of threat from nuclear and radiological terrorism has once again found some traction in the Western countries. Some have argued that the possible risk of use of nuclear and radiological material might just be higher than it has previously been, and yet there are others who don’t want to attach a sense of alarmism to such a threat just yet. In the Indian context, what is alarming is the lack of media or public attention and knowledge on the issue of radiological security and the threat from non-state actor use of radiological materials (i.e., radiological terrorism). Hence, with the long history of evolving and sophisticated attacks of terror in urban centres of India, there is a need for more public discourse on the nature of such a threat.

these sources are highly beneficial for mankind, some of these very same sources, however, can also be critical ingredients for a Radiological Dispersal Device (RDD), more generally termed as a ‘dirty bomb’.

Radiological Terrorism 101

There are tens of thousands of functioning radioactive sources in over 100 countries, and these sources find applications in multiple medicinal (including cancer treatment), industrial, and agricultural purposes. While



CBRNE-TERRORISM NEWSLETTER – February 2016

Radiological terrorism falls under the broader umbrella of CBRN (Chemical, Biological, Radiological and Nuclear) Terrorism/WMD (Weapons of Mass Destruction) Terrorism. Simply, radiological terrorism can be defined as the intentional and malicious use of radiation from the decay of radioactive materials to cause injury (fatal or otherwise) to person or property by unlicensed exposure through a particular device or method. The notable exception here is the use of nuclear yield-producing devices (Improvised Nuclear Devices or INDs), which would fall under the purview of nuclear terrorism, as such a device would involve the injuries/deaths being caused by a nuclear fission or fission-fusion reaction leading to a nuclear explosion.

What is a 'dirty bomb'?

A 'dirty bomb' is defined as a crude device that is intended to disperse powdered (or ground) high-risk radioactive material through the detonation of a mixture of said radioactive material and varying quantities of conventional explosives.

What are the high-risk radioactive materials?

From a security risk point of view, radioisotopes having what we may call "intermediate" half-lives, i.e., ranging from a few days to about a thousand years are of specific concern. A majority of radioisotopes either have a very short or very long half-life, and so that leaves us with about a couple of dozen radioisotopes that match the criteria of having intermediate half-lives. Add to that the high level of prevalence of use of such a group of radioisotopes in commercially used and widely available radioactive sources, and we are left with no more than a dozen high-risk radioisotopes.

Cobalt-60 (Co-60), cesium-137 (Cs-137), strontium-90 (Sr-90), iridium-192 (Ir-192),

among others, are some of the highly radioactive isotopes that are widely used in various medicinal, commercial, and industrial sources of applications including sterilisation and food irradiation, single- and multi-beam tele-therapy, industrial radiography, high- and medium-dose brachytherapy, research and blood irradiators, level and conveyor gauges, radioisotope thermoelectric generators, etc. The International Atomic Energy Agency, keeping in mind the potential harm to human

health, has categorised the commercially used radioactive sources based on radiation safety hazards as high-risk Category 1, 2, and 3 sources.

The relative security threat from each of these isotopes will vary and some of them will pose a bigger threat than the others depending upon: the *amount of particular radioisotope* present in a radioactive source & the *corresponding specific activity* (amount of material decaying per second) of the isotope; the *type of radiation emitted* (alpha, beta or gamma); and, the *kind of exposure* (internal or external). The respective *half-lives* also play a role in establishing the threat potential of a radioisotope. So, there are a lot of permutations and combinations that go into selecting the right amounts of the right radioisotope.

Is a 'dirty bomb' the only malicious way of disseminating high-risk radioactive materials?

Generally, the threat from radiological terrorism is almost exclusively restricted to the use of 'dirty bombs' – which is technically just one type of a Radiological Dispersal Device (RDD), which itself is one of the different possible ways of disseminating radioactive materials. While, a 'dirty bomb' may well be the most plausible form of dissemination of radioactive materials, a complete disregard for other forms of dissemination can lead to a misappropriation and limitation of the perceived threat from radiological terrorism.

Can there be other radiological weapons?

Drawing from a proposed definition by George Moore, a radiological weapon can more simply be defined as any device or method, except for a nuclear yield-producing device, that intentionally and maliciously uses, or intends to intentionally and maliciously use, radiation from the decay of radioactive materials to cause injury to person or property by unlicensed exposure.

Thus, in addition to a 'dirty bomb', other types of RDDs may comprise the **spread of radioactive materials through non-explosive and passive or active means**. The design and form of attack of a dirty bomb limits the use of a gamma emitting radioactive material to maximise the external radiation threat. However, in their 2007 study, James Acton, Brooke M. Rogers, and Peter



CBRNE-TERRORISM NEWSLETTER – February 2016

D. Zimmerman have suggested alternative non-explosive forms of radiation dispersal, focussing on terrorist intention to killing by inducing large internal radiation doses (bringing into play a larger number of alpha and beta emitting radioactive materials, which are highly dangerous once inside the body) through what they described as the “inhalation, ingestion, and immersion, or I3, attacks”.

The **scenarios** include the spreading of radioactivity through dissemination of radioactive materials in an aerosolised form to be more effective in getting the targets to inhale them. Sprayers can be used in crowded streets or at iconic sites of a city; airplanes used for crop dusting can also be employed to do the same. The aerosolised material can even be disseminated through ventilation systems in closed places such as theatres, concert venues, sports arenas, etc. Even the intentional spreading of materials by mail (similar to the Anthrax attacks) would constitute an RDD. If carried out successfully, the I3 attacks can be operationally more useful and at the same time presumably easier to carry out for the non-state actors. Unlike a dirty bomb attack, these attacks may take longer to be identified, leading to a wider spread of contamination. A relevant example here would be the use of Polonium-210 (possibly by the Russian government) to poison Alexander Litvinenko, a former KGB agent. He reportedly died within three weeks of being exposed to the radioactive material. It was already too late by the time it could be successfully detected that he was in fact suffering from radiation sickness.

Radiation Emission Device (RED) is another possible type of radiological weapon, which can include an unshielded stationary or mobile radioactive source that is emitting radiation. This type of device can be used to expose: a large number of people (a large source of highly radioactive material placed in a crowded place or being moved around through a large crowd – for instance, a device placed in a metro or train compartment); or, a specific or a small set of individuals (a smaller source and amount of highly radioactive material placed in close proximity – for example a device concealed in a part of the office of particular high-profile victim/s).

What are the possible effects of a radiological attack?

The most relevant case-study for understanding the scenarios of widespread malicious dispersal of radioactive material was the non-terror radiation accident in Goiania, Brazil, in 1987 – where a mishap initiated by the callousness in disposing an old radio-teletherapy machine in Goiania led to the death of 5 people. Scrap metal scavengers took away the source capsule from the machine, which contained about 1375 Curie of powdered Caesium-137, and later one of the scavengers punctured the source capsule which allowed the powder to leak out.

What are the health effects?

Different types of radiations interact with and damage the human body differently, and this is expressed by a factor called the Relative Biological Effectiveness (RBE). For example, if ingested or inhaled a material emitting alpha radiation is more potent. Thus, the effective radiation dose is the product of the energy deposited by the ionising radiation and the RBE for that particular type of radiation, and is measured by Roentgen Equivalent Man (rem) in the traditional system (SI unit: Sievert (Sv)). Broadly, radiological health effects can be classified as *deterministic and stochastic*.

As the name suggests, a **deterministic effect** is one where classic symptoms like radiation sickness (haematological effects, vomiting, loss of hair, likely death etc.) or radiation burns on the skin will be invoked and observed fairly instantly depending on the effective radiation dose received. Having said that, the threshold dose for deterministic effects is very high for external exposure from radioactivity. Loss of white blood cells is evident typically at doses in excess of 50rem (at times, some individuals can be affected by doses around 25-50rem). Victims exposed to doses in the range of 100-300rem experience vomiting and other symptoms of mild to high radiation sickness. Doses of 400-500rem and above are considered increasingly lethal to the exposed population. If inhaled or ingested (internal exposure), even a small quantity of an alpha emitter can deposit a high enough dose to bring about considerable deterministic health effects in the exposed population. For example, one gram of Americium-241 (Am-241), which can be found in smoke detectors, can produce over one million doses of 500rem or more to the whole body over the course of a year.



CBRNE-TERRORISM NEWSLETTER – February 2016

A **stochastic effect**, simply put, is the degree of carcinogenic impact from low levels of radiation exposure leading to an increased risk of delayed development of cancer and other health problems in a lifetime. Those exposed to doses in the range of 10s of rem are likely to have a higher probability of premature ageing, genetic effects and risk of development of cancer and tumours.

In the Goiania incident, around 250 people were identified as contaminated at the emergency response centres, of which 49 were admitted for further treatment. Out of the 49, around 20 people were reported to have received doses between 100-800 rads, which finally resulted in the death of five people.

What are the economic effects?

A successful and large-scale RDD attack in strategic and iconic locations in an urban city, can lead to a large-scale economic disruption. Such an attack could lead to a temporarily indefinite shutting down of the affected area, till the area is fully decontaminated and the radiation levels are restored to below the usual background levels. The present decontamination techniques are largely restricted in their effectiveness to say the least and according to relevant U.S. government officials, “existing decontamination techniques and procedures cannot facilitate quick, efficient recovery in a large urban environment” and that in the case of large-scale radiological terror acts it could take “billions of dollars and years or even decades to complete” decontamination efforts of such a massive scale. Additionally, if the affected area were a commercial hub or a market (shopping or stock), all trade and businesses, small or large, and related economic activity would come to a halt. Depending on the time to completely decontaminate the concerned area, it would be long before any commercial activity can resume. This resumption could be further affected by the reluctance of people to head back to the area, as the fears of radiation will continue to exist in people’s memories.

85 buildings in the city of Goiania were identified as being significantly contaminated, of which 7 were deemed uninhabitable and subsequently destroyed. A total of over 3500 cubic metres of radioactive waste was collected and disposed. With agriculture being the primary occupation in the area, the event

led to “the almost absolute interruption of the economic intercourse with the rest of Brazil”.

What are the psychological effects?

Furthermore, an act of radiological terrorism will, in all probability, cause distress and a psychological disorder among those directly affected by it, and is also very likely to have strong psychological impacts of different sorts even on those not directly affected. Initially, these effects will emerge in the form of spread of mass hysteria born out of the misinformed fears of radiation, leading to a disruption of the social order and overwhelming the already stretched emergency response and medical systems. The ones who had property and/or businesses or jobs in the affected area, as discussed earlier, will be dealing with the psychological effects of such heavy economic losses and livelihoods. A temporary moratorium might be placed by the government, on the city’s/area’s population on travelling to other parts of the country, invoking feelings of being ostracised, causing further psychological damage.

All of the above effects were observed in the case of Goiania, as around 112,000 people lined up for monitoring outside the emergency response centres. Additionally, a brief moratorium was placed on the people of Goiania which prevented them from travelling to other parts of Brazil.

Thus, to build on the effects observed in Goiania, an act of radiological terrorism is expected to only be that much more disruptive by its virtue of being a planned and malicious act of intentionally disseminating radioactive material. While, a radiological attack is unlikely to cause mass casualties, but, the scope for stochastic health effects, huge economic losses, and terrifying psychological and societal effects, is a significant one. This is perhaps why such a device is considered to be a weapon of mass disruption and not mass destruction.

To provide a more contemporary context to the possible effects of a large and successful radiological attack, let us consider the case of the recent terror attack on the airport and the metro station in Brussels. The explosions led to multiple deaths and injuries and also resulted in the shutting down of the particular airport terminal for a few days. Now imagine if instead of conventional explosions, these were in fact ‘dirty bombs’ that



CBRNE-TERRORISM NEWSLETTER – February 2016

exploded at the airport and the metro station. In addition to the deaths and injuries caused by the explosions and other health effects from the radiation, there would be enormous economic losses – owing to the direct and related costs of a complete shut down and decontamination of the entire airport and the metro system for an indefinite period of time. The resulting psychological effects and societal effects would be even more disastrous and would possibly result in widening the already existing religious and socio-ethnic cleavages, leading to a violent backlash across the globe.

What is the scope of the threat in India?

The potential for radiological terrorism in a volatile region like South Asia, and especially India, can be identified as a sum of: the persistence of terrorist threats and attacks from various non-state actors in the country and the region (where groups have shown a proclivity towards sophisticated means of causing mass disruption and deaths); and, the wide availability of commercial radioactive sources in places with less stringent security measures like hospitals and universities, etc. The possible acquisition pathways of getting hold of radioactive materials/sources can include theft from the various facilities holding such sources, insider threat, fraudulent purchase of radioactive sources, and orphaned sources. Radiological terrorism, with its ability to cause mass disruption and not apocalyptic destruction (associated with a non-state actor use of nuclear weapons), can be viewed as a complex and unanticipated extension to conventional terrorism. At worst, radiological terrorism can offer an added dimension of the

fear of the unknown and can be a potent way of bringing about mass disruption through deaths, radiation injuries, and a psychological, political, and economic breakdown of society and possibly the breakdown of the state's machinery.

Having said that, and in assuaging the alarmist fear of the possibility of an act of radiological terrorism, it should also be noted that the list of Indian regulatory, legal, and other official provisions for the safety and security of radioactive sources is exhaustive. On paper, the institutional infrastructures are strong, comprehensive, and in accordance with the international standards. This was reinforced further by PM Modi in his recent assurances at the 2016 NSS.

Other than the threat issued by Chechen rebels in 1995 of releasing radioactive material in one of Moscow's iconic parks and al Qaeda's broad expression of interest in using CBRN weapons, there has been no known instance of radiological terrorism.

The probability and potential of a particular act of terrorism is usually contingent on two important factors: capability of carrying out the act, and the motivation and perceived benefit (for the non-state actor) of carrying out the act. So, in conclusion, it can be said that while implementation of provisions to prevent non-state actors from gaining access to radioactive materials, and a perceived lack of motivation among terrorist groups of carrying out such an act of terrorism thus far, suggests that the threat of radiological terrorism may not be as acute as is made out to be at times, yet there is a need for preparedness and public awareness to guard against such a terrible eventuality.

Uday Deshwal works on South Asian and other global security and conflict issues, and is an alumnus of the Department of War Studies at King's College London. He has previously worked as a Research Associate at the Centre for Air Power Studies, New Delhi.

Nuclear emergencies and the masters of improvisation

By Sonja Schmid

Source: <http://thebulletin.org/chernobyl-fukushima-and-preparedness-next-one>

April 26 marks the 30th anniversary of the Chernobyl disaster, and those old enough to remember the event can recall the explosion, the evacuation, and the dread. But they rarely remember an immense milestone in the *response* to the disaster: the completion in November 1986 of a concrete encasement of Chernobyl's reactor number four. Workers drawn from all across the Soviet Union built this "sarcophagus" under extreme radiological conditions, on the ruins of the destroyed reactor. They used unimaginable amounts of concrete—and a great deal of imagination. This concrete mausoleum has held up, with some assistance, for 30 years now.



CBRNE-TERRORISM NEWSLETTER – February 2016

(A [larger containment structure](#) that will fit over the existing sarcophagus is now being built.)

Over the years, as the ranks of those who *responded* to Chernobyl have thinned, new generations of nuclear professionals have been trained to *prevent* another disaster. Their training has emphasized "safety culture." This, along with "inherently safe designs," was going to guarantee an accident-free nuclear future. For a while, it seemed as if the world was on the verge of forgetting forever what responding to a nuclear emergency really required. Then, in March 2011, multiple reactors at one of the world's largest nuclear power plants melted down as a consequence of a massive earthquake, a tsunami, and a sustained power outage.

As a student of the Soviet nuclear power program and the Chernobyl disaster, it was painful for me to watch the blame game that played out immediately after Fukushima. Almost to the letter, the Chernobyl "script" was followed. First, the plant's operators were blamed. Then the reactor design was at fault. Finally, it was the turn of the national nuclear regulatory structure. "Culture," of course, received a great deal of blame as well.

But while Chernobyl could ultimately be dismissed as a Soviet-made disaster that "could never happen here"—wherever "here" happened to be—Fukushima has not allowed such steadfast denial. Indeed, Fukushima has proved the death knell for a nuclear safety philosophy that focused exclusively on *preventing* accidents. Disaster preparedness and response were given scant attention in the years between Chernobyl and Fukushima, but now they have been added to the vocabulary of the world's nuclear industries. Curiously, however, this shift is only partial. Disaster prevention retains the greatest emphasis; preparedness is sometimes treated adequately; but resources (and imagination) devoted to actual *response* strategies remain limited.

The "lessons learned" from Fukushima—and new reports on these lessons continue to be published—focus predominantly on technical and legal fixes, organizational reform, and liability concerns. In the United States, the [Nuclear Regulatory Commission responded to Fukushima](#) by overhauling its rules and guidelines for accident prevention, preparedness, and response. The US nuclear industry, meanwhile, implemented "[FLEX](#)," a

program designed to provide nuclear reactors in distress with hardware such as extra pumps and generators, both on site and stored at regional centers. In Europe, power reactors were subjected to "[stress tests](#)" after Fukushima, and these tests sparked conversation among nations hosting nuclear power reactors about harmonizing, if only loosely, national regulations concerning natural (and other) hazards to nuclear power plants.

Steps such as these go in the right direction. But emphasizing prevention and preparedness over response ignores a simple fact: Nuclear disasters tend to exceed people's worst expectations. There is a good reason that the nuclear industry refers to disasters as "[beyond design-basis accidents](#)"—only a limited number of scenarios can be anticipated and prepared for. Disasters, therefore, require the development of creative, skill-based, and team-based response strategies (along with strenuous efforts to avoid disasters entirely).

Training for emergency responders in general tends to emphasize flexibility and imagination, with a premium placed on performing quick assessments and triage in unprecedented situations. But in nuclear emergency response training, the situation is different. The nuclear industry seems deeply troubled by using human imagination to address situations that go "beyond the checklist." In Europe and the United States, at least—I can't speak for the entire world—the nuclear industry seems hung up on the idea of control. There is a plan for every conceivable situation. Should plans fail, there are more plans. Staff are trained to follow procedures and execute instructions. If they don't, that's always bad.

Such an approach, as documented by the anthropologist [Constance Perin](#), fundamentally fails to acknowledge the messiness of operating imperfect, real-world technologies (and *all* technologies are imperfect). Worse yet, it incapacitates an aspect of creativity that, though it's more often associated with jazz, can be tremendously important in nuclear emergencies: improvisation. In music, improvisation calls to mind wild, random, and perhaps solitary acts. But if emphasized in training for nuclear emergencies, the metaphor of improvisation can help prepare responders to pursue skill-based, team-oriented, and highly organized actions under challenging conditions.



CBRNE-TERRORISM NEWSLETTER – February 2016

In any disaster, improvisation occurs. It happened at Chernobyl, even if creative imagination was thoroughly expunged from all written reports. Improvisation happened at Fukushima, and in fact a lot more improvisation will be necessary if the Fukushima disaster is

ever to "end." It is tempting to remember creative action only when it fails. Making this mistake locks in a mindset of control and controllability. Any such mindset will be exploded—yet again—by the next nuclear emergency.

Sonja Schmid is an associate professor in Science and Technology Studies at Virginia Tech. Her expertise is in the history of technology, science and technology policy, and social studies of risk. Fluent in Russian, she investigates the history and organization of nuclear industries in the former Soviet Union and Eastern Europe and studies the way national energy policies, technological choices, and nonproliferation concerns shape each other. In a current project funded by a National Science Foundation CAREER Award, she is investigating the challenges of globalizing nuclear emergency response. She is the author of Producing Power: The Pre-Chernobyl History of the Soviet Nuclear Industry.

Learning from nuclear accidents, expanding nuclear energy

By Augustin Simo

Source: <http://thebulletin.org/chernobyl-fukushima-and-preparedness-next-one>

Nuclear energy accounts for about 11 percent of world electricity production, and this share is likely to increase over the medium term as the world seeks to limit carbon dioxide in the atmosphere and thereby mitigate climate change. But since the Fukushima accident, global expansion of nuclear energy has slowed—just as it did after the Chernobyl disaster. Accidents at power reactors, even when their severity is limited, can create in the public an unjustified phobia about nuclear energy.

The Chernobyl disaster of 1986 was caused by factors including [a flawed reactor design](#), [insufficient training of plant operators](#), and [a lack of nuclear safety culture](#). About 30 people died soon after the explosion as a consequence of acute radiation syndrome, and [the death toll has since risen to 56 or so](#). Any premature death is regrettable. But Chernobyl mobilized scientists and engineers to improve electronic control of reactor operations. It led to improved instruction in nuclear safety culture. The probability of another accident similar to Chernobyl now appears very low.

The world's second major nuclear accident, 25 years after the first, was the Fukushima disaster of five years ago. In this case the cause was external events—a high-magnitude earthquake and tsunami. No deaths related to radiation were reported, though quite a few deaths can be attributed to anxiety or other psychological effects. Of the 160,000 people who were displaced from the accident area,

about 60,000 have returned to their homes and others are returning slowly.

The global nuclear community is still learning the lessons of Fukushima. But it is already using those lessons to prevent future accidents. When new power plants are designed, severe external hazards are now being taken into account. Substitutes are being developed for components that failed at Fukushima. Mobile systems have been developed to provide electricity or cooling water to power plants when their own systems fail. Many countries have subjected their nuclear power installations to stress tests, and many have reviewed their legal and safety frameworks. Under the leadership of the International Atomic Energy Agency (IAEA), international safety standards have been strengthened. Networks of regulators, operators, and vendors have been established at the international, regional, and sub-regional levels to enhance the global nuclear safety regime. International conferences have been organized with a focus on understanding the origins and harmful effects of the Fukushima accident. As a result, nuclear power plants around the world are receiving improved guidance for strengthening their safety measures.

So both the Chernobyl and Fukushima accidents have provided lessons that are improving nuclear safety. And the international nuclear community is making consistent, effective efforts to



CBRNE-TERRORISM NEWSLETTER – February 2016

avert loss of human life (even though it is impossible to exclude that possibility in the event of a severe nuclear accident). Yet space exists for further improvement. International cooperation among nuclear power plant operators should be enhanced. More nations should participate in the international peer reviews of nuclear installations that the IAEA's board of governors recommended in a [2011 action plan](#). These missions are a good step toward enhancing safety culture and winning public acceptance of nuclear energy—and toward improving emergency preparedness and response.

Global harmonization

Indeed, where preparedness and response for nuclear and radiological accidents are concerned, the IAEA has already developed specific safety standards. But there is still a need to harmonize approaches to emergency preparedness and response around the world. Each country, whether it uses nuclear power or not, should continuously develop and maintain its response capabilities at all levels, taking into account the harm that nuclear or radiological accidents can cause to individuals and the environment in other countries, whether neighboring or far away.

In many developing countries, such as my own Cameroon, the greatest cause for concern is emergencies involving radioactive sources. These emergencies could include sabotage at nuclear installations, theft or loss of radioactive sources, and accidents during the transport of radioactive materials. But then, whenever nuclear or radiological accidents occur, standards for emergency preparedness are reviewed to ensure that any such events in the future remain controlled. The international nuclear community is quite aware of the need to continuously improve the management of nuclear accidents and mitigate negative consequences for human beings and the environment.

Augustin Simo has been director-general of Cameroon's National Radiation Protection Agency since January 2010. His past positions include permanent secretary of the National Committee for Technology Development and head of the Energy Research Laboratories at the Institute of Geological and Mining Research. He is also current chairperson of the Forum for Nuclear Regulatory Bodies in Africa and Cameroon's national liaison officer for the International Atomic Energy Agency. He has taught at the University of Douala and the University of Yaoundé. In 1982, he was awarded a doctorate in physics/energy from France's University of Aix Marseille III.

The IAEA, to improve member states' preparedness for nuclear and radiological accidents, recently launched a new web-based tool, the Emergency Preparedness and Response Information Management System—a "self-assessment tool" that Elena Buglova, head of the IAEA's Incident and Emergency Centre, believes "will make an important contribution to preparedness levels of member states." It is also worth recalling that the agency, according to the [Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency](#), has specific responsibilities "with regard to assisting states in developing their own preparedness arrangements for nuclear and radiological emergencies."

It is also vital for effective emergency response that technical information about nuclear power plants and accidents be shared widely. Operators, regulators, vendors—all the stakeholders in nuclear industries—can only make appropriate contributions to the management of accidents if they have access to the same information. Effective emergency preparedness requires a global outlook.

Change of course

Nuclear energy deserves a high-priority position in the global strategy for establishing sustainable energy systems. According to the International Energy Agency and the Nuclear Energy Agency, global nuclear capacity must double by 2050, and [nuclear energy must supply 17 percent of overall electricity production, if global warming is to be limited to 2 degrees above pre-industrial levels](#). Many politicians today promise to exclude nuclear energy from their countries' electricity mix. But it's almost certain that they'll change course very soon—embracing nuclear power because it is among the most reliable and sustainable options for electricity supply.



Great progress since Chernobyl—and the distance still to go

By Manpreet Sethi

Source: <http://thebulletin.org/chernobyl-fukushima-and-preparedness-next-one>

A disaster is an event of unanticipated severity and scale that causes damage too great to allow quick recovery. It poses dangers that do not remain within a manageable range. Otherwise, a disaster would not be a disaster—only a crisis.

The key to handling disasters, therefore, is to anticipate—and prepare for—the worst. Fortunately, as science and technology have advanced, so too has human capacity to anticipate and respond to disasters. Nature continues to produce extreme environmental events. But today, the hazardous activities in which human beings engage are generally designed with emergency preparedness and response in mind.

Producing nuclear power is one such activity, but in more than 60 years of operations at power reactors—[16,000 cumulative reactor-years](#)—the nuclear industry has witnessed only two disasters, at Chernobyl and Fukushima. And only Chernobyl resulted in fatalities—30 very soon after the event and about two dozen more in the years since, with additional deaths projected in the long term. What these figures indicate is that the nuclear industry attaches due importance to the safety of reactor operations. It well recognizes that even two disasters in six decades, only one of them involving fatalities, have been sufficient to create negative public perceptions of nuclear power!

There are three primary ways to address this issue. First, the safety of reactor operations can continually be improved. Second, better emergency preparedness and response can be instituted. Third, improvements on both fronts can be communicated to the public. Both the Chernobyl and Fukushima disasters rendered important lessons along all three of these dimensions—but the focus here is improved disaster preparedness since the 1980s.

The improvement has been substantive. Chernobyl led to the creation of an international legal framework for emergency preparedness and response, as well as a set of related regulatory processes and official guidelines. Implementing all this is a question of national responsibility. But implementation proceeds in accordance with international benchmarks that

were largely created after Chernobyl, and in some cases revised after Fukushima.

Steps taken

The International Atomic Energy Agency (IAEA) has been the lead agency in establishing conventions that specify guidelines for handling emergencies. After Chernobyl, the first such instrument to be adopted was the [Convention on Early Notification of a Nuclear Accident](#). Because Chernobyl had made the transboundary implications of nuclear disasters quite conspicuous, nations brought the Convention into force quickly—by the end of October 1986. The [Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency](#) was adopted simultaneously, though it did not enter into force until the next year. Both instruments placed specific obligations on states parties, and on the IAEA, to establish arrangements for nuclear or radiological emergencies. These obligations are strengthened by two later conventions—the [Convention on Nuclear Safety](#) and the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management. These four conventions cover quite a wide range of nuclear activities.

Over the years, [the IAEA has published a series of safety standards](#) meant to enhance national arrangements for safety, preparedness, and response at nuclear power plants. The agency also works to ensure the compatibility of national, bilateral, regional, and international mechanisms and procedures for disaster response. After Fukushima, the agency's General Safety Requirements were revised to incorporate lessons newly learned. This led to publication of "[Preparedness and Response for a Nuclear or Radiological Emergency](#)," a document recommending standards for preparedness and response. Nations can enforce these standards by adopting legislation and regulations; assigning responsibilities to nuclear operators and national and local officials; and establishing regulatory frameworks through which effective implementation can be verified.



CBRNE-TERRORISM NEWSLETTER – February 2016

But the IAEA is by no means the only agency involved in improving disaster preparedness. In 1986, the [Inter-Agency Committee on Radiological and Nuclear Emergencies](#) was created in recognition that cooperation and coordination among agencies is extremely important. Eighteen organizations are part of this mechanism, and they are as diverse as the Comprehensive Nuclear Test Ban Treaty Organization, the World Health Organization, and the International Civil Aviation Organization. The Committee has created a Joint Radiation Emergency Management Plan to harmonize international standards for emergency preparedness and response. The Plan allows for a common understanding of participating organizations' roles, responsibilities, and capabilities—and also provides an overall concept of the group's operations so that quick, coordinated responses are possible.

Steps still to take

After Fukushima, nearly all countries operating nuclear reactors undertook reviews of their emergency response systems—and the [Japanese government](#) and the [IAEA](#) produced reports highlighting several ways in which emergency preparedness could be improved. One such recommendation is that, during an emergency, public officials must have quick access to informed scientific opinion and expert judgment so they can make good decisions in extreme time pressure. Certain errors committed during the Fukushima emergency—regarding the timing and extent of evacuations, for example—might have been avoided if officials had had better advice.

A second recommendation is that officials be given the resources to correctly classify the severity of an incident as it occurs. That way, the correct set of standard operating procedures can be activated at the earliest

possible moment. Classifying an incident as less severe than it really is—or more—can squander precious time and credibility. Third, the provision of accurate information at all levels is crucial. If operators, for example, attempt to conceal an accident (or its extent) from national or international authorities, an appropriate response is only delayed. At Chernobyl, for example, only limited evacuations from the affected area were ordered—and [only after 36 hours had passed](#). To be sure, Chernobyl's immediate fatalities remained very limited compared to many non-nuclear emergencies. But the disaster was felt across the physical, socioeconomic, political, and psychological spectrum of countries in the region. These effects could have been reduced if accurate information had been available. Finally, emergency capabilities must be coordinated across the local, state, and national levels. But this is only possible if operators conduct periodic drills involving all relevant entities and if deficiencies are conscientiously rectified.

Choosing, preparing

Energy is the essence of human progress. For countries seeking an energy-rich future, nuclear power is one of many options. Nations will make their own sovereign choices, based on their own calculations, about nuclear power. Countries that opt for nuclear power well understand that a great deal of legal and regulatory infrastructure is required if they are to operate nuclear sectors safely and sustainably. One element of this infrastructure is emergency preparedness and response. It is incumbent on nations to continually improve their capacity for disaster management. Fortunately, international mechanisms for, and national efforts at, disaster preparedness are making this task progressively easier.

Manpreet Sethi is a senior fellow at the Centre for Air Power Studies in New Delhi, where she heads the project on nuclear security. She is the author of Code of Conduct for Outer Space: A Strategy for India and Nuclear Strategy: India's March Towards Credible Deterrence; and editor of Nuclear Power: In the Wake of Fukushima. She received a doctorate in international relations from the School of International Studies at Jawaharlal Nehru University in 1997. She is a recipient of the prestigious K. Subrahmanyam Award for excellence in strategic studies.

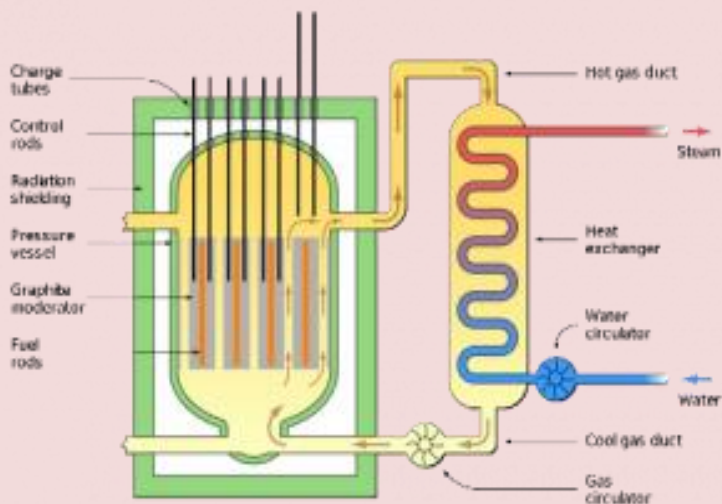


Dealing with irradiated nuclear graphite

Source: <http://www.homelandsecuritynewswire.com/dr20160427-dealing-with-irradiated-nuclear-graphite>

Apr 27 – During the existence of nuclear power industry a large number of channel uranium-graphite nuclear power reactors was built across the world. Russia alone operates four units of the Leningrad Nuclear Power Plant, four units of Kursk NPP, three units of Smolensk NPP, and four units of Bilibino NPP. Also, thirteen industrial uranium-graphite reactors were built (IUGR) have been built. To date, they all are on the output stage of the operation or decommissioning preparation.

Approximately 250,000 tons of irradiated graphite are accumulated in the world, including ~ 60,000 tons in Russia. Due to the specificity of irradiated graphite, the treatment of this type of radioactive waste has not been determined yet.



Nuclear economics

At the moment, the problem of irradiated nuclear graphite has been partially solved only for a select group of industrial uranium-graphite reactors. TPU reports that this is possible by referring graphite waste to “special waste”. Thus, in September 2015 it was successfully completed a pilot project to establish a point of long-term preservation of special waste at the site of the industrial uranium-graphite nuclear EI-2 reactor. To implement this project the experts of JSC “PD UGRC” developed and patented the unique technology of IUGR output of operation. For a long time they together with leading institutions (IPCE RAS, NIKIET OKBM, MEPI, VNIINM, Institute of Nuclear Power Plant, and others) have conducted R & D to

develop techniques and technical solutions to treat graphite waste.

However, this technology is not applicable for most reactors. “From these reactors it is necessary to extract graphite, then process to remove the most active radionuclides. Therefore, it is required to develop technologies, devices and hardware systems to reduce radioactive waste activity, which will make disposal of graphite economically profitable,” explains Evgeniy Bepala, a Ph.D. student from the Department of Technical Physics. Disposal of different classes of waste has a different price: the price for disposal of high-level, intermediate-level, and low-level waste differs enormously. If we reduce the amount of radioactive nuclides in reactor graphite, the cost of its disposal will be economically feasible.

Now scientists from different countries are searching for methods for reprocessing irradiated nuclear graphite. There are different ways: from pyrolytic incineration to centrifugation. Which one is the best is still unknown.

Bepala has been addressing the issue of nuclear graphite reprocessing for more than five years. Currently, he is an R & D engineer at JSC “Pilot and Demonstration Center for Uranium-Graphite Reactors Decommissioning” (the city of Seversk, Russia). Last year, the polytechnician became one of the winners of the UMNIC program and received financial support to perform his research.

Approaches for reducing graphite activity

The technology proposed by the polytechnician implies the heating of reactor graphite in a low-temperature plasma to more than three thousand degrees by Celsius. As a result, graphite and radionuclides contained therein sublimate. Further there is a stepwise deposition of substances in a special plasma-chemical reactor. To create such a reactor is a task before the scientist.

Carbon and radionuclides evaporate together, they are separated one from another in steps in different parts of plasma chemical reactor due to the difference in physicochemical properties. Thus, radioactive nuclei are selectively extracted from graphite.



CBRNE-TERRORISM NEWSLETTER – February 2016

Therefore, carbon black, which is formed by plasma-chemical reactions within the plasma chamber, is getting less active, says Evgeniy Bespala.

According to the polytechnic the technology itself is not new: previously radioactive waste has been processed in plasma. However, this was low-level metal waste.

Within the UMNİK grant, researchers will deal with creating a facility that provides mass graphite processing without human intervention. This will allow automating the entire process and protecting people from hazardous radioactive sources. According to the plan, irradiated nuclear graphite will be loading to the facility only and then carbon

waste with less activity compared to the original will be removed, - says the polytechnic.

Tomsk scientists and Seversk colleagues already are testing their technologies. The Department of technical physics at Tomsk Polytechnic University conducts required experiments for graphite evaporation in low-temperature plasma. All radiation research, in turn, is held in Seversk, as there is an opportunity to follow all the rules of radiation safety. For the present, the technology has been tested on mixtures of carbon stable isotopes. TPU notes that Next year, the scientists plan to test their facility on irradiated reactor graphite.

— Read more in *E V Bespala et al., “Analysis of Wigner energy release process in graphite stack of shut-down uranium-graphite reactor,” IOP Conference Series: Materials Science and Engineering (2015): 012065.*

Forget Fukushima: Chernobyl still holds record as worst nuclear accident for public health

By Timothy J. Jorgensen

Source: <http://www.homelandsecuritynewswire.com/dr20160426-forget-fukushima-chernobyl-still-holds-record-as-worst-nuclear-accident-for-public-health>

Apr 26 – The 1986 Chernobyl and 2011 Fukushima nuclear power plant accidents both share the notorious distinction of attaining the highest accident rating on the International Atomic Energy Agency (IAEA) [scale of nuclear accidents](#). No other reactor incident has ever received this Level 7 “major accident” designation in the history of nuclear power. Chernobyl and Fukushima earned it because both involved core meltdowns that released significant amounts of radioactivity to their surroundings.

Both of these accidents involved evacuation of hundreds of thousands of residents. Both still have people waiting to return to their homes. And both left a legacy of large-scale radioactive contamination of the environment that will persist for years to come, despite ongoing cleanup efforts.

So the tendency is to think of these accidents as similar events that happened in different countries, twenty-five years apart.

But the IAEA scale isn’t designed to measure public health impact. In terms of health ramifications, these two nuclear accidents were not even in the same league. While Fukushima involved radioactivity exposures to hundreds of

thousands of people, Chernobyl exposed hundreds of millions. And millions of those received substantially more exposure than the people of Fukushima.

On the occasion of the thirtieth anniversary of the 26 April 1986 Chernobyl accident in Ukraine, we do well to reflect on the health burden it caused – and compare it with what we expect to see from Japan’s Fukushima nuclear accident. As I report in my book [Strange Glow: The Story of Radiation](#), from a public health standpoint, there’s really no comparison between the two events.

Higher doses of radiation, more health harm

Chernobyl was by far the worst reactor accident of all time. A total of 127 reactor workers, firemen, and emergency personnel on site sustained radiation doses sufficient to cause radiation sickness (over 1,000 mSv); some received doses high enough to be lethal (over 5,000 mSv). Over the subsequent six months, [fifty-four died from their radiation exposure](#). And it’s been estimated that twenty-two of the 110,645 cleanup workers may have [contracted fatal](#)



CBRNE-TERRORISM NEWSLETTER – February 2016

[leukemias](#) over the next twenty-five years.

In contrast, at Fukushima, there were no radiation doses high enough to produce radiation sickness, even among the reactor core workers. Two Fukushima workers who had leaky respirators received effective doses of [590 mSv and 640 mSv](#). That's above the Japanese occupational limit for conducting lifesaving rescue work (250 mSv), but still below the threshold for radiation sickness (1,000 mSv). Due to their exposure, the two workers' lifetime cancer risks will [increase about 3 percent](#) (from the 25 percent background cancer risk rate to about 28 percent), but they are unlikely to experience other health consequences.

Beyond just the plant workers, over 572 million people among forty different countries got at least some exposure to Chernobyl radioactivity. (Neither the United States nor Japan was among the exposed countries.) It took two decades to fully assess the cancer consequences to these people. Finally, in 2006, an international team of scientists completed a comprehensive [analysis of the dose and health data](#) and reported on the cancer deaths that could be attributed to Chernobyl radioactivity.

Their detailed analysis included countrywide estimates of individual radiation doses in all forty exposed countries, and region-wide estimates for the most highly contaminated regions of the most highly contaminated countries (Belarus, Russian Federation, and Ukraine).

Using statistical models, the scientists predicted a total of 22,800 radiation-induced cancers, excluding thyroid cancers, among this group of 572 million people. Thyroid cancer warranted separate special scrutiny, as we will discuss presently; this hormonally important gland is uniquely affected by a specific radioactive isotope, iodine-131.

So that's 22,800 non-thyroid cancers in addition to the approximately 194 million cancer cases that would normally be expected in a population of that size, even in the absence of a Chernobyl accident. The increase from 194,000,000 to 194,022,800 is a 0.01 percent rise in the overall cancer rate. That's too small to have any measurable impact on the cancer incidence rates for any national cancer registries, so these predicted values will likely remain theoretical.

Chernobyl's iodine-131 thyroid effects far worse

Unfortunately, at Chernobyl, the one type of cancer that could have easily been prevented was not. The population surrounding Chernobyl was not warned that iodine-131 – a radioactive fission product that can enter the food chain – had contaminated milk and other locally produced agricultural products. Consequently, people ate iodine-131-contaminated food, resulting in thyroid cancers.

For the local population, iodine-131 exposure was a worst-case scenario because they were already [suffering from an iodine-deficient diet](#); their [iodine-starved thyroids](#) sucked up any iodine that became available. This extremely unfortunate situation would not have happened in countries such as the United States or Japan, where diets are richer in iodine.

Thyroid cancer is rare, with a low background incidence compared to other cancers. So excess thyroid cancers due to iodine-131 can be more readily spotted in cancer registries. And this, in fact, has been the case for Chernobyl. Beginning five years after the accident, an increase in the rate of thyroid cancers started and continued rising over the following decades. Scientists estimate that there will ultimately be about [16,000 excess thyroid cancers](#) produced as a result of iodine-131 exposure from Chernobyl.

At Fukushima, in contrast, there was much less iodine-131 exposure. The affected population was smaller, local people were advised to avoid local dairy products due to possible contamination and they did not have iodine-deficient diets.

Consequently, typical radiation doses to the thyroid were low. Iodine-131 uptake into the thyroids of exposed people was measured and the [doses were estimated to average](#) just 4.2 mSv for children and 3.5 mSv for adults — levels comparable to annual background radiation doses of approximately 3.0 mSv per year.

Contrast this to Chernobyl, where a significant proportion of the local population received thyroid doses in excess of 200 mSv — fifty times more — well high enough to see appreciable amounts of excess thyroid cancer. So at Fukushima, where iodine-131 doses approached background levels, we wouldn't expect thyroid cancer to present the problem that it did at Chernobyl.



CBRNE-TERRORISM NEWSLETTER – February 2016

Nevertheless, there has already been one report that [claims there is an increase](#) in thyroid cancer among Fukushima residents at just four years post-accident. That's earlier than would be expected based on the [Chernobyl experience](#). And the study's design has been criticized as flawed for a number of scientific reasons, including the [comparison methods used](#). Thus, this report of excess thyroid cancers must be considered suspect [until better data arrive](#).

Chernobyl has no comparison

In short, Chernobyl is by far the worst nuclear power plant accident of all time. It was a totally human-made event — a "safety"

[test gone terribly awry](#) — made worse by incompetent workers who did all the wrong things when attempting to avert a meltdown.

Fukushima in contrast, was an unfortunate natural disaster – caused by a tsunami that flooded reactor basements — and the workers acted responsibly to mitigate the damage despite loss of electrical power.

26 April 1986 was the darkest day in the history of nuclear power. Thirty years later, there is no rival that comes even close to Chernobyl in terms of public health consequences; certainly not Fukushima. We must be vigilant to ensure nothing like Chernobyl ever happens again. We don't want to be "celebrating" any more anniversaries like this one.

Timothy J. Jorgensen is Director of the Health Physics and Radiation Protection Graduate Program and Associate Professor of Radiation Medicine, [Georgetown University](#).



All Belgian residents issued with iodine tablets to protect against radiation

Source: <http://www.telegraph.co.uk/news/2016/04/28/all-belgian-residents-issued-with-iodine-tablets-to-protect-again/>



Apr 28 –**The entire population of Belgium is to be issued with a ration of iodine tablets, months after warnings about the threat of Isil building a dirty bomb.**

Iodine pills, which help reduce radiation build-up in the thyroid gland, had previously only been issued to people living within 20km (14 miles) of the Tihange and Doel nuclear plants.

Maggie De Block, the Health Minister, said that would be extended to 100km, covering the whole country of 11 million people, following advice from an expert council.

The pills will be sent to pharmacies, and the public would be ordered to collect their ration in the event of a meltdown. Children, pregnant women and those breast-feeding would be given priority.

It emerged following last month's terrorist attacks that an Isil cell may have been plotting to kidnap a nuclear expert in order to build a "dirty bomb". Eleven nuclear workers had their passes revoked.



CBRNE-TERRORISM NEWSLETTER – February 2016

Ibrahim and Khalid el-Bakraoui, the brothers behind the suicide strikes on Brussels airport and Metro, are believed to have been involve the plot to scatter radioactive material over a populated area.

A senior Belgian nuclear industry official was secretly filmed by jihadists late last year, according to the country's nuclear authority, and the brothers were linked to the surveillance.

There are also concerns over Belgium's ageing nuclear plants that have been subject to repeated safety warnings, including defects in pressure vessels and fires.

Last week Germany asked that the 40-year-old Tihange 2 and Doel 3 reactors be turned off "until the resolution of outstanding security issues".

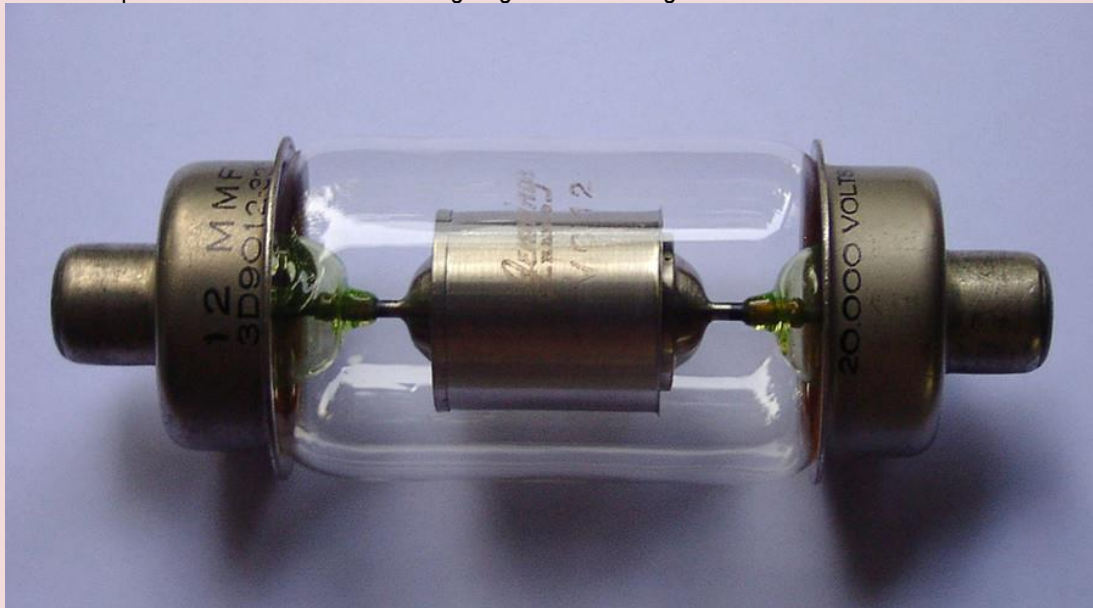
The reactor pressure vessels at both sites have shown signs of metal degradation, raising fears about their safety. They were temporarily closed but resumed service last December.

Belgium's official nuclear safety agency (AFCN) rejected the German request, saying the two plants "respond to the strictest possible safety requirements."

The key figure in the suspected dirty bomb plot is Mohammed Bakkali, 28, from Brussels, who was arrested in November on suspicion of helping to plan the Paris massacre. Police raided his wife's flat and found a ten-hour video taken by a camera hidden opposite the home of an executive at the Centre for the Study of Nuclear Energy in Mol, northern Belgium. The executive had access to radioactive isotopes at the country's national nuclear research centre.

Uranium season: 2nd group of isotope smugglers busted in Georgia in 10 days

Source: <https://www.rt.com/news/341222-georgia-uranium-illegal-sellers/>



Apr 28 – **Georgia's security service says it has detained a group of five Georgian citizens, alleged to have been trying to sell radioactive Uranium for \$3 million.** The group was caught in possession of Uranium-238 and Uranium-235, Reuters reports.

"Officers of Georgia's State Security Service detained five Georgian citizens, who were trying to sell uranium," security service investigator Savle Motiashvili said.

"The detainees were planning to sell nuclear material, Uranium-238 and Uranium-235, weighing 1.66 kilograms for \$3 million," he added.

"They were arrested when they were moving the radioactive material to a flat in Kobuleti," a member of the Georgian security service told a press conference, according to RIA Novosti.

The arrests come less than two weeks after the country's security service detained six individuals who were trying to sell Uranium-238. Three Georgians and three Armenian citizens were arrested. The group was hoping to sell the weapons-grade material for \$200 million, Motiashvili said at the time.

Motiashvili added that a radioactive proof container for transporting the Uranium-238 was found at the apartment of one of those arrested on Thursday.



CBRNE-TERRORISM NEWSLETTER – February 2016

"Given the gamma ray emission, the identity of the source and radiological expertise report, the seized substance endangers life and health," he said, as cited by Reuters.

Uranium-238 is a highly radioactive substance and an important component in the manufacturing of armor-piercing weapons.

In January, Georgia's security service said it had foiled a plot to sell radioactive cesium. The agency said three men were arrested in the capital Tbilisi for trying to peddle Cesium-137 for \$100,000.

Cesium-137, obtained as a by-product from nuclear reactors, can be utilized for medical and industrial purposes. However, it can also potentially be used by terrorists who want to create a dirty bomb as it would disperse deadly radiation after detonation.

Uranium-238 is the most common natural uranium isotope. Although it can't undergo a nuclear chain reaction, it can be used to produce plutonium 239, which can be exploited for the production of nuclear weapons.

What we learned from Chernobyl about how radiation affects our bodies

By Ausrele Kesminiene

Source: <http://www.homelandsecuritynewswire.com/dr20160428-what-we-learned-from-chernobyl-about-how-radiation-affects-our-bodies>

Apr 28 – The world has never seen a nuclear accident as severe as the one that unfolded when a reactor exploded in Chernobyl on 26 April 1986, sending vast amounts of radiation into the skies around Ukraine, Belarus and Russia.

The planet had experienced massive releases like this before, in the bombings of Hiroshima and Nagasaki in 1945. But Chernobyl-related radiation exposure had a more protracted character.

It was the first time in history that such a large population, particularly at a very young age, was exposed to radioactive isotopes, namely iodine-131 and cesium-137, not just through direct exposure, but through eating contaminated food as well.

In 2006, the International Agency for Research on Cancer (IARC) [published estimates](#) of how many excess cancers would occur as a result of this contamination.

While noting that these estimates are subject to substantial uncertainty, the authors found that **1,000 cases of thyroid cancer and 4,000 cases of other cancers had already been caused by the accident.** They further estimated that by 2065, 16,000 cases of thyroid cancer and 25,000 cases of other cancers could be attributed to the effects of Chernobyl radiation.

Research on the health impact of the Chernobyl disaster has mainly focused on [thyroid cancer](#), in particular in those exposed to radioactive iodine isotopes in childhood and

adolescence. Large amounts of iodine-131 were released into the atmosphere after the explosion, and children were exposed by consuming locally produced milk and vegetables.

Efforts were made to better understand the mechanisms of radiation-induced thyroid cancer and which factors could modify the radiation risk. This allowed us to identify a molecular "radiation fingerprint", which can point to changes that are specific to radiation exposure, as opposed to any other factors.

Studies were also conducted to evaluate the risk of [haematological malignancies](#)— tumors that affect the blood, bone marrow, lymph, and lymphatic system – in children and Chernobyl clean-up workers in the three most affected countries. Studies of cancer incidence and mortality, [cardiovascular diseases](#) and all-cause mortality were also conducted on clean-up workers. Although of variable quality, the list of studies done on people affected by the blast is long.

What we found

Today, there is an overall agreement among scientist that thyroid cancers increased following exposure to radiation in childhood and adolescence. Several studies have also indicated an increase in [haematological malignancies](#) and thyroid cancer in Chernobyl clean-up workers.

[Findings](#) on radiation-associated risk both for chronic lymphocytic leukemia



CBRNE-TERRORISM NEWSLETTER – February 2016

and other types of leukemia in clean-up workers were reported in 2013. Before then, chronic lymphocytic leukemia was not considered to be sensitive to radiation. Further research will be required to confirm these findings.

Some studies focused on non-cancer health consequences of exposure to radiation. [Convincing results](#) on eye lens cataracts among Chernobyl clean-up workers led to the revision and considerable reduction in the recommended radiation dose limit for the lens of the eye.

Chernobyl also led to a greater knowledge on optimizing treatment and follow-up of survivors of [acute radiation sickness](#). A better understanding of thyroid cancer radiation risks allowed us to respond better to other disasters, such as Fukushima, to minimize potential adverse health consequences.

What we still don't know

Despite these important findings, many grey areas still remain. For example, we still have no convincing evidence for childhood leukemia associated with Chernobyl. It is unclear if this is due to methodological limitations or for other reasons.

Nor do we know how radiation risk changes over time after a someone is exposed as a child, as a longer follow-up study is required. We also don't yet understand the potential transgenerational affects on children born to exposed parents.

The need for more research is immense, yet funding is declining. We need a sustainable approach to Chernobyl health research – similar to that taken after the [Hiroshima and Nagasaki bombings in Japan](#). Without this, it is unlikely that the true impact of Chernobyl will ever be fully understood.

Ausrele Kesminiene is Deputy Section Head Section of Environment and Radiation at IARC, International Agency for Research on Cancer (IARC).

Should you buy iodine pills?

By Stephen Bryen

Source: <http://acdemocracy.org/>

Growing nuclear proliferation global radical Islamist terror network has raised the possibility of nuclear terror attacks, including potential sabotage of nuclear facilities, as well as the use of conventional explosives to disperse radioactive material (dirty bomb).

Investigations after recent attacks in Belgium and France revealed the Islamist terrorists plans to attack nuclear reactor sites and associated laboratories, and that many facilities have been already penetrated by Jihadists. Incredibly, there is virtually no available evidence that suggests such threats have been removed. Instead, **Belgium and Holland have now ordered iodine pills for their entire populations.**

Why all of a sudden are they buying up such large supplies of these pills?

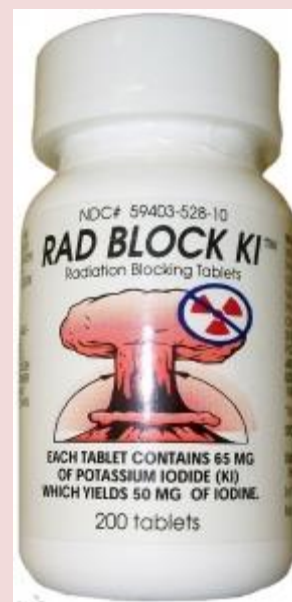
The reason for buying iodine pills is the danger of a nuclear accident, caused either by technical failure or a natural event such as an earthquake, tidal wave or flooding like what caused the still-continuing Fukushima crisis. [The Max Planck Institute for Chemistry in Mainz](#) has calculated that such events may

occur every 10 to 20 years, some 200 times more than earlier estimates.

When a nuclear reactor incident occurs, a variety of radioactive poisons are released, some of which become airborne and the rest contaminate the earth and underground and surface water sources.

The typical radioactive fallout includes radioactive iodine (I131, I132), Cesium (Cs137, Cs134) and Tellurium (Te132).

Radioactive iodine is a major uranium and plutonium fission product. It has a half-life of a little more than



CBRNE-TERRORISM NEWSLETTER – February 2016

eight days, and it is the greatest immediate threat to populations near a nuclear reactor or nuclear storage site. (The other nuclear contaminants can last from hundreds to thousands of years!)

The human thyroid will rapidly absorb radioactive iodine, which can immediately cause severe radiation sickness and leading to a variety of cancers starting with thyroid cancer. However, if the thyroid is pre-treated with non-radioactive iodide salts, it will have no room to absorb radioactive iodine. Consequently, the best defense against radioactive iodine caused by a nuclear "event" is either a potassium iodide pill or liquid that can be rapidly administered before an individual has been exposed to radioactive iodine. These pills and liquids (for infants and the elderly) are what the Department of Homeland Security and the Europeans are stockpiling.

One of the earliest and worst nuclear accidents was at the secret reactor built by the Russians to produce plutonium for nuclear weapons. Called the **Mayak ("Lighthouse") reactor** (similar to the US Hanford site, which [remains highly contaminated](#)), it was built between 1945 and 1948 and was prone to multiple accidents. The worst happened on September 27th, 1957 when a storage tank located at [Kyshtym exploded](#). The Russians told no one, and information about the disaster only became available in 1979, twenty-two years later. The explosion of the storage tank destroyed more than two dozen villages and contaminated a


vast area, rendering Lake Irtysh and the [Techa River](#) unusable and exposing more than 470,000 people to radiation.

The **Fukushima accident** involved three nuclear meltdowns; **Chernobyl** one. Both caused long-term population evacuations and no-go areas. The Chernobyl area has been [closed off for thirty years](#). Fukushima may have convinced the Germans to consider shutting down nuclear reactors (there are 8 in Germany), and the [Italians to reverse a decision to go back into the reactor business](#).

In the United States, the worst nuclear accident reported was, of course, **Three Mile Island** (1979) near Harrisburg, Pennsylvania. Since then we are repeatedly told that the country's civilian and military nuclear facilities present no danger to the population because the best security measures are in place to prevent malfunction and to guard against intruders.

But accidents happen. If a reactor failure occurs in Maryland or Virginia, for example, it would create a massive crisis as people scramble to try to get their hands on iodine pills. It would be even worse if a dirty bomb hits New York City or downtown Washington DC.

While the Department of Homeland Security (DHS) purchased [14 million iodine pills](#) in 2014, many questions arise whether governments are capable of rapidly distributing the pills and liquids they have purchased. In Israel, which is under constant chemical, biological and nuclear threats, [kits are pre-distributed](#) and renewed on a regular basis.



The following steps are necessary to prevent nuclear terrorism and protect civilian populations against radiation disasters:

First – Securing nuclear facilities and the area around them. Bringing-in competent and powerful forces to guard the facilities against external attack and removing potential security risks inside. In the U.S., the National Guard may be called to protect the perimeter of nuclear sites, and the FBI to vet employees and validate security systems. In Europe, it means using NATO forces for perimeter protection and Interpol to check internal security and validate employees. Law-enforcement agencies should have the authority to remove anyone suspected of any connection to radical Islamic groups.

Second – Setting up a distribution system of response toolkits - using the Israeli model - for people living in the vicinity of nuclear installations and sensitive urban areas under threat; Ensuring ready-supply of potassium iodine in the hands of businesses and families now, not after a terrorist strike.

Third – Fighting to extinguish the jihadist movement and its terrorists abroad before they reach American soil and using whatever deterrence necessary to discourage sympathizers at home. The European's wimpy approach to and accommodation of radical Islam resulted in growing attacks and penetration of nuclear facilities. The U.S. isn't much better. To prevent the spread of the Islamic terrorism, radical Islamic movements and Muslims associated with them should be acknowledged as an existential threat and treated accordingly. Called the "Big Satan" by radical Shiite and Sunni Muslims alike, America should take all necessary steps to prevent the Islamist terrorist threat.

CBRNE-TERRORISM NEWSLETTER – February 2016

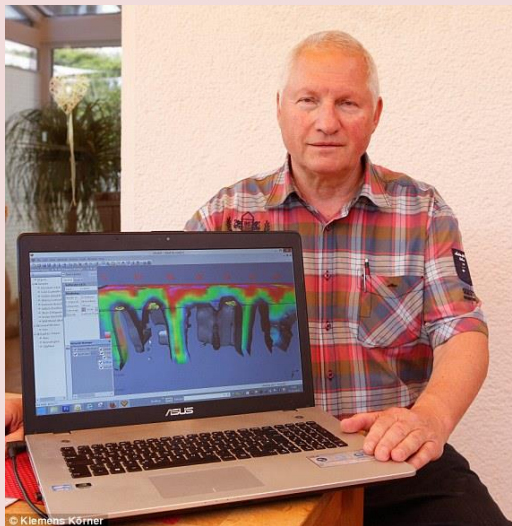
In the meantime, if you live anywhere near a nuclear reactor, especially if you live or work downwind from a reactor you should consider buying Potassium Iodide (Iodine) tablets for yourself and your family. They are readily available in the U.S. for individual purchase on the open market without a prescription. Check out the [CDC website](#) and consult your physician before ordering radiation toolkits and iodine pills.

Dr. Stephen Bryen is the former Director of the Defense Technology Security Administration and a fellow of the American Center for Democracy. Some parts of this article are from his new book, [Technology Security and National Power: Winners and Losers](#) (Transaction Publishers).

Engineer claims he has found Adolf Hitler's secret NUCLEAR BOMBS in a German cave and warns 'if they decay we could have another Chernobyl on our hands'

Source: <http://www.dailymail.co.uk/news/article-3594579/Engineer-claims-Adolf-Hitler-s-secret-NUCLEAR-BOMBS-German-cave-warns-decay-Chernobyl-hands.html>

May 17 – A pensioner claims he has found Adolf Hitler's secret atom bombs inside tunnels dug by the Nazis underneath a mountain valley in central Germany.



Peter Lohr, 70, claims to have found five large metal objects in a cave in the Jonas Valley in Thuringia state, of which at least two are 'atomic bombs'.

Mr Lohr is certain that the objects are weapons of mass destruction manufactured by the Nazis towards the end of the Second World War.

'Proof': Peter Lohr, 70, shows the result of his 3D radar research in the Jonas Valley, which he claims shows five large metal objects in a cave, of which at least two are 'atomic bombs'

The former mechanical engineer claims the shape of the objects match that of a nuclear bomb, The Local reports.

Using a radar with 3D technology, Mr Lohr claims to be able to prove that the objects are atomic bombs, warning that they could cause a nuclear disaster.

'The metal's been lying there for 71 years. At some point it will decay and then we will have a second Chernobyl on our hands' he said.



CBRNE-TERRORISM NEWSLETTER – February 2016



The centre of the Jonas Valley was a scene of secret military construction towards the end of the Second World War, with thousands of concentration camp prisoners forced to dig tunnels under the mountains. It is not known what purpose the tunnels were meant to have as it was never completed.

Sure thing: Mr Lohr is certain that the objects are weapons of mass destruction manufactured by the Nazis towards the end of the Second World War

The tunnel system stretches for miles underneath the mountain, with thousands of caves, bunkers and storerooms, and it is believed that it was intended to be the Alamo of the Third Reich leadership.

The Jonas Valley was liberated by American troops in April 1945, and US authorities have since classified all 1945 documents relating to Ohrdruf for a minimum of 100 years.

This is not the first time rumours of a Nazi nuclear bomb has surfaced.

Last year, a documentary called 'The Search for Hitler's Atom Bomb,' quotes sealed records from Russia and America said to prove the Nazis were close to creating a weapon of mass destruction.

The programme quoted interrogation reports of Nazi scientists, eyewitness account and the records left behind by researchers, many of which were shipped to America after the war.





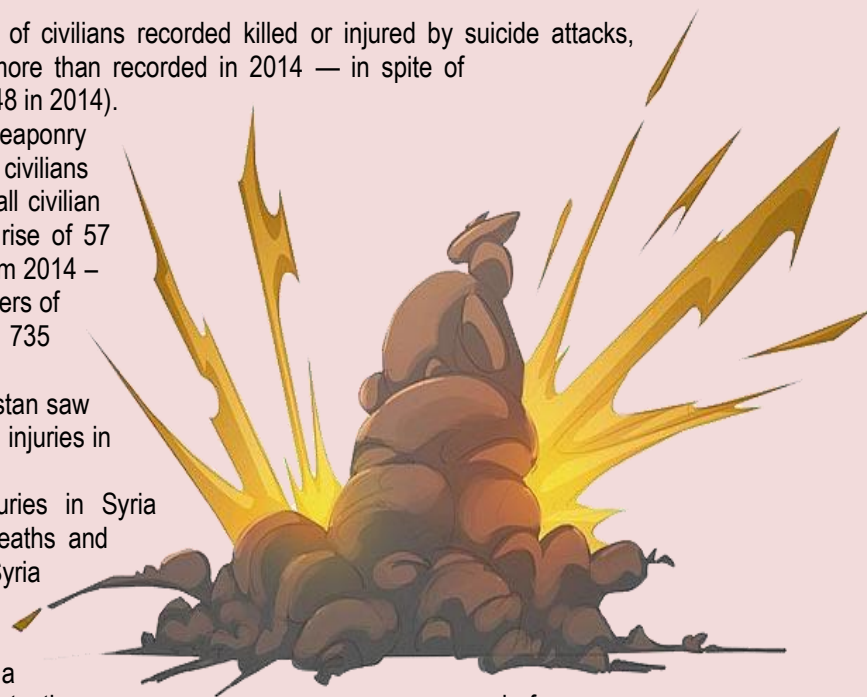
Number of civilian casualties from explosives around the world continues to grow

Source: <http://www.homelandsecuritynewswire.com/dr20160427-number-of-civilian-casualties-from-explosives-around-the-world-continues-to-grow>

Apr 27 – For the fourth year in a row, 2015 saw a rise in the number of civilian casualties from explosive violence around the world. In [Unacceptable Harm, Action on Armed Violence](#) (AOAV) has recorded 33,307 civilians having been killed or injured by explosive weapons – up 2 percent from 2014, and 54 percent more than when AOA's monitor began in 2011.

AOAV says that the key findings of the report are:

- AOA recorded 43,786 deaths and injuries by explosive weapons in 2,170 incidents in 2015. Of these, 33,307 were civilians – 76 percent.
- When explosive weapons were used in populated areas, 92 percent of those killed and injured were civilians. This compares to 31 percent in other areas.
- Civilian deaths and injuries in populated areas represented 89 percent of all reported civilian deaths and injuries.
- Civilian deaths and injuries rose by 2 percent in 2015 from 2014. This is the fourth consecutive year in which recorded civilian casualties of explosive violence have increased. In 2011, 21,499 civilians were killed or injured.
- There was a sharp rise in the number of civilians recorded killed or injured by suicide attacks, reaching 9,205. This was 67 percent more than recorded in 2014 — in spite of similar incident numbers (253 in 2015, 248 in 2014).
- Incidents caused by air-launched weaponry killed and injured a reported 9,200 civilians worldwide, accounting for 28 percent of all civilian deaths and injuries. This represents a rise of 57 percent in civilian deaths and injuries from 2014 – in spite of a 32 percent drop in the numbers of incidents recorded (501 in 2015, 735 in 2014).
- Syria, Yemen, Iraq, Nigeria, and Afghanistan saw the highest number of civilian deaths and injuries in 2015.
- Numbers of reported deaths and injuries in Syria continued to rise. More than 10,000 deaths and injuries were recorded by AOA in Syria in 2015.
- A number of countries saw a significant rise in civilian deaths and injuries as a result of explosive weapons compared to the year before: Turkey (7682 percent), Yemen (1204 percent), Egypt (142 percent), Libya (85 percent), Syria (39 percent), and Nigeria (22 percent).
- Six countries and territories had over 1,000 civilian deaths and injuries in 2015.
- Incidents were recorded in sixty-four countries and territories around the world – five more countries than in 2014. In 23 of these countries no incidents were recorded in 2014.
- Despite this increase in deaths and injuries, there was a 20 percent decrease in the number of recorded explosive weapon incidents compared to 2014. This means there was a higher average lethality than previous years – a reflection of the increasing use of explosive weapons deliberately targeting populated areas. In 2014 AOA had recorded 41,847 deaths and injuries from 2,702 incidents.



— Read more in [Unacceptable Harm – Monitoring Explosive Violence in 2015](#) (AOAV, April 2016).



'Bomb scare' leaves Man Utd red faced as Bournemouth clash is pushed back to Tuesday night

Source: <http://www.telegraph.co.uk/football/2016/05/15/bomb-scare-leaves-man-utd-red-faced-as-bournemouth-clash-is-push/>

May 15 – A farcical security blunder led to Manchester United's final Premier League game of the season being cancelled after a private security firm forgot to remove a fake



bomb taped to the back of a toilet door as part of a training exercise at Old Trafford.

The colossal error had sparked fears of another potential terrorist attack and resulted in the match against Bournemouth being called off as tens of thousands of fans were evacuated from one of the world's most famous sports grounds.

A bomb disposal unit carried out a controlled explosion after what had been described as a fake but "incredibly lifelike" bomb was

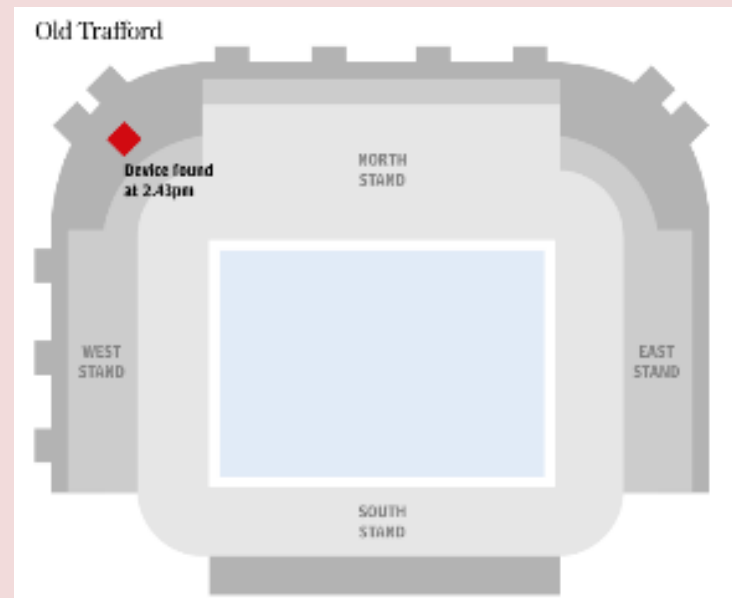


discovered in the north west quadrant at Old Trafford in the run up to kick-off of a game attended by around 76,000 fans.

But it later emerged during an investigation by Greater Manchester Police (GMP) that the

dummy device had been left by an external company following a training drill involving sniffer dogs. It is thought that the company responsible only owned up to the blunder after being contacted by officers.

Tony Lloyd, Greater Manchester's Police and Crime Commissioner, condemned the incident as "outrageous" and a "fiasco" and demanded a full inquiry into an "unacceptable" situation that he claimed put people in "unnecessary



danger" and proved a waste of police time and resources. Ander Herrera, the United midfielder, said the mood had been "very tense" in the dressing room and that players were "nervous" about the events unfolding.

This was the first time in 24 years that a Premier League match has been cancelled on security grounds and provided a dramatic, disturbing and ultimately embarrassing end to one of the most unpredictable top flight seasons in memory.

Ed Woodward, the United executive vice chairman, said a full investigation would be launched with senior sources at the club admitting there was "anger" that such a situation had arisen. It remains to be seen if the security company at the centre of



CBRNE-TERRORISM NEWSLETTER – May 2016

the controversy has its contract with United cancelled and what compensation claims may follow.

The Premier League announced on Sunday that the fixture had been rescheduled for 8pm on Tuesday night following talks between senior officials from United and Bournemouth



and GMP. United and Bournemouth will provide fans with a full refund and provide free entry to the game on Tuesday night. Bournemouth supporters had made a 500-mile round trip for no reason in the end. Refunding fans is likely to cost United £3m.

Tens of thousands of supporters in the Sir Alex Ferguson Stand and Stretford End started being evacuated around 20 minutes before the match was due to kick-off, with United formally announcing over the stadium PA system that the game was off at 3.19pm. At that point, fans in the north and east stands were evacuated as part of a careful strategy to avoid any crushes and disperse people safely. Both teams are thought to have remained in their dressing rooms for about 40 minutes before being moved to an executive suite where they mingled.

Some United players are believed to have watched Manchester City's game at Swansea City live on television with their local rival's 1-1 draw at the Liberty Stadium effectively ending any hopes Louis van Gaal had of finishing in the top four and damaging his prospects of keeping his job.

Army bomb disposal experts carried out a controlled explosion of the suspect package, which had been discovered by a member of United's staff.

GMP said a detailed examination of the package, which is thought to have consisted of a mobile phone taped to the back of a toilet door, was not "viable" as a full search of Old Trafford continued to check no other devices had been planted.

But John O'Hare, assistant chief constable of

GMP, later admitted that the item was "a training device which had accidentally been left by a private company following a training exercise involving explosive search dogs."

He added: "Whilst this item did not turn out to be a viable explosive device, on appearance this device was as real as could be, and the decision to evacuate

the stadium was the right thing to do, until we could be sure that people were not at risk."

Lloyd reacted furiously to the news. "It is outrageous this situation arose and a full inquiry is required to urgently find out how this happened, why it happened and who will be held accountable," he said.

"This fiasco caused massive inconvenience to supporters who had come from far and wide to watch the match, wasted the time of huge numbers of police officers and the army's bomb squad, and unnecessarily put people in danger, as evacuating tens of thousands of people from a football stadium is not without risk.

"Whilst this in no way demeans the professionalism of the police and stewards responsible for getting the fans out, or the supporters' calmness and cooperation during the evacuation, it is unacceptable that it happened in the first place."

United will have to beat Bournemouth on Tuesday by 19 clear goals to guarantee Champions League qualification but the best the club can realistically hope for is a place in next season's Europa League. A point against Bournemouth or victory in the FA Cup final against Crystal Palace on Saturday would secure entry into the Europa League group stage.

But United face the nightmare scenario of having to negotiate a



CBRNE-TERRORISM NEWSLETTER – May 2016

two-legged Europa League third qualifying round tie in late July and early August in the event they are beaten by Bournemouth to finish sixth in the Premier League, behind Southampton on goal difference, and lose to Palace on Saturday.

The first leg would be on July 28, which could scupper part or all of their planned pre-season tour to China, where they are due to face

Borussia Dortmund in Shanghai on July 22 and Manchester City in Beijing three days later. It would also put Wayne Rooney's testimonial under threat.

Although no date has been confirmed for that game against Everton, it had been tentatively scheduled for Aug 3 – a day before the second leg of a potential Europa League third qualifying tie.

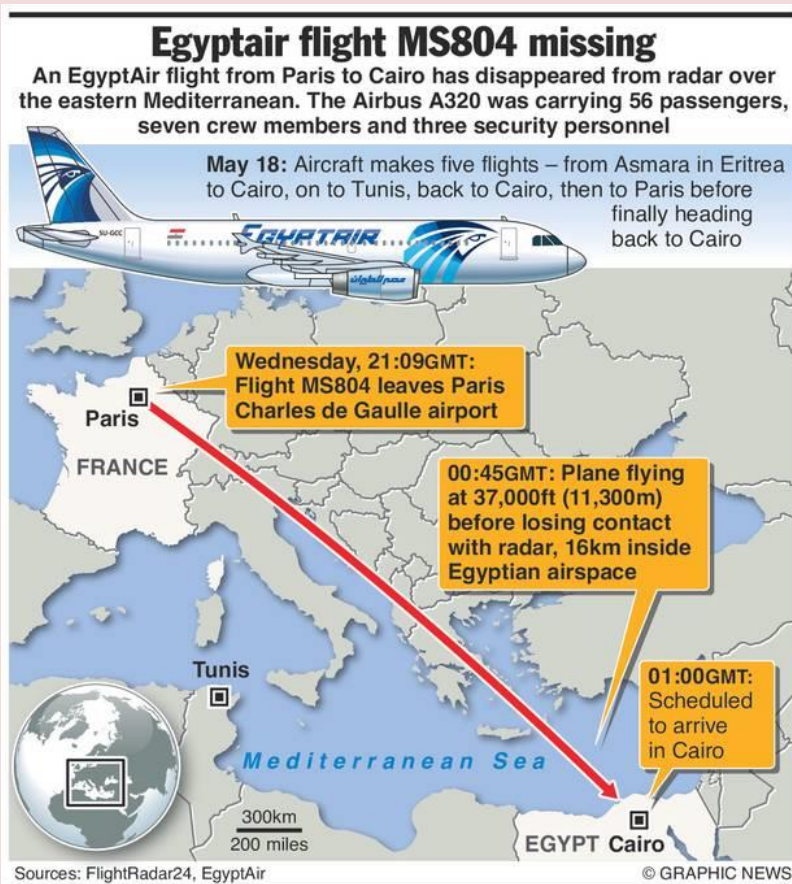
EDITOR'S COMMENT: When a surgery ends, OR head nurse counts all the medical items used to see if there is anything forgotten inside the patient. Similar procedures should be applied to terrorism drills when mock devices are used. This is the second time that recently such a thing happens – remember the forgotten "bomb" in a school bus in the US? These are human errors that can cause lives and money for no apparent reason!



Missing EgyptAir Flight Sparks Search for Clues

Source: <https://www.stratfor.com/analysis/missing-egyptair-flight-sparks-search-clues>

May 19 – An EgyptAir flight traveling from Paris to Cairo went missing in the early hours of May 19 about 16 kilometers (10 miles) into Egyptian airspace, according to information released by the airline. The Airbus A320 was reportedly flying just under 37,000 feet at the time it disappeared from radar. A company official said the pilots did not make a distress call or indicate any trouble ahead of the plane's disappearance.



Mechanical failure at cruising altitude is unlikely — such an event typically occurs at takeoff or landing, when stress on the aircraft is at its highest. Catastrophic failure of the airframe cannot be ruled out. A surface-to-air missile strike is also possible, though militants in Egypt and surrounding areas are not believed to have access to missiles capable of hitting an aircraft at that altitude.

Detonation of an improvised explosive device is a more obvious possibility. Unlike the bombing of Metrojet Flight 9268 from the Sinai city of Sharm el-Sheikh in October 2015, however, EgyptAir Flight 804 originated in Paris. Security measures at Charles de Gaulle Airport are stringent compared with those of many other airports, and security has been raised since the recent attacks in Paris and Brussels. But even a relatively small and unsophisticated IED in either the passenger cabin or the cargo hold could significantly damage a plane at cruising altitude and lead to flight complications. Inside assistance contributed to the success of the Metrojet 9268 bombing, and if the

- 30 Egyptian
- 15 French
- 2 Iraqi
- 1 British
- 1 Belgian
- 1 Kuwaiti
- 1 Saudi
- 1 Sudanese
- 1 Chadian
- 1 Portuguese
- 1 Algerian
- 1 Canadian

cause of this flight's disappearance was an attack rather than an accident, **some degree of insider involvement is likely.** A cargo handler (as in the Metrojet case), a crew member, or even a pilot (as in the 1999 EgyptAir Flight 990 crash or the March 2015 Germanwings Flight 9525 crash) could have been involved.



CBRNE-TERRORISM NEWSLETTER – May 2016

The Egyptian government's civil aviation authority has reportedly sent search and rescue teams to determine more. Once the plane is located, its condition will be key to determining what caused its disappearance. An electrical failure, for instance, would likely enable pilots to glide the plane toward the ground and prevent a catastrophic disintegration, meaning the debris field would be small. An intentional crash would also leave a small debris field. An IED or projectile, on the other hand, would cause a catastrophic breakup of the aircraft — especially considering the plane's high altitude — and the debris field would be much wider.

EDITOR'S COMMENT: There will be a lot of scenarios about the causes – some mentioned in this article. Could it be a stolen FIM-92 Stinger (1996 version: range of 26,000 feet (7,900 m) fired from a cargo ship in the Med Sea? An air-to-air missile is almost impossible to go undetected in this area at this time of the year (you know why). The IED hypo is the most realistic one. There is an estimate that the plane crashed in one of the deepest locations of the Med Sea. The eastern Med basin is longer and deeper. The deepest part of the Mediterranean Sea is the 5121 metres of the Matapan trench in the Ionian Sea, south of Peloponnisos. This makes it even deeper than the faults in the Atlantic ocean. The eastern basin has a bigger continental shelf than the western basin, mainly in the Adriatic and Aegean Seas. The south-eastern edge of the biggest basin (Levantine) runs alongside the continental shelf off the mouth of the Nile, north of Egypt. If the latter is the final crash point (south-east of Crete Island), then it would be extremely difficult – if impossible – to recover the pieces of the plane for forensic examination. Was that a coincidence as well? Unless it is another case of flight 9525 of Lufthansa Germanwings (March 2015).

UPDATE (May 21, 2016)



Saab Tackles Maritime IED Threat with 'Sea Wasp'

Source: <http://www.hstoday.us/single-article/saab-tackles-maritime-ied-threat-with-sea-wasp/5c90683fa87b541a6597bcc06b286716.html>

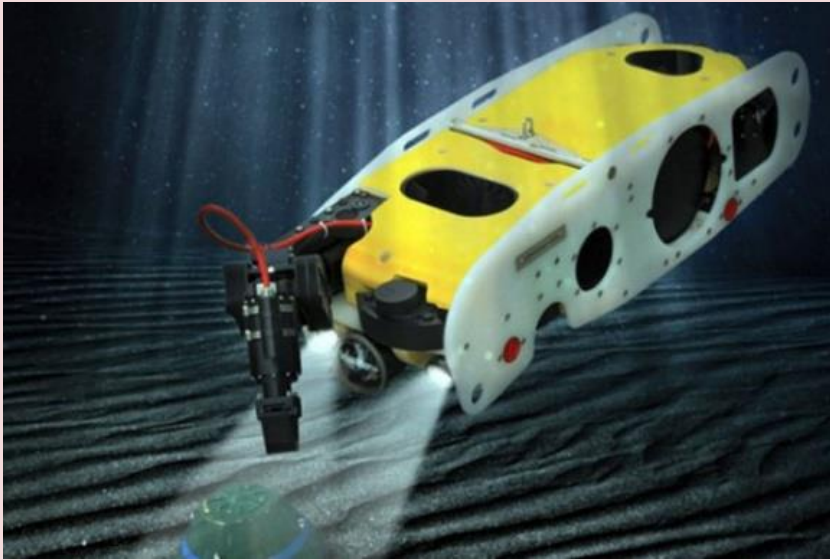
May 16 – The underwater improvised explosive device (IED) represents an increasingly pernicious threat within the maritime domain. An attack on the nation's ports and harbors using an underwater IED would have a crippling impact on the economic health and security of the nation.

Consequently, government and industry are researching and developing innovative solutions to deter, detect and interdict potential security threats to US ports. One such solution is Saab's Sea Wasp, a remotely operated vehicle (ROV) designed for disarming underwater IEDs.



CBRNE-TERRORISM NEWSLETTER – May 2016

Defense and security company Saab presented the Sea Wasp at the Navy League's



Sea-Air-Space Exposition in National Harbor, Maryland on May 16.

Jon Kaufmann, Vice President of Naval Programs at Saab North America, Inc., told *Homeland Security Today* that Saab developed the Sea Wasp to counter the emerging threat of IEDs in ports and harbors.



"In the United States, there are a number of targets in the port and harbor environments, such as ships and the cruise line industry," said Kaufmann. "Nothing really bad has happened yet—and hopefully it won't—but if it does the Department of Defense's Combating Terrorism Technical Support Office (CTTSO) is looking for how they might deal with it."

Developed over a period of 18 months in collaboration with the US Underwater Hazardous Device Team, the Sea Wasp is the latest generation Saab ROV. The vehicle is piloted from the surface using a control console onboard a support vessel or from a control vehicle at a beach or harbor.

In designing the Sea Wasp, Saab aimed to take humans out of the threat situation. Kaufmann said that up until this point, a small ROV with a camera could be used to

potentially locate an IED, and then an Explosive Ordnance Disposal (EOD) diver could go in and remove or disable the device.

"If you saw something with the camera on the ROV and felt strongly it was an IED, the last thing you would want to do is put a person in close proximity," Kaufmann explained. "So the genesis of this project was really to do what we have been doing on land with IEDs for the past 15 to 20 years, and that is to use a robot to approach IEDs whenever possible."

Although more challenging in the water than on land, advancements over the past

decade have brought ROV capabilities up significantly. Saab's Sea Wasp is operated remotely by two-person teams, allowing for a safe distance between operators and IEDs.

The vehicle features a five-function manipulator arm, which allows the operator to use a wide range of tools and techniques to disarm an IED. Additionally, it has high maneuverability, as well as the ability to hover, allowing the operator to lock the position of the vehicle and focus on using the manipulator arm without having to worry about the vehicle's position.

The vehicle's six thrusters provide enough



power to operate in harsh conditions, including tidal currents of up to 2.5 knots. It has a maximum operating depth of 60 meters.

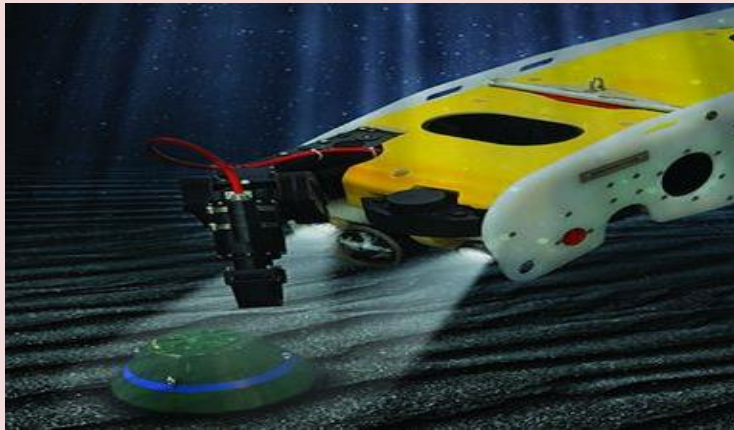
"The strength of this vehicle's design is the thrust to weight ratio, the ability to hover, and the manipulator arm, which features an elbow and wrist. It can unscrew things, cut things, attach things, pick them up and move them," said Kaufmann.

Saab has partnered with CTTSO in providing Sea Wasp prototypes to three EOD agencies: the US



CBRNE-TERRORISM NEWSLETTER – May 2016

Navy EOD Group 2, the FBI Counter-IED Unit, and the South Carolina Law Enforcement



Division's Counter-Terrorist Operations Maritime Response Unit.

In January 2016, representatives of these agencies met with a team of Saab employees from the United States, Sweden and the UK for four days of Sea Wasp training in Charleston,

South Carolina. The Charleston Law Enforcement Training Center's waterside location provided a perfect training setting, testing the vehicle's maneuverability in the challenging harborside environment.

Since then, the agencies have been testing the Sea Wasp prototypes. Kaufmann said the company has already received some feedback and come up with a second generation of software, which will increase the voltage of the thrusters, allowing

for an even higher thrust to weight ratio.

"The US unmanned underwater vehicle market is very important for Saab," said Kaufmann.

"Our goal with Sea Wasp is to meet US national security needs with an underwater, anti-IED device that keeps EOD teams safe."

Explosive Environments – the Israeli Challenge

By Ilan Cohen, ITL CTO

Source: <http://i-hls.com/2016/05/explosive-environments-the-israeli-challenge/>



May 19 – Two decades ago Israel was not a player in the explosive environment arena. There was some minimal activity in the military industry to comply with military standards for "MIL" products only.

Natural Gas finding, a number of Israeli regulator decisions and the accreditation of labs and inspection bodies placed Israel on a new track. Now the Industry must provide approvals and must be assessed and certified in order to be regarded as a safe environment for explosive atmospheres.

In Israel a number of major milestones defined the way we deal and comply with explosive environments:

- Global standards adoption- Based on a decision by ministry of economy, during the time Naftali Benet was the minster, it was decided that when an international standard exist it needs to be adopted. Original Israeli standards will not be written when there is a globally acceptable standard like IEC or ISO.



CBRNE-TERRORISM NEWSLETTER – May 2016

- Umbrella Standards – in order to regulate the usage and implementation of global standards a number of Umbrella standards were written. These are similar to European directives (for example ATEX directive) and their goal is to create a framework of regulations and procedures. The Umbrella Standards do not replace the International standards of ISO and IEC.
- IECEx approvals – Israel Testing Laboratories (I.T.L.) was accredited as a Test Lab and a Certification body for products for Explosive environment and the inspector for factories that manufacture products for explosive environment. This is a service that was provided by International labs like Veritas, DNV, Intertek, TUV and is provided now locally by ITL.

Milestones which are under work:

- Inspection Bodies framework- the regulator, the Ministry of Energy, is leading an umbrella standard to inspect factories and facilities which are supplied with Natural Gas.
- Household Gas supply- There is a preliminary discussion on creating a framework and to regulate the household safety.

On one hand, implantation of the new milestones was not simple. The industry is not easily ready to adopt, make changes and to align with global requirements. We can take for example the Israeli Electrical company (חברת החשמל), ICL (כיל), Phoenicia (פניציה). These companies have made major investment in the past in equipment and facilities that were approved to arbitrary requirements which we can only hope are safely done.

On the other hand, Israeli leading R&D industry is making products for local markets and global export. Products like controllers, blowers, measuring equipment, gasoline stations systems which require approvals like: IECEx, ATEX and similar. These products can be fully tested and inspected by Israel Testing Laboratories (I.T.L) which was approved on 2015 for this by the IECEx and the Ministry of Economy.

There is still a way to go in order to make our environment safe and to regulate additional areas. Nevertheless the train has left the station and it looks like we are on the right track of adopting globally used standards, regulations and procedures to make our environment safer.



Pentagon “dropping cyberbombs” on ISIS

Source: <http://www.homelandsecuritynewswire.com/dr20160426-pentagon-dropping-cyberbombs-on-isis>

Apr 26 – Deputy Secretary of Defense Robert Work has said that the U.S. military is “dropping cyberbombs” on ISIS.

Earlier this month, Defense Secretary Ashton Carter announced that the U.S. Cyber Command had been given its “first wartime assignment” – attacking and disrupting ISIS cyber infrastructure.

Not much is known about the operations of the Cyber Command, which was created in 2009 and which is located near the NSA headquarters in Fort Meade, Maryland.

CNN reports that in the last few months, the Pentagon has allowed more information to be published about the U.S. military’s cyberwar against ISIS. Work, describing the Cyber Command’s operations at a news conference, said: “We are dropping cyberbombs. We have never done that before.”

Work added: “Just like we have an air campaign, I want to have a cyber campaign. I want to use all the space capabilities I have.”

The U.S. cyber campaign against ISIS has so far focused mostly on disrupting ISIS communications systems, on which the Islamist militants rely to spread their message, recruit new fighters and organize attacks.

Cyberattacks have also been used to disrupt ISIS finances.

Some in the intelligence community have expressed their worry that successful cyberattacks against ISIS could force the organization to go underground and adopt more low-tech alternatives – making it more difficult for Western intelligence to track and target the militants.

Carter has said, however, that this may well be a blessing in disguise. At a February briefing, he said: “As we disrupt the Isis communications via cyber or other methods, sometimes we do drive them to other means. But it cuts both ways. Sometimes, those other means are easier for us to listen to.”

“So by taking away some of the ways that they are used to operating, they’re protected and that they regard as an information sanctuary, drives them to other, including older technologies.”

“So one way or another, it is a very effective tool.”

FBI does not know how the \$1m iPhone hack works

Source: <http://www.homelandsecuritynewswire.com/dr20160429-fbi-does-not-know-how-the-1m-iphone-hack-works>

Apr 29 – **U.S. government sources told Reuters that the FBI does not know how the hack which was used to unlock the San Bernardino terrorist’s iPhone 5C works, even though the agency paid about \$1 million for the technique. The mechanism can be employed to unlock any other iPhone 5C running iOS 9.**

The *Wall Street Journal* reports that the hack was bought from professional hackers, and that the amount the agency paid for it was less than earlier reports which talked of more than \$1.3 million.

The sources told the news agency that the FBI can use the technique any time it wants without further payments.

FBI director James Comey said last week that the agency paid more to get into the iPhone 5C than he will make in the remaining seven years and four months he has in his job. **Based on the director’s salary, journalists calculated that this means the hack cost more than \$1.3 million.**

After the FBI, in March, unlocked the iPhone, the agency withdrew its request that a court force Apple to create software to unlock the iPhone 5C.

The *Journal* says that the FBI bought a physical mechanism used to unlock the phone, but does not know the details of the hack which makes it work. The identity of the hackers who sold the technique to the agency is a closely guarded secret, and the FBI director himself does not know who they are.

The FBI said it would not tell Apple about the security flaw which the hacking technique exploits, not only because the FBI wants to be able to hack future phones, but also because the agency does not know how the hack works.



Islamic State-linked hackers post target list of New Yorkers

Source: <http://www.reuters.com/article/us-new-york-islamic-state-idUSKCN0XQ2AC>

Apr 29 – A group of hackers linked to Islamic State has posted online a list of thousands of New York residents and urged followers of the militant group to target them, according to a source with knowledge of the matter.

Federal agents and New York City police officers have been contacting the individuals on the list to inform them of the posting, but the source said law enforcement does not believe there is any credible threat.

In a statement, the Federal Bureau of Investigation said, "While our standard practice is to decline comment on specific operational and investigative matters, the FBI routinely notifies individuals and organizations of information collected during the course of an investigation that may be perceived as potentially threatening in nature."

The list includes names, home addresses and email addresses. Some of the information appears to be outdated, according to the source, who was not authorized to discuss the investigation publicly.

Last year, an Islamic State-related group posted what it claimed were names, addresses and photos of 100 U.S. military service members and called upon followers to kill them.

The militant group controls swaths of territory in Syria and Iraq and has claimed responsibility for several major attacks in various countries, including coordinated attacks in Paris in November that killed 130 people.

U.S. authorities have arrested more than 70 individuals for attempting to support Islamic State since 2013.

ISIS developing Google-style driverless cars for attacks

Source: http://zeenews.india.com/news/world/isis-developing-google-style-driverless-cars-for-attacks_1881251.html



CBRNE-TERRORISM NEWSLETTER – May 2016

May 02 – **London: Islamic State (ISIS) technicians are working to develop a Google-style driverless car that could navigate itself into a crowded area before detonating an explosive device, a NATO security expert has warned.**

ISIS' research and development department in the terror group's de facto Syrian capital, Raqqa, is believed to be producing the vehicles at the same time as US Internet giant Google attempts to perfect the same technology.

If successful, the invention could prove to be a major headache for security services in Britain and throughout Europe and North America, where self-driving cars are expected to become commonplace, Daily Express reported.

Thousands of driverless cars are expected to be on Britain's roads within the next few years and there is a very real prospect jihadis could prey on the new technology to launch attacks in the UK.

Jamie Shea, NATO's deputy assistant secretary general for emerging security threats, said the Islamic extremists were using their bomb making factory in Raqqa to develop the technology.

He said ISIS was using its "technical expertise" to "play around" with driverless cars in a "worrying" development.

Shea said: "We are focusing very much on...Raqqa at the moment, where ISIL [ISIS] has its bomb making factory.

"It is not just Google that is producing the autonomous car, ISIS is also trying to do the same."

The technology would remove the need for suicide bombers and could help the death cult - also known by its Arabic acronym Daesh - cope with the dramatic drop in its numbers, which has seen its fighting force cut almost in half.

The FBI has long argued autonomous cars could be used by criminals as lethal weapons.

“Burner” phones, social media and online magazines: understanding the technology of terrorism

By Thomas Holt

Source: <http://www.homelandsecuritynewswire.com/dr20160502-burner-phones-social-media-and-online-magazines-understanding-the-technology-of-terrorism>

May 02 – Amid the global threat of terrorism, the actual attacks that occur can vary widely. Terrorists aim at different targets in different locations, and tend to be either shooting or bombing or both. There is, however, a central point of connection linking all these events: the use of technology to coordinate and organize the incident.

[Recent reporting](#) suggests that terrorists used “burner” phones, prepaid disposable mobile phones, to coordinate their actions during last year’s Paris terror attacks. **This is not a new or innovative tactic.** Drug dealers, street prostitutes and other criminal groups in the U.S. regularly use these devices for communication: they are cheap, plentiful and difficult to link to a real identity. Their value lies in real-time communication, via text or voice call, that needs no software nor even a computer to connect.

Having researched cybercrime and technology use among criminal populations for more than a decade, I have seen firsthand that throwaway phones are just one piece of the ever-widening

technological arsenal of extremists and terror groups of all kinds. Computers, smartphones and tablets also draw people into a movement, indoctrinate them and coordinate various parts of an attack, making technology a fundamental component of modern terrorism.

Attracting attention

Different resources and applications are pivotal at different phases in the process of radicalization to violence, and for good reason. For instance, social media platforms like Facebook, Twitter, Instagram, and Periscope give extremist groups a venue to attract individuals to join their movements.

Social media is especially effective for terrorist groups because it allows people to share and spread short messages, including text and images, in rapid bursts. With access from nearly any device, such as desktop or laptop computers and mobile phones — including burners — individuals can connect to larger networks of members



around the world. Those communities can then reinforce ideological beliefs and spin messages.

The Islamic State group has a significant presence on Twitter. It uses hundreds of thousands of user accounts to broadcast information about its activities on the ground in real time, as well as to attract individuals to the movement. There have been several examples over the last few years of young people being recruited into the Islamic State group via social media and encouraged to travel to join the fight.

Since social media posts are shared in near-real time, terror groups can also post messages to claim responsibility for a terror attack or act of violence. People who see it can share it with others, drawing attention to this news and giving these groups additional attention from people who might join their cause.

Engaging in discussion

Web forums are another important venue for information sharing, radicalization and recruitment. Forums are asynchronous, meaning posts made can be seen at any time – seconds, minutes or even days after being made. Forums also let individuals post lengthy messages with images, hyperlinks and text that may take more time to read and interpret. As a result, they are more conversational and lead people to participate over long periods of time. Forums are essential for long-term construction of shared cultures underlying extremist movements. They let people debate at length topics and minutiae of belief systems beyond what is possible on social media. In fact, one of the oldest web forums used by members of neo-Nazi and other radical far-right extremist groups in the United States, called Stormfront, has been in operation since 1996.

Individual websites also play an important role in the spread of information and radicalization because creators can tailor specific messages to audiences in ways that may not be readily contradicted. For instance, the racist group Stormwatch operates a website about civil rights leader Dr. Martin Luther King Jr. The site (martinlutherking.org) appears to be filled with biographical information, but in reality attacks King, questioning his motives and his morals. It also takes facts about his life and quotes from speeches out of context in an attempt to

undermine his role in the American civil rights movement.

In addition, websites allow groups to publish highly stylized media materials to support and promote their agendas. For example, *Inspire* magazine appears to be a lifestyle publication published in multiple languages, but is published by al-Qaida in the Arabian Peninsula to promote a jihadist agenda. Evidence suggests that the perpetrator of the San Bernardino terror attacks of 2015, Syed Rizwan Farook, and his neighbor would regularly consume radical jihadist media including *Inspire* magazine and online videos produced by al-Qaida's Somali branch, Al-Shabaab.

Planning and acting

Extremist groups can also use online information to plan their attacks. For instance, al-Qaida-linked actors allegedly used Google Earth in the run-up to their eventually failed attack against oil processing facilities in Yemen in 2006. Similarly, Google Earth maps were used by terrorists to navigate during the 2008 Mumbai attacks.

Once someone is radicalized and expresses willingness to travel to engage in foreign training or an actual attack, the use of burner phones becomes essential to reduce detection by law enforcement. It does take more work than regular use of a mobile phone: to sustain communications over time, users must share and keep track of often-changing phone numbers.

Privacy advocates suggest that burner phone users never actually store contacts' numbers on the device itself, which would save them on the phone's SIM card. That could let police use that data during an investigation. So users must write down or memorize phone numbers, which keeps the information available but easily abandoned in case of emergency.

Burner phones can also be used to activate bombs, since only the maker may know the phone number and call it to activate the device. After they are used, burner phones can be destroyed to further reduce the likelihood of identification and forensic evidence collection.

Taken as a whole, we must recognize that technology use by extremist groups extends well beyond any one type of device, across the continuum of both hardware and software communication platforms. As technologies continue to evolve,



CBRNE-TERRORISM NEWSLETTER – May 2016

extremists will continue to stay on the cutting edge of communications, whether they are encrypted or completely open. Law enforcement and intelligence agencies must be able to adapt investigative resources to these

various platforms and do so quickly in order to better respond to these threats. Otherwise, gaps in collection and analysis may lead to intelligence failures and successful attacks.

Thomas Holt is Associate Professor of Criminal Justice, Michigan State University.



Cybersecurity's weakest link: **humans**

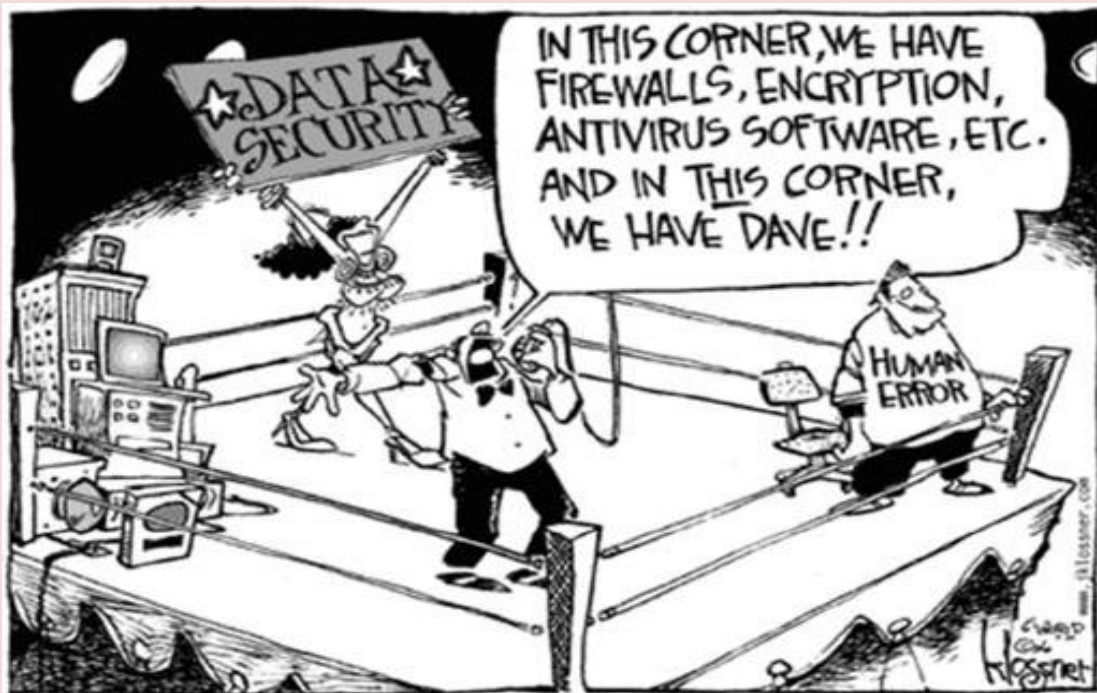
By Arun Vishwanath

Source: <http://www.homelandsecuritynewswire.com/dr20160506-cybersecurity-s-weakest-link-humans>

May 06 – There is a common thread that connects the hack into the sluiceway controllers of the [Bowman Avenue dam in Rye, New York](#); the breach that compromised twenty million federal employee records at the [Office of Personnel Management](#); and the recent

the user's computer or even to an entire corporate network. Sometimes attacks like this also come through text messages, social media messages or infected thumb drives.

The sobering reality is there isn't much we can do to stop these types of attacks. **This is**



spate of [“ransomware” attacks](#) that in three months this year have already [cost us over \\$200 million](#); they were all due to successful [“spearphishing” attacks](#).

Generic – or what is now considered “old school” – phishing attacks typically took the form of the infamous **“Nigerian prince” type e-mails, trying to trick recipients into responding with some personal financial information.** “Spearphishing” attacks are similar but far more vicious. They seek to persuade victims to click on a hyperlink or an attachment that usually deploys software (called “malware”) allowing attackers access to

partly because spearphishing involves a practice called [social engineering](#), in which attacks are highly personalized, making it particularly hard for victims to detect the deception. Existing technical defenses, like antivirus software and network security monitoring, are designed to protect against attacks from outside the computer or network. Once attackers gain entry through spearphishing, they assume the role of trusted insiders, legitimate users against whom protective software is useless.



CBRNE-TERRORISM NEWSLETTER – May 2016

This makes all of us Internet users the sole guardians of our computers and organizational networks – and the weakest links in cyberspace security.

The real target is humans

Stopping spearphishing requires us to build better defenses around people. This, in turn, requires an understanding of why people fall victim to these sorts of attacks. My team's recent research into the psychology of people who use computers developed a way to understand exactly how spearphishing attacks take advantage of the weaknesses in people's online behaviors. It's called the [Suspicion, Cognition, Automaticity Model \(SCAM\)](#).

We built SCAM using simulated spearphishing attacks – conducted after securing permission from university research supervision groups who regulate experiments on human subjects to ensure nothing inappropriate is happening – on people who volunteered to participate in our tests.

We found two primary reasons people are victimized. One factor appears to be that people naturally seek what is called “cognitive efficiency” – maximal information for minimal brain effort. As a result, they take mental shortcuts that are triggered by logos, brand names or even simple phrases such as “Sent from my iPhone” that phishers often include in their messages. People see those triggers – such as their bank's logo – and assume a message is more likely to be legitimate. As a result, they don't properly scrutinize those elements of the phisher's request, such as the typos in the message, its intent, or the [message's header information](#), that could help reveal the deception.

Compounding this problem are people's beliefs that online actions are inherently safe. Sensing (wrongly) that they are at low risk causes them to put relatively little effort into closely reviewing the message in the first place.

[Our research shows](#) that news coverage that has mostly focused on malware attacks on computers has caused many people to mistakenly believe that mobile operating systems are somehow more secure. **Many others wrongly believe that Adobe's PDF is safer than a Microsoft Word document**, thinking that their inability to edit a PDF translates to its inability to be infected with malware. Still others erroneously think Google's free Wi-Fi, which is available in some

popular coffee shops, is inherently more secure than other free Wi-Fi services. Those kinds of misunderstandings make users more cavalier about opening certain file formats, and more careless while using certain devices or networks – all of which significantly enhances their risk of infection.

Habits weaken security

Another often-ignored factor involves the habitual ways people use technology. Many individuals use email, social media and texting so often that they eventually do so largely without thinking. Ask people who drive the same route each day how many stop lights they saw or stopped at along the way and they often cannot recall. Likewise, when media use becomes routine, people become less and less conscious of which emails they opened and what links or attachments they clicked on, ultimately becoming barely aware at all. It can happen to anyone, even the director of the FBI. When technology use becomes a habit rather than a conscious act, people are more likely to check and even respond to messages while walking, talking or, worse yet, driving. Just as this lack of mindfulness leads to accidents, it also leads to people opening phishing emails and clicking on malicious hyperlinks and attachments without thinking.

Currently, the only real way to prevent spearphishing is to train users, typically by simulating phishing attacks and going over the results afterward, highlighting attack elements a user missed. Some organizations punish employees who repeatedly fail these tests. This method, though, is akin to sending bad drivers out into a hazard-filled roadway, demanding they avoid every obstacle and ticketing them when they don't. It is much better to actually figure out where their skills are lacking and teach them how to drive properly.

Identifying the problems

That is where our model comes in. It provides a framework for pinpointing why individuals fall victim to different types of cyberattacks. At its most basic level, the model lets companies measure each employee's susceptibility to spearphishing attacks and identify individuals and workgroups who are most at risk.

When used in conjunction with simulated phishing attack tests, our model lets organizations



CBRNE-TERRORISM NEWSLETTER – May 2016

identify how an employee is likely to fall prey to a cyberattack and determine how to reduce that person's specific risks. For example, if an individual doesn't focus on email and checks it while doing other things, he could be taught to change that habit and pay closer attention. If another person wrongly believed she was safe online, she could be taught otherwise. If other people were taking mental shortcuts triggered by logos, the company could help them work to change that behavior.

Finally, our method can help companies pinpoint the "super detectors" – people who consistently detect the deception in simulated attacks. We can identify the specific aspects of their thinking or behaviors that aid them in their

detection and urge others to adopt those approaches. For instance, perhaps good detectors examine email messages' header information, which can reveal the sender's actual identity. Others earmark certain times of their day to respond to important emails, giving them more time to examine emails in detail. Identifying those and other security-enhancing habits can help develop best-practice guidelines for other employees.

Yes, people are the weakest links in cybersecurity. But they don't have to be. With smarter, individualized training, we could convert many of these weak links into strong detectors – and in doing so, significantly strengthen cybersecurity.

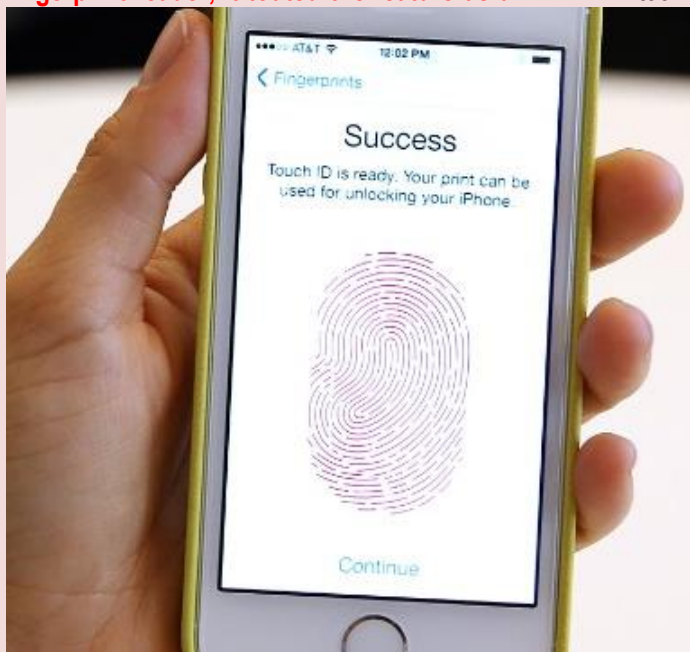
Arun Vishwanath is Associate Professor of Communication, University at Buffalo, The State University of New York.



Police Can Force You to Use Your Fingerprint to Unlock Your Phone

Source: <http://www.nextgov.com/defense/2016/05/police-can-force-you-use-your-fingerprint-unlock-your-phone/127999/>

May 03 – **When Apple announced in 2013 that its next iPhone would include a fingerprint reader, it touted the feature as a**



leap forward in security. Many people don't set up a passcode on their phones, Apple SVP Phil Schiller said at the keynote event where the Touch ID sensor was unveiled, but making security easier and faster might convince more users to protect their phones. (Of course, Apple

wasn't the first to stuff a fingerprint reader into a flagship smartphone, but the iPhone's Touch ID took the feature mainstream.)

The system itself proved quite secure—scanned fingerprints are stored, encrypted, and processed locally rather than being sent to Apple for verification—but the widespread use of fingerprint data to unlock iPhones worried some experts.

One of the biggest questions that hung over the transition was legal rather than technical: How might a fingerprint-secured iPhone be treated in a court of law?

The question went unanswered for a year, until a Virginia judge [ruled in 2014](#) that police can force users to unlock their smartphones with their fingerprints. But until this February, when a federal judge in Los Angeles signed a search warrant that

required a woman to use her fingerprint to unlock her iPhone, it didn't appear that any federal law-enforcement agency had ever used that power. The iPhone belonged to Paysar Bkhchadzhyan, the 29-year-old



CBRNE-TERRORISM NEWSLETTER – May 2016

girlfriend of a man accused of being a member of an Armenian gang, according to Matt Hamilton and Richard Winton of the *LA Times*. She was sentenced in February for one count of identity theft, and just 45 minutes later, a federal judge signed [a warrant](#) authorizing law-enforcement officers to place her finger or thumb on the Touch ID sensor of her iPhone. It's not clear what prosecutors are searching for on her phone.

The warrant was [first discovered by Thomas Fox-Brewster of Forbes](#) in March. Fox-Brewster examined “hundreds of court documents” but wasn't able to find any previous example of a federal warrant for device-unlocking fingerprints.

The federal judge in Los Angeles may have moved quickly to sign and execute the warrant because there's only a 48-hour window during which an iPhone will accept its user's fingerprints. After that window—or after a restart—the phone will require a PIN or passcode to unlock.

The Fifth Amendment, which protects people from incriminating themselves during legal proceedings, prevents the government from compelling someone to turn over a memorized PIN or passcode. But fingerprints, like other biometric indicators—DNA, handwriting samples, your likeness—have long been considered fair game, because they don't reveal anything in your mind. (Marcia Hofmann, a digital-rights lawyer, wrote [a comprehensive rundown of the question](#) in late 2013, when it was still hypothetical.)

Now that it's clear that police are willing to ask for warrants for phone-unlocking fingerprints—

and that judges are willing to sign them—security-conscious smartphone users are faced with a menu of mostly unsavory options.

A fingerprint and a long passcode provides a good balance between convenience and security—or it did, until courts began compelling fingerprint unlocks, said Chris Soghoian, the chief technologist at the American Civil Liberties Union. The alternatives are worse: A short PIN “lets you use your phone like a human,” Soghoian said, but can be guessed by a computer algorithm in certain cases. And a long passcode, while secure, is a pain to type in every time you want to check Tinder.

The only way to turn off an iPhone's fingerprint-reader on the fly—without waiting for the 48-hour window to expire—is to turn it off. When it's powered back on, it will ask for the device's PIN or passcode, and won't accept fingerprints. (If Bkhchadzhyan's phone was off when police found it in her boyfriend's home, her fingerprints won't unlock it.)

Since Apple began encrypting its iPhones in 2014 and rolled out further security improvements alongside Touch ID, law enforcement has had to get increasingly creative to access the contents of the computers, tablets, and phones that they seize. The court fight over an iPhone used by one of the San Bernardino shooters, for example, only ended when the FBI paid for a technique to bypass the phone's security. Similar hacking techniques—and more warrants for fingerprints—may become commonplace as the government confronts increasingly secure devices.

Shift in Nature of Cyberattacks in 2015

By Krysta Dodd (Contributing Writer)

Source: <http://www.hstoday.us/single-article/forcepoint-report-shift-in-nature-of-cyberattacks-in-2015/6a1d1a5c820c05ea5361bb2c6f447907.html>



May 05 – Today's cyber threats are not only increasingly advanced and damaging, they are widely dispersed, ever-evolving, and challenging to stop. According to Forcepoint's 2016 Global Threat Report, these threats include everything from ransomware to insiders to a new botnet, dubbed “Jaku,” targeting Asia.

The report analyzed more than three billion data points per day in 155 countries around the world. The data was collected and evaluated using the Threatseeker Intelligence Cloud, and the Forcepoint team—which included researchers and engineers in Europe, the Middle East, and North America—provided expert interpretation.



CBRNE-TERRORISM NEWSLETTER – May 2016

“The rapid evolution of the cyber threat environment has consequences that are much broader than just technical, operational, and financial – they can impact every piece of a business,” said Forcepoint Chief Scientist Dr. Richard Ford. “With this Threat Report, we want to demystify these threats and help enable businesses with tools, recommendations and, quite simply, knowledge, so they can continue to move forward without fear.”

The key findings of the report include:

- Malicious content in email increased 250 percent compared to 2014, driven largely by malware and ransomware
- The United States hosts more phishing websites than all other countries combined
- Ransomware focus is sharpening, targeting countries, economies and industries where a high ransom is more likely to be paid
- “Insiders” – malicious and accidental – represent the biggest threat to company security and the one for which businesses feel least prepared
- Advanced evasion techniques are gaining in popularity and are combining multiple evasion methods, such as IP fragmentation and TCP segmentation, to create new ways to bypass access controls, attack watering holes and disguise traffic

In the face of the rapidly evolving cyber threats facing organizations and government agencies, security professionals must enhance their cybersecurity defense strategy.

Bob Hansmann, Director of Security Analysis & Strategy for Forcepoint, told *Homeland Security Today* that industry leaders must take

these threats seriously, and be proactive in investigating them. He explained, “Organizations are still focusing budgets on inbound security rather than on identifying potential breaches, even as publicly reported breaches become an almost weekly occurrence.”

Hansmann added, “We are talking about more than system downtime. Jobs, businesses, and even lives are at stake in the current cyber war.”

To build a better and more secure information network for communication and storage, Forcepoint suggests making progressive changes. The report revealed that the company advocates a new, holistic approach to cybersecurity, which gives enterprises a 360-degree view of the threat landscape, as well as real-time analysis and meaningful alerts that can help customers act quickly to defeat even the most advanced adversaries.

Putting in place important organizational changes is critical in safeguarding an organization from attack. Educating personnel on what changes have been made to internal systems, and directing them on how they can promote a safe and secure cyber environment is vital.

Additionally, supervising network connections for theft or abnormal activity, installing data theft prevention tools, and enhancing email and Internet connections and transfer policies can also prove beneficial.

“It’s not a matter of ‘if’ I get breached, or even preparing for ‘when’ I will be breached. The question is: ‘Am I currently breached,’” said Hansmann.

► **Download the report from:** https://www.forcepoint.com/resources/whitepapers/forcepoint-2016-global-threat-report?utm_source=Forcepoint&utm_medium=Home%20Page%20Banner

The cyberattack that changed the world

By Patrick Howell O’Neill

Source: <http://www.dailydot.com/politics/web-war-cyberattack-russia-estonia/>

May 20 – Some moments that change the course of history are obvious instantly. The Sept. 11, 2001, terrorist attacks. The 2003 invasion of Iraq. Broadcast live around the globe, the gruesome images of these events set the stage for the 21st century. Everyone knew it even while the cameras were rolling. Others you have likely never heard of.

On a chilly Baltic spring day in 2007, a much quieter act of violence began with just an error message here, a disconnected server there. It would end by crippling the institutions of a major European capital, escalating what had been a war of words between two countries, Russia and Estonia, into



CBRNE-TERRORISM NEWSLETTER – May 2016

something unprecedented: Cyberwar.

This surreptitious smash into Estonia's digital heart sparked a shift in the fighting stance of the world's most powerful militaries, richest governments, and most cutting-edge private companies that continues to this day.

Estonians compare the day to their own 9/11. Imagine what would happen if Wall St. financial institutions and every American bank was



crushed under the weight of a cyberattack while Washington, D.C.'s institutions fell apart under the same withering offensive. Meanwhile, what if no one could read newspapers or call 911?

That's the level of attack that Estonia faced.

In July 2016, the world's most powerful military alliance will meet in Poland. Over the last decade, NATO's priorities have changed. In the wake of the fall of the Soviet Union, an attack by Russia—of any kind—once seemed almost inconceivable.

But military tension has returned to Eastern Europe as Russia and NATO eye each other warily. The Western alliance was shifting, its centers of power moving steadily eastward to capitals like Warsaw, Ankara, and Tallinn. Two old rivals are standing up.

The pressure has been building since that historic moment in 2007.

It's been called Web War I. That's how new and monumental this incident was for those who experienced it. It set the stage for Web Wars to come. And it all started with a statue.

Soviet "liberators"

As with so many historic singular moments, the lead up to Web War I is marked by decades of blood and oppression.

Estonia is a small country in Northern Europe. It borders the Baltic Sea, Latvia, and Russia. That last one is big in every sense of the word. A former Soviet satellite, Estonia was on the wrong end of a half-century occupation that

turned the country into a hyper-militarized border zone from which the Soviet Army poised its war-fighting power toward the West.

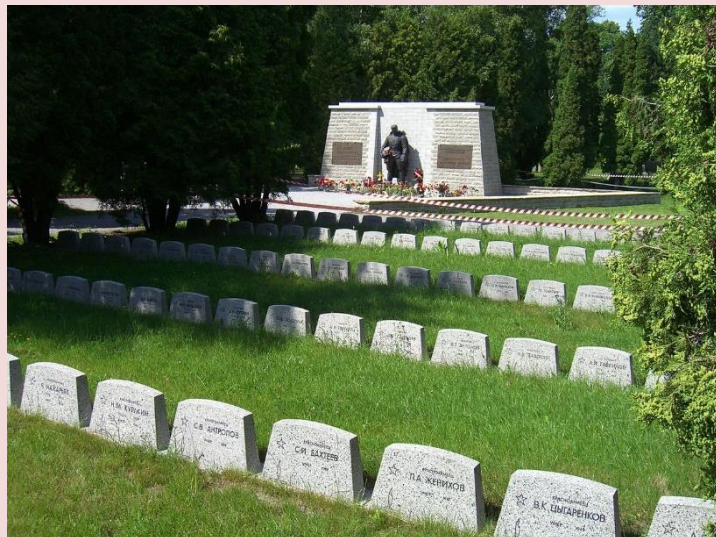
In the middle of the 20th century, the country was traded back and forth between the Soviets and Nazis in bloodshed that resulted not just in tens of thousands of Estonian deaths but also a brutal authoritarian disruption to their society that ultimately lasted for decades. Before that, Estonia was ruled for centuries by powers like Sweden and Denmark.

True independence was a foreign concept to many Estonians, but the 20th century brought a "national awakening" in which millions yearned for sovereignty.

When the Soviets and Nazis divided up Eastern Europe preceding World War II, Estonia went to the Russians, who promptly occupied the country and installed a puppet government. The Nazis invaded and occupied from 1941 to 1944, when the Soviets returned for what seemed would be forever.

Estonia's Russian overlords didn't see their occupation as brutal or disruptive or illegal the way the West did. The Soviet propagandists—and today's Russian government—very earnestly said it was all legitimate.

In 1947, with Eastern European rubble still soaked in the horrors of war, the Soviets built a **six-foot-tall bronze statue** memorializing their



soldiers and war effort. They put it right in downtown Tallinn, Estonia's coastal capital. The Soviets called it Monument to the Liberators of Tallinn.

From whom, exactly, did the Soviets liberate Tallinn?

With the specter of the Red Army looming, the Nazis withdrew from



CBRNE-TERRORISM NEWSLETTER – May 2016

that city without fighting. It was the Estonians who re-established an independent country on Sept. 18, 1944. By Sept. 22, the Soviets took hold of the city again. In that way, the Russians “liberated” Tallinn from the Estonians themselves.

As a result, the Bronze Soldier of Tallinn is seen by many Estonians as a symbol of Soviet occupation. After the fall of the Soviet Union, a growing number of Estonians wanted it gone. More hard-line activists pushed to have the thing outright destroyed.

In 2007, the Estonian government was getting ready to finally move the Bronze Soldier. In response, ethnic Russians in the country rioted in the worst unrest Estonia had seen since the brief but bloody war of independence that commenced when the Soviets occupied the country in 1944.

In two nights of rioting, one man was killed, 153 people were injured, and 800 arrests were made in the capital. Protesters chanted “Russia” and waved Russian flags. They threw molotov cocktails, looted, and let their dissatisfaction be known through the international language of arbitrary destruction. The unrest became known as the Bronze Night.

Ethnic Russians felt the removal of the statue was one act of discrimination among many, just another kick in the gut in a war against their equal rights in Estonia.

The Russian government, just over the Estonia’s eastern border, warned the small country that removing the statue would be “disastrous for Estonians.”

After the first night of rioting, on April 27, the Estonian government dismantled the Bronze Soldier and moved it from its original location.

Web War I

That’s when the crucial and historic moment began.

As the petrol bombs flew on the streets, a wave of digital violence hit Estonia that caught the country completely off guard.

Estonia is Europe’s most connected country. They’ve pioneered e-government and Internet voting. They’re a world leader in Internet freedom. To say the country is “wired” would be a misnomer—it’s Wi-Fi that saturates the air these days, so they’re thoroughly wireless.

The nation relies more on Skype, which was created in the country in 2003, than old fashioned phone systems. A whopping 98

percent of the country’s bank transactions are done online. They rely so heavily on the Internet, and they did it earlier than any perhaps other country in the world.

That’s why it was such a shock to their system when, with unprecedented speed, the website of Estonia’s largest newspaper was brought to its knees, convulsing, crashing, and ultimately collapsing under the weight of a wave of Internet traffic it couldn’t support.

The techies at the *Postimees*, Estonia’s leading newspaper, told Joshua Davis at *Wired* what happened that day:

“The future was looking perilous. Ago Väärsi, head of IT at the Postimes newspaper, watched as automated computer programs continued to spew posts onto the commentary pages of the Postimees Web site, creating a two-fold problem: The spam overloaded the server’s processors and hogged bandwidth. Väärsi turned off the comments feature. That saved bandwidth — the meter showed that there was still capacity — but what did get through tied the machines into knots and crashed them repeatedly. He discovered that the attackers were constantly tweaking their malicious server requests to evade the filters. Whoever was behind this was sophisticated, fast, and intelligent.”

A few days later, it happened again.

Internet traffic from around the world flooded into Estonian networks and overwhelmed them. The *Postimes* website crashed, as did other Estonian publications. The only option Väärsi saw was to block all international traffic. That fended off the attacks and brought the site up. But it also meant no one from outside Estonia could reach the *Postimes*. They had had to go silent to beat the attackers. For journalists, that means they got beat.

That was the start.

The tsunami of traffic was a botnet—numerous botnets, really—a horde of computers numbering in the hundreds of thousands, enslaved by hackers to act as a weapon for a botnet master. In enough quantity, bandwidth is a hard, blunt object that threatens to knock networks down.

Over the course of several days, the botnets hit banks, broadcasters, police, and the national government. The parliament and ministries networks were overwhelmed, government communication networks were knocked down. The national



CBRNE-TERRORISM NEWSLETTER – May 2016

emergency number buckled. The country's Internet infrastructure was being hit hard with unrelenting traffic that was orders of magnitudes larger than what Estonian networks were capable of handling.

The immediate defense was, again, to cut Estonian networks off from the outside world, block all international traffic, and then regroup. But if you're effectively cut off from the outside world, getting outside help is a challenge.

A stroke of luck hit when Estonian authorities learned that they just happened to have Internet royalty in their capital during this attack. In town was Kurtis Lindqvist, CEO of the Swedish independent Internet infrastructure organization called Netnod. Netnod runs i.root-servers.net, one of 13 DNS root-name servers in the world, which manages worldwide Internet traffic.

After four days under attack, it took face-to-face meetings between Lindqvist and Estonia's top cybersecurity authorities to begin to persuade the world's Internet Service Providers to single out and blacklist the attackers.

The Russian government denied involvement in the attacks as Estonia's foreign minister directly accused President Vladimir Putin's government of being behind the offensive.

Incensed, Estonian Foreign minister Urmas Paet said, "The European Union is under attack, because Russia is attacking Estonia. The attacks are virtual, psychological, and real."

Moscow proclaimed its innocence but remained hostile in its rhetoric.

As troops marched for Russia's celebration of Victory Day, commemorating their triumph over Nazi Germany, Putin told troops marching in Red Square, "Those who are trying today to ... desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and people."

Russia also implemented limited sanctions against Estonia during this period, suspending some trains carrying passengers and raw materials to Tallinn.

In Estonia, the message was received loud and clear: You're not as safe as you think you are. But a question remained: Could anyone prove who was sending the message?

Origins of the attack

Pinpointing and crediting a state-level cyberattack is a difficult task that can easily rise to near impossible.

But here there are some crucial clues. *Wired*, working with the security firm Arbor Networks, identified overlap between the botnet attacking Estonia and botnets that were previously used to attack Russian opposition politicians like Garry Kasparov.

Russian-language forums were full of messages urging an attack and enlisting foot soldiers in the lead-up to the offensive.

Then, two weeks after the digital blitzkrieg began, it stopped without warning. The botnets ceased their offensive and the weight on Estonian networks lifted. Pressure had been exerted.

Russians are the chief suspects, but proof positive is another question. And whether this was direct government action or private hackers or a potent combination of the two, that's a more difficult question. A single ethnic Russian living in Estonia was [charged](#), admitted his guilt in taking part, and was convicted in 2008.

This whole affair might sound familiar: Ethnic Russians in a country bordering the motherland, a country previously occupied by Soviets, Moscow's shadowy but forceful reach into a smaller neighbor on the basis of helping those ethnic Russians.

If it sounds like a dress rehearsal for 2014's war in Ukraine, you're not alone.

Web War I was one of the first steps taken into a modern Europe where tensions between Russia and her neighbors are rising, military budgets are growing, and hard American power is seen now in tanks on the ground across Eastern Europe and a cyberwar stance with eyes directly on Moscow.

Estonia is a member of the North Atlantic Treaty Organization (NATO), the world's most powerful military alliance, and, from a Russian perspective, one of the world's most aggressive villains. Not coincidentally, the expansion of NATO and Ukraine's potential membership was one of the matches that set the country aflame in 2014.

Ene Ergma, who was speaker of the Estonian parliament during the 2007 attacks, [said](#), "Attacking us is one way of checking NATO's defenses. They could examine the alliance's readiness under the cover of the statue protest."

In the wake of these attacks, Estonia compared them to terrorist action and urged a strong NATO response. The alliance wasn't



CBRNE-TERRORISM NEWSLETTER – May 2016

ready—there had never been a cyberattack like this, there was no playbook to study.

They were unprepared on a technological and strategic level. As such, this moment also started fundamental debates that are still being sorted out.

Should a massive attack like this be treated as an act of war? [It's a question that is still being sorted out](#). NATO networks were under attack from the same botnets that hit Estonia, and they were defended by a 5-year-old program that, after Estonia, was expanded beyond NATO networks. A year later, NATO established its cyberdefense center in Estonia's capital.

In 2016, it's easy to forget how new a cyberattack of this scale was for the world's great powers. Only one attack, called Titan Rain, was larger than the bombardment of Estonia. It endured from around 2003 to around 2006 and targeted American networks. The British and Russians may have been in the crosshairs as well. [China got the blame](#), as they so often do, but proof remains illusive.

A decade later, we still don't know what was stolen in Titan Rain and even who entirely was hit.

The attack on Estonia, however, was loud and clear. The scale and sophistication of the attack was unprecedented. It's set the tone for Eastern Europe, and the world, ever since, as [cyberwar capabilities have increasingly come into focus](#). When you hear of the worst-case scenarios when it comes to the future of cyberwar, experts are imagining Estonia first when they imagine the future.

Estonian authorities' comparison of Web War I to 9/11 is tricky, obviously, but it has real merit. America's course in the world shifted as a result of 9/11. What the U.S. did with its military, how American power interacted with the world—this all changed.

Web War I changed all this with Estonia, too, and it had broader effects that continue to ripple through NATO to Russia and to the rest of the world today.

Estonia in 2007 is when the threat began to grow in the minds of the world's great powers. When a country's banks cannot freely move money, that's when you've hit a nerve.

Now NATO is shifting. In Western Europe, military budgets are mostly shrinking. The three European titans—France, Germany, the United Kingdom—are not looking like they'll play the same role in the alliance moving forward. But in the East, there's a new combativeness that is in large part responding to Russia's resurgence.

Little Estonia—tiny but wealthy and long on the cutting edge of technology—has become a cornerstone of the West's cyberwar capabilities. Poland is building up its military, and Turkey is spending more on fighting capabilities and NATO itself.

Web War I changed the face of NATO, it changed the minds of European powers, and it changed the fighting stance of a world that was caught totally off guard by these attacks.

When they write the history books on the 21st century, expect special attention to be paid to the day in Tallinn where molotov cocktails flew and networks crashed.

Patrick Howell O'Neill is a senior reporter at the Daily Dot. He reports on security and politics.



6 Information Management Challenges In An Emergency Response!

Source: <http://d4h.org/blog/post/20150216-6-information-management-challenges-in-an-emergency-response>



When an incident occurs, both incident responders and managers are faced with high volumes of information. Their priority is to bring the incident to a swift ending. This means that efficient management of information can relieve some pressure. There are however a number of common information management challenges associated with incident response. They include:

1. Paper Based information Gathering

When an incident occurs, a high volume of information is traditionally captured by completing paper-based forms by hand, which are later processed. The biggest shortcomings of the paper-based system is the poor quality of the records, a lack of contextual information and difficulty in instantly analysing any data captured.

2. Time Stamping Information

After an incident has occurred there is a need to report on the events. A major difficulty is recording the times and sequence in which events and tasks occurred. When using paper a possibility is the use of rubber stamps, these are often used in offices to stamp the current date, however this is a cumbersome task. The most efficient method is using a digital timestamp, the time at which an event is recorded by a computer.

3. Recording of Tasks

Task management is the process of managing a task through its life cycle. Effective task management requires managing all aspects of a task, including its status, priority, time, human and financial resources, notifications and so on. These can be lumped together broadly into the basic activities of task management. The difficulty during a high stakes event is that tasks are assigned to multiple individuals or teams and there are a number of stages to

monitor from who has been assigned the task to whether its completed/failed.

4. Access to Documentation

Often response plans are bulky paper documents in folders that are stored on a bookcase in an operation centre. When needed such folders may not be available immediately at the scene and depending on the scenario personnel may not be familiar with the relevant parts of a plan they are to enact.

5. Managing Multiple Sources of Information

During an incident, information is everywhere and arriving in many forms. Managers may be receiving radio communications, video streams, photos, calls, emails, texts, alarm notifications, and paper forms. Finding the best method to manage it is a major challenge. The ideal solution when managing such large volumes of information is to capture all the data in an information management system which acts as a single source of truth.

6. Quickly Querying Information

Being able to effectively query information captured during an incident can be difficult as it is coming from multiple sources. However, when managed effectively it can improve an organizations situational awareness. Situational awareness



CBRNE-TERRORISM NEWSLETTER – May 2016

is more complex than simply noticing what is happening around you. An emergency manager must capture clues and cues in the

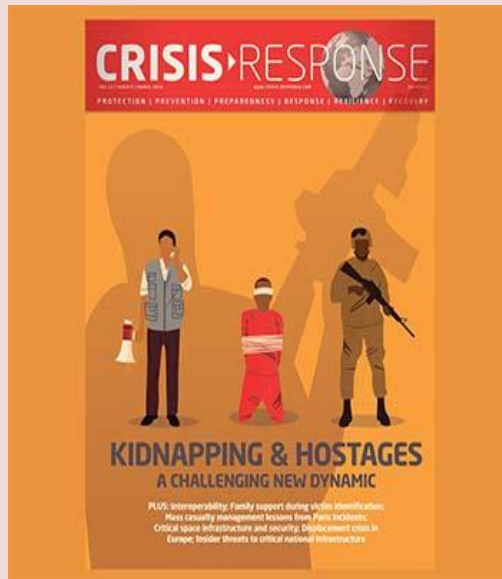
emergency environment, make sense of the information, and predict what will happen next.

Emergency Response Journal

Emily Hough – Editor-in-Chief

Source: <https://www.crisis-response.com/news/news.php?article=1209>

March 2016 – This issue (CRJ 11:3) features reports on flooding in Georgia and the terrorist attack on a university in Pakistan, as well as a look at the self-regulating dynamic of informal settlements, and



examines interoperability between emergency services in the UK. We discuss legal liabilities and response options for INGOs and NGOs whose personnel have been kidnapped and publish a feature on conflict and displacement.

In addition, advice on how to help families through the traumatic experience of identifying the bodies of their loved ones after a mass casualty attack is provided, and France's RAID unit presents lessons learnt in mass casualty medical care after the Paris attacks.

We publish selected views from the UNISDR Science and Technology conference, and the two winning papers from the RUSI Resilience 2050 competition, which look at critical space infrastructure and security, along with an examination of the insider attack threat on interconnected systems within an age of the Internet of Things.

There's much more in this issue, due to be published

soon – read on for more details:

Comment: Zain Daudpoto delves into the murky world of forestry and politics as he highlights deforestation in Sindh Province Pakistan.

Resilience in informal settlements: It is vital to understand the self-regulating dynamic of informal settlements, contends Evgenia Mitroliou of ICLEI Resilient Cities, who says people living in these communities should be actively involved in improving conditions and infrastructure.

Flood response in Georgia: Last year Tbilisi suffered devastating floods that killed 22 people and hundreds of animals from the Georgian capital's zoo (see photo below).



Flooding in Georgia (photo: EMA Georgia)

Interoperability utopia: The word 'interoperability' doesn't necessarily flow easily from the lips, which is somewhat analogous to the difficulty of achieving interoperability in practice, according to Brian Dillon.

Why do we still make the same mistakes? For decades, crisis management has been institutionalised and taught at universities. Corporations and businesses have crisis procedures in place, yet they often seem to forget this learning when crisis strikes, says Caroline Sapiel of CS&A.

INGO kidnap – a challenging new dynamic: Andrew Brown traces how fatalities and subsequent lawsuits against law enforcement and shipping companies have improved



CBRNE-TERRORISM NEWSLETTER – May 2016

response and hostage negotiation in kidnapping and piracy, arguing that these pressures now also apply to INGOs and NGOs.

The Bacha Khan University attack: Four gunmen stormed the Bacha Khan University in Pakistan's Khyber Pakhtunkhwa, killing 21 and injuring another 22. Luavut Zahid visits the scene and talks to those who were caught up in the attack.

Helping families through the identification process: Losing a loved one after a major disaster is inevitably traumatic. But responders and psychologists can work with families to ensure that mental scarring is kept to a minimum during the identification processes, say Erik de Soir and Emily Hough.

Earthquake public preparedness: The challenge is convincing people to take public preparedness initiatives seriously and to maintain levels of readiness during times of relative quiet, according to Gillian Dacey.

Iraq's mental healthcare crisis: As the violence in Iraq continues, it is becoming increasingly apparent that mental health needs require careful and urgent attention according to Alys Brown of the AMAR Foundation.

Sexual violence in conflict: Understanding how, why, if and when sexual violence is used, and against who and by who, should be a central part of how we understand and respond to armed conflict, contend Dr Dyan Mazurana (Associate Research Professor, Research Director at the Feinstein International Center at the Friedman School of Nutrition Science and Policy) and Phoebe Donne.

Mass sexual abuse: A symptom of wider crisis? Lina Kolesnikova and Emily Hough say an increase in sexual attacks is in serious danger of damaging European cohesion and must be addressed, both for the sake of the victims and to avoid wider societal crisis implications.

Displacement Crisis in Europe: Much has been facilitated, enabled and achieved to respond to the emergency looming on Europe's doorstep, explain Lisa Hastert and Marcia Kammitzi of DG ECHO. But political solutions and commitment will be required to tackle the root cause of the current crisis.

The border security paradigm: Dr Attila Freska says there are three strategic security imperatives that governments and global security leaders should implement when seeking solutions to effective control of frontiers in an age of porous borders and global radicalization.

Picking up the pieces: UXO in Syria. James Le Mesurier and Ethan Wilson describe the training and equipment planned to help the White Helmets assist the civilian communities of Syria, who are facing staggering levels of bombing with cluster munitions.

Urban services in protracted armed conflict: Some 50 million people are affected by armed conflict in urban areas, with knock-on effects that go beyond the visible signs of destruction, say Jean Philippe Dross, Michael Talhami, Evaristo de Pinho Oliveira, Javier Cordoba (ICRC); and Dr Mark Zeitoun (University of East Anglia), who call for a paradigm shift in humanitarian action.

Is the North Atlantic to blame for our weather extremes? Dr Aurélie Duchez and colleagues explain that when it comes to connecting the dots between climate change, extreme weather and health, many questions are still unanswered.

The Aral Sea disaster: Dr Abror Gadaev and colleagues from Uzbekistan attended the UNISDR Science and Technology conference and presented a group work raising promoting possible sustainable solutions to the Aral Sea disaster.

Simulation aids training in Japan: At the UNISDR event Dr Sonoe Mashino outlined Japanese university collaboration on a disaster nursing global leadership programme, and how they use technology during multi-site training exercises.

Europe's emergency medical corps: This February, the EU launched the European Medical Corps, which can mobilise medical and public health teams, along with equipment, to respond to emergencies worldwide, writes Monique Pariat, Director General of Humanitarian Aid and Civil Protection (ECHO).

Mass casualty management in counter-terror operations: Emergency medical support specialists from France's elite counterterrorist tactical unit – RAID – present some valuable lessons learnt from their responses to the recent terrorist incidents in France.





RAID's medics are embedded within France's SWAT teams. Here, they share their lessons learnt from responding to the terrorist attacks in France (photo: RAID)

CRJ R&D: First responder safety. This issue's regular section, curated by Ian Portelli and Megan Mantaro, looks at how new technology could provide a solution to the increasing risk of firefighter fatalities, as well as looking at a device that can sense dangerous chemicals.

Critical space infrastructure and space security: In the winning entry to the RUSI Resilience Prize, Dr Liviu Mureşan and Alexandru Georgescu look at how the complex evolution of space systems create benefits and vulnerabilities, and how the latter are likely to develop in the future.

The ripple effect of insider threat attacks: The winner of the CRJ category of the RUSI Essay competition was Ryan Meeks, who looked at resilient critical national infrastructure in the age of connected systems in the Internet of Things

Social media analysis tools: It is important to integrate social media into emergency management practices, say Hayley Watson, Susan Anson and Kush Wadhwa of Trilateral Research and Consulting. But don't be daunted, there are tools to help.

Spatial information sharing: Ivan Baehr provides an overview of how spatial information for humanitarian response has developed, as well as the challenges in implementing this technology

Innovation in crisis management: The EU-funded [Driver project](#) aims to valorise the wealth of European innovation and science in crisis management by assessing and delivering solutions that can be used – and combined – to address crisis management.

Hover power: Dr Dave Sloggett looks at the ways that helicopters provide assistance to people in disaster stricken areas and the vital role that they perform

Legal liability in nuclear accidents Protecting the victim or the nuclear industry? Alina Alexe examines the limitations of current legislation within today's nuclear risk landscape.

Effective decision-making records: Previously, Roger Gomm considered the importance of maintaining clear records while responding to an incident, giving advice on how to do so. In the final part of this series, he provides some examples drawn from real life incidents.

A logbook for chaotic times: Emily Hough speaks to Patrick Lagadec about his new book, which charts the successes – and failures – of leadership in today's volatile and 'wicked' crises

Looking back: The Chernobyl nuclear accident. The explosion at the Chernobyl nuclear power plant thirty years ago was – and remains to this day – the most destructive nuclear accident to occur, writes Tony Moore.



CBRNE-TERRORISM NEWSLETTER – May 2016

Frontline: Empowering communities. Emily Hough speaks to Dr Martina C Fuchs of the Real Medicine Foundation about her passionate belief that a paradigm shift is required in humanitarian development to empower people and communities.

DuPont unveils next generation firefighter protection

Source: <http://i-hls.com/2016/04/dupont-unveils-next-generation-firefighter-protection/>

Apr 29 – DuPont Protection Solutions has unveiled a new game-changing technology to help better protect firefighters – **DuPont Nomex Nano** for thermal liners in turnout gear and DuPont Nomex Nano Flex for firefighter hoods.

Nomex Nano is engineered to be thinner than other advanced flame-resistant (FR) materials used for thermal liners. Providing up to a 40 percent reduction in thermal liner thickness, Nomex Nano can reduce bulk in turnout gear and offers increased mobility and better range of motion for reduced heat stress without compromising thermal protection.

Nomex Nano Flex is a highly breathable, FR material with exceptional elasticity and superior particle barrier performance. It can help make products like firefighter hoods more comfortable and more protective.

“Based on the Nomex brand that has been trusted by firefighters around the world for more than 50 years, Nomex Nano and Nomex

Nano Flex are not only the next generation of FR solutions from DuPont, they represent the future of turnout gear,” said Christine Christmas, North America marketing leader, DuPont Protection Solutions. “Nomex Nano can help reduce heat stress, which now causes more firefighter injuries than any other single factor. And, Nomex Nano Flex helps provide improved particle barrier protection in the neckline and upper jaw area that historically are known to be most vulnerable and least protected.”

DuPont Nomex is known worldwide as the leading flame-resistant fiber. More than 3 million firefighters, as well as workers across the manufacturing, chemical, oil and gas industries, and emergency response and armed forces personnel, depend on its thermal protection to help keep them safe. It’s possible for Nomex fiber to help enable protective apparel to have lower weight at a higher level of protection, breathability for reduced heat stress, and the ability to effectively wick away moisture.

Emergencies and Effective Decision Making

Source: <https://www.d4htechnologies.com/blog/post/20160504-emergencies-and-effective-decision-making>

Decision making and problem solving are critically important skill areas for emergency managers, planners, first responders, voluntary agency coordinators, and other professionals in emergency management.

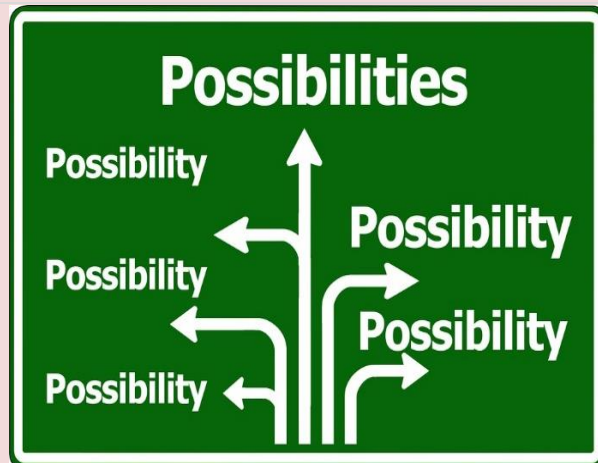
Gaining control of an incident is difficult. Lives, reputation or property hang in the balance. Emergency Response could be stated quite simply as problem solving. Emergencies are typically complex problems with limits on time and severe consequences of failure and a host of other difficulties. Effective decision-making, perhaps more than any other skill, is critical to successful outcomes.



CBRNE-TERRORISM NEWSLETTER – May 2016

Let's clarify what we mean by problem solving and decision making and how they relate to one another. Problem solving is a set of activities designed to analyze a situation systematically and generate, implement, and evaluate solutions. Decision making is a mechanism for making choices at each step of the problem-solving process. Decision making is part of problem solving, and decision making occurs at every step of the problem-solving process.

Therefore, a decision making process is a critical component in any organizations response.



Following are the important steps of the decision making process. Each step may be supported by different tools and techniques.

Step 1: Identification of the purpose of the decision.

The first step is to recognise any problems and identify options that may be available.

Step 2: Information gathering.

What is relevant and what is not relevant to the decision? What do you need to know before you can make a decision, or that will help you make the right one?

Step 3: Principles for judging the alternatives.

What alternative courses of action may be available to you? What different interpretations of your data may be possible?

Step 4: Brainstorm and analyse the different choices.

Generate several possible options. Ask "what if" questions.

Step 5: Evaluation of alternatives.

What criteria should you use to evaluate. Which alternative will best achieve your objectives?

Step 6: Select the best alternative.

Explore the provisional preferred alternative for future possible adverse consequences. What problems might it create? What are the risks of making this decision?

Step 7: Execute the decision.

Commit to making the decision work, allocate resources and put a plan in place to implement the decision.

Step 8: Evaluate your results.

Capture the lessons learned from past successes and failures, with the goal of improving future performance. It is an opportunity to reflect on an event so that you can do better the next time.

As an emergency response professional, your ability to identify current and potential problems and to make sound, timely decisions before and during an emergency can literally affect the lives and well-being of the local citizenry. **Your decisions can impact the ability of response agencies to do their jobs and can make the difference in how quickly the community is able to recover from an event.**

San Andreas fault "locked, loaded, and ready to roll"

Source: <http://www.homelandsecuritynewswire.com/dr20160509-worries-in-southern-california-san-andreas-fault-locked-loaded-and-ready-to-roll>

Apr 09 – **Top seismologists have warned residents of southern California that the region is overdue for a major earthquake. The San Andreas fault is "locked, loaded and ready to go,"** said Thomas Jordan,

director of the Southern California Earthquake Center.

Jordan, speaking at a seismology conference, said that "The San Andreas fault is locked, loaded



CBRNE-TERRORISM NEWSLETTER – May 2016

and ready to roll. The springs of that fault have been wound pretty tightly and the situation is



San Francisco on 18 April 1906.

there where we could have major earthquakes in California.”

The Earthquake Center has released a graphic which simulates how far the shaking would travel if, as he suggests, it is of 8.0 magnitude.

The *Daily Mail* reports that there has been a growing concern among experts that the San Andreas fault may be close to a new, major

more destructive than the 1994 Northridge earthquake. That earthquake hit a different fault northwest of Los Angeles, killing sixty people.

In 2008 the the US Geological Survey (USGS) warned that even a 7.8 magnitude earthquake on the southern portion of the San Andreas Fault would cause more than 1,800 deaths, 50,000 injuries, \$200 billion in damage. In addition to the physical damage to infrastructure, there would be serious health risks as sewage systems would be destroyed. In October, Los Angeles mayor Eric Garcetti persuaded the City Council to pass legislation requiring as many as 15,000 buildings be reinforced, including concrete buildings considered brittle and apartment blocks built



ruction if only because the length of time since it happened last. In 1857 the southern portion of the fault was struck by a 7.9 tremor.

In the intervening 159 years, the tectonic plates which meet at the fault have been moving at a rate of about two inches per year – meaning that there has been a shift of about twenty-six feet, with the Pacific plate moves in a northwesterly direction relative to the American continental plate.

Seismologists note that an 8.0 magnitude shake in southern Carolina would likely be far

mostly from timber.

Jordan praised the city for taking steps to mitigate the risks. “It’s remarkable that this happened,” he said. “We know politically how difficult it is to make these kinds of changes.”

While California is worried about the Big One, Washington State is worried about a swarm of as many as 130 small earthquakes in recent weeks under Mount St. Helens, signaling increasing dangers of a volcanic eruption.



CBRNE-TERRORISM NEWSLETTER – May 2016

USGS said, however, that at this point, "there is absolutely no sign that it will erupt anytime soon, but the data we collect tells us that the volcano is still very much alive."

USGS said that the tremors began on 14 March and now reach as many as forty a week. In 1980, a major eruption of the volcano blew a 1,000 feet off the top of the mountain, ignited forest fires, and killing fifty-even people.

"The earthquakes are volcano-tectonic in nature, indicative of a slip on a small fault. Such events are commonly seen in active hydrothermal and magmatic systems," USGS said.

Most of the earthquakes now being detected are of 0.3 magnitude or less, with the largest at 1.3 magnitude.

Lessons Learned From Katy, Texas, Area Floods

Source: <http://www.emergencymgmt.com/disaster/Lessons-learned-from-Katy-area-floods.html>



A person paddles through a flooded neighborhood, Tuesday, April 19, 2016, in Spring, Texas AP/David Phillips

May 04 – Mark Michalk was in Rockport on April 18 when the water rose into his Katy home. He had been out of town to help his aunt repair her summer home. When he reached his house on Y Street and Avenue D three days later, Michalk stood shocked at damage from 1-foot-deep water in the building.

"We have to gut my house, tear the Sheetrock out of the walls at least 4 feet up," said Michalk, who has lived in his downtown Katy home more than 10 years. "All the damages will probably cost \$80,000 to \$90,000 to repair. I have no flood insurance."

Aid came from members of Kingsland Baptist Church, who helped tear out Michalk's moldy wallboard and cabinets days after historic flooding hit the Houston region.

Local emergency officials praised such groups' role in assisting those hit by flooding and said cooperation went well between agencies conducting rescues and otherwise helping residents. But they also said the flood exposed needs for improvement related to flood response and communication with the public.

Lessons from the flood

The city of Katy's fire department, backed by groups such as Katy ISD police, Texas Parks and Wildlife Department game wardens and the Harris County Sheriff's Office, made more

than 75 high-water rescues in the area, mostly north by Cypress Creek.

"We had air boats with the game wardens and received a bus from (Katy ISD) for those that were



CBRNE-TERRORISM NEWSLETTER – May 2016

rescued to be transported out," said Maria Galvez, emergency management coordinator at the city of Katy Office for Emergency Management. "Neighbor was helping neighbor, friend helping friend."

Eight people died from the floods in the Greater Houston area, but none in the Katy ISD boundaries, district spokesperson Denisse Coffman said.

High water affected downtown Katy and along South Mayde Creek and Kingsland Boulevard. Flooding extended from Brookshire east to the Addicks and Barker reservoirs and north to Cypress Creek communities.

In the city of Katy, 112 residences and 31 businesses sustained damage estimated at \$10.3 million, Galvez said. Hundreds of homes outside the city were affected by floods fueled by a storm dropping between 12 and 17 inches of rain.

Among the worst hit areas were Bear Creek and Bear Creek Village subdivisions, where 308 homes flooded, according to the Harris County Office of Emergency Management.

The Waller County emergency management office aided those affected by flooding between FM 529 and U.S. 90 and also in Brookshire.

Galvez believes communication could have been better to Katy residents, saying that details need to be uploaded faster to the city's website during such events.

And Waller County Office of Emergency Management coordinator Brian Cantrell said response time from emergency personnel could improve. He noted that about two hours passed until emergency personnel were fully organized once the flooding became worrisome.

He and Galvez said purchasing added air boats and high-water vehicles could help the response when roads flood.

In Katy, police could improve how quickly they block streets during flooding, Katy police Capt. Byron Woytek said.

City officials also had problems with residents driving past barricades, some seeking to drive through high water for amusement.

This month, Harris County Office of Emergency Management will host personnel from Katy and other emergency management offices in the county to discuss what improvements are needed, according to county OEM spokesperson Francisco Sanchez.

"We're going to identify quick fixes like, for example, data that has info on where the

lowest points are in our bayous," Sanchez said. "For long-term fixes one of the things that could be done better is - how do we get all major thoroughfares in Houston that are not state highways being posted online in one place and being updated on a regular basis?" Other issues, he said, are how to better barricade flood-prone locations such as highway underpasses.

'Phenomenal rainfall' recorded in the area

The Harris County Flood Control District's upcoming projects include creating a \$6 million flood basin on the intersection of FM 529 and Greenhouse Road near the Addicks and Barker reservoirs as well as a feasibility study for potential South Mayde Creek flood projects, according to Alan Black, the district's engineering director.

The district has spent more than \$1.5 billion in projects throughout the county in 15 years but is limited in what it can do on a year-to-year basis, Black said. The district receives about \$60 million annually from property taxes and seeks grants from other resources such as federal disaster relief funds.

"There's no one smoking gun to fix all the problems. There's only so much funding every year," Black said. "The amount of rain that fell is tremendous. I think people are reasoning that a phenomenal rainfall brought a phenomenal flood, and people responded in a phenomenal way. There are limits to what any flood structure can take."

Said Cantrell, "I think most residents understand that when you have that many inches of rain, you're going to have problems no matter what."

At his Avenue D home, Michalk is hoping to receive aid from the Federal Emergency Management Agency. FEMA, he said, "can afford to write me a \$25,000 check."

On April 25, President Barack Obama issued a disaster declaration for Harris County, making flood victims eligible for assistance likely to total millions of dollars. Katy's other two counties, Waller and Fort Bend, have not received the declaration.

Galvez urges Katy residents to report flood damage on www.cityofkaty.com, which could potentially assist in other Katy areas receiving federal aid, as well as businesses.





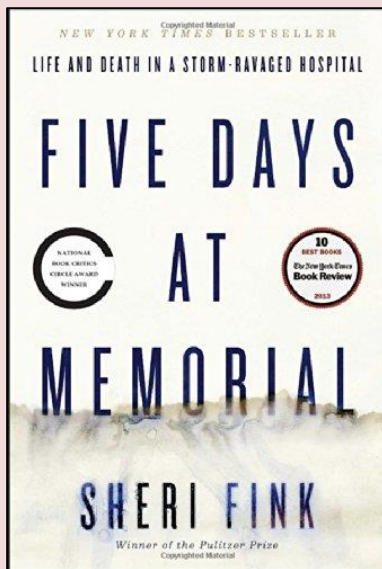
Plan D: A Bosnian Healthcare Worker' Survival Guide

Source: http://www.domesticpreparedness.com/Commentary/Interviews/Plan_D%3a_A_Bosnian_Healthcare_Worker%60_Survival_Guide/

“Everybody has a plan until they get punched in the mouth.”

—Mike Tyson, *Boxing Heavyweight Champion*

This article derives from an extended interview with Dr. Rajko Anic. As a physician during the [1992-1995 Yugoslav war](#) and an accomplished mixed martial arts fighter, Anic explained that – when in a fight and the opponent seems to be countering every move – “If Plan A doesn’t work out for you, then try B, C, or even D.”



May 11 – In the opening chapters of the celebrated book, “[Five Days at Memorial](#),” the author Sheri Fink recounted in detail the horrifying facts of “life and death in a storm-ravaged hospital” following Hurricane Katrina in 2005. She described a major medical center without electricity, clean water, wastewater treatment, and ventilation, as well as only limited communications, supplies, and transportation. Patients, deprived of lifesaving technology, lingered and then died in the heat. Of the 16 U.S. critical infrastructure sectors, Healthcare and Public Health is particularly important in the immediate response and recovery phase of a disaster. The populations served – critically ill, injured, and hospitalized patients – are vulnerable segments of society. The Healthcare and Public Health sector is also one of increasing complexity that relies on a combination of support from the other sectors, especially the power grid, and increasingly on moment-to-moment connectivity with information technology (IT) and the internet.

Lessons From Bosnia

Dr. Rajko Anic’s firsthand knowledge and recollections of what it was like for a European country to devolve quickly into chaos – and the need for healthcare providers to continue providing care – are instructive. He and his family lived in Bosnia during the first half of the war, until they were able to escape to Germany via a series of refugee camps, leaving their former lives (and extended family) behind. Beginning in March 2016, Anic was interviewed several times in Colorado Springs, Colorado, about what it was like to practice medicine, or attempt to, without reliable electricity or supplies for approximately one year.

Although this interview describes Anic’s experience in a conflict zone – sometimes referred to as a “complex humanitarian emergency” – conclusions can be drawn from his experience in the former Yugoslavia and applied to a prolonged power outage in the United States. The fact that a prolonged power outage would affect all critical infrastructure sectors is especially worrisome because of the

“interconnectedness” of these sectors. Anic described how the long-term power outages affected the various sectors and, therefore, healthcare responsibilities.

Hospitals, Physicians & Surgeons

Within 3-5 days, hospitals needed to adapt to the new normal – without electricity. The military was called in to provide support to hospitals, as many of the injured were also soldiers. The military medical units stayed intact with their own chain of command but supplemented and worked alongside the staff of the civilian hospitals. Throughout the war, hospital supplies were mostly provided by the military, but also by international humanitarian aid agencies. Depending on location, there was intermittent electrical power, perhaps a few hours per day. Central Bosnia was fortunate to have some of its power supplied by hydroelectric dams and their power stations.

Shelling structurally damaged hospitals, which markedly



increased the difficulty of providing care. Eventually these hospitals were abandoned and “buildings of opportunity” were set up to function as field hospitals. One of the best and most capable was located underground. Although the civilian medical staff was initially motivated to “come to work,” as their patriotic duty, the continued shelling of cities (and hospitals) changed this motivation over time.

Anic was able to go home at night to see his family, but others were not so fortunate. He was able to continue to take care of patients as long as there were supplies trickling in. Later in the war, confusion at the front lines made it difficult to distinguish friendly from enemy casualties, but casualties from all sides were treated at his hospital. Unless medical staff members were reassured that their families were taken care of, there was a steady loss of doctors and nursing staff over time.

Surprisingly, Anic stated that, “Surgeons continued to perform life- and limb-saving surgery even under very austere circumstances.” Trauma surgery outside the chest cavity and orthopedic injury were the most likely cases to be undertaken. However, not surprising, he stated, “the post-surgical infection rate increased and the mortality rates increased accordingly,” given the difficult conditions – for example, operating rooms without glass or even screens in the windows. In many cases, “anesthesia needed to be provided by an anesthesia tech or even with OJT (on the job training) for a medical assistant.” The ability to use an injectable anesthetic or even ether by a drip method, although extremely dangerous, was a useful skill to have. Unlike in the United States where a pack of sterile items is opened to use once and the rest discarded, he said that healthcare workers would, “plan on sterilization and re-use of single use items.”

Logistics, Barter & Exchange

“Elevators no longer worked. Stairs became the only access to upper floors in hospitals,” Anic said. Therefore, “there was an increased need for physical manpower to move patients up/down stairs.” This need for additional physical labor was also apparent in the aftermath of Katrina, which was highlighted in Fink’s book. Related to that event, in the urban environment, multi-story buildings presented a special hazard. “Patients or the elderly stuck several floors up in an apartment block were in

real trouble unless there was a coordinated effort to assist them.” Because of lack of communications, transportation, a means of exchange, and means of local production, everything became harder. “Taxi drivers became ‘kings’ or ‘generals’ for a variety of reasons: local knowledge, contacts, transportation, and communications,” he said.

Anic’s comments followed exactly with a book about the Yugoslavian War, “[Lie in the Dark](#)” by Foreign Correspondent Dan Fesperman. Anic further commented that, “Hard currency, preferably in large denomination notes (i.e., 100DM or US\$100) were still the best means of exchange.” Obviously, credit or debit cards did not work. Anic explained that, “coins were essentially useless; gold, jewelry, other similar tangibles did not work very well for trading either. Tobacco, cigarettes, alcohol, and coffee were always welcome in trade.” For a variety of uses, especially for radios and flashlights, batteries of standard types were also very welcome in trade.

According to Anic, “Some trade happened with weapons and ammunition; ammo was cheap and widely available but also heavy to carry in quantity.” Hospitals and physicians (and perhaps patients who require chronic lifesaving medication) should, “stockpile medications and medical supplies in advance, if possible.” Anic stated that they did not, “worry too much about expiration dates,” since most prescription medications are still safe and effective for some period beyond the expiration dates when kept in controlled environments. “Narcotics or illicit drugs were not exchanged in trade, as it was not a part of the culture,” he said. Finally, he stated with encouragement for any incident, “Remember this, somewhere, perhaps a long distance away, someone will have the resources you need. You just have to locate them.”

Communication, Transportation & Migration

The need for improved communications is the most frequently mentioned “after action” debriefing item in disaster after disaster. The same was true in the former Yugoslavia. Anic stated, “AM and FM broadcasts continued throughout the war. HAM



CBRNE-TERRORISM NEWSLETTER – May 2016

(amateur) radios were very helpful.” In fact, HAM radio links could be used to connect the local telephone system outside the conflict area, to pass messages to loved ones in another country.

In other communications, Anic said, “word of mouth information (rumors) passed amazingly fast, but it was not always accurate.” Because Anic was in the Bosnian military, he had access to the military communication systems. “The military always had communications and was one of the best sources of outside information, if you could access it.” There was some civilian use of handheld radios for local communications, but this was not always reliable. “Public safety and emergency services communications were severely stretched,” he said.

“Early on, there was mass migration of the population. Anyone who could get out early, did so.” For those left behind, just getting around was a major effort. “Roads were controlled by the military. You had to have documentation to travel.” For persons who still had access to automobiles, “all the gas stations were empty; gasoline/diesel was a very critical and very scarce resource.” As such, gasoline was one of the most sought after items of trade because any gasoline remaining in underground tanks was inaccessible unless electricity was available to run the pumps.

Particular to this conflict, “migration within Yugoslavia was for alignment by race, religion, and culture.” Throughout the conflict, there was still trading between the opposing factions. However, two groups moved in and out of the conflict area transporting people. First, “transportation for refugees provided by the United Nations (UN) was a Godsend but rare.” Second, “human smugglers were in high demand and became rich as a result of their services.”

Public Health & Wellbeing

Although few did it, “stockpiling of nonperishable food in advance turned out to be important,” Anic said. Food was either consumed quickly or used in trade, so lack of food caused people to migrate from one area to another. However, despite a few specific nutritional deficiencies, Anic saw no signs of obvious starvation. A complex disaster such as war still brings about some predictable patterns of disease. For example, he said that, “Water borne and food borne illnesses were frequently

on the rise. The elderly, pregnant women, and children were hit especially hard. Communicable disease increased in relationship to the duration of the emergency.” In contrast to some scenarios, “disposal of corpses turned out not to be such a risk for spread of infectious diseases, although the smell was horrific.” Many families had to bury their own. In addition, clean water was always in short supply, so those who did not have their own wells (with pump handles) had to “plan on carrying water some distance, each day.”

Anic is an amazingly resilient person. He was able to reflect back on some of his feelings during his time in the war zone, and experienced symptoms similar to post-traumatic stress disorder. He said that, “in a state of constant stress, you remain alert for possible threats,” yet “street smart (as opposed to book smart) people were much more resilient and better able to survive.” Unfortunately, those who were “nice, civilized people did not remain that way for very long.”

Weapons were ubiquitous in the former Yugoslavia, so snipers on the hillsides kept everyone in a constant state of fear. Surprisingly, people adapted and changed their patterns of behavior to accommodate that risk. Unfortunately, “weapons were equal to law” and “people were willing to use them for personal benefit.” Even this many years later, Anic said that it is still difficult for him to completely relax and is always in a semi-alarm or increased alert state.

Anic dealt with many life-and-death decisions during his time in the conflict zone. “Physicians and others did the very best they could for their patients, with what was at hand. There were many hard choices to be made.” Patients in severe pain without hope of survival posed particularly difficult scenarios. As humanitarian assistance medicine has become increasingly professionalized since the 2005 tsunami/earthquake in Indonesia and the 2010 earthquake in Haiti, disaster responders must abide by the “highest possible” standards of medical care. This assumes the possibility of re-supply of pharmaceuticals and other consumables, as well as free movement of healthcare workers into and out of the “conflict zone.” In the former Yugoslavia, this was not the case (re-supply or free movement) for prolonged periods.



CBRNE-TERRORISM NEWSLETTER – May 2016**Call to Action**

Although the experience that Anic and his family had was extreme and not as likely to occur in the United States, numerous other scenarios could result in an extended loss of power over a large geographic area. When that happens, hospitals will be especially vulnerable under current requirements, which include having only a limited number of days of fuel for the emergency electrical generation system. For example, during Hurricane Sandy in 2012, at least one large hospital lost power and had to close and evacuate its patients, so such

requirements are being reviewed and updated as needed.

Education about the vulnerability of the power grid – especially for emergency planners and other policy makers – is essential. In addition, a continued call for preparedness at a variety of levels (individual, family, community, medical staff, and other hospital staff) would save many lives. In general, the concept of resilience – that is, to be able to “take a punch in the mouth and still remain standing,” to paraphrase Mike Tyson – is essential for healthcare institutions that plan to continue to provide healthcare during and after a disaster.

James Terbush, MD, MPH, belongs to an FBI sponsored organization Infragard EMP-SIG, which is focused on several specific threats such as a prolonged and widespread power outage. He was previously (2012-2014) the medical lead for Innovation and Experimentation, Science and Technology Directorate, North American Aerospace Defense Command (NORAD), and United States North Command. His particular area of interest is in protection of public health and healthcare critical infrastructure.

Dr. Rajko Anic graduated with a Doctorate of Medicine in 1988 from the University of Sarajevo, Bosnia and Herzegovina (former Yugoslavia). During the breakup of Yugoslavia, he was living and practicing medicine in Bosnia until 1993, when he left hometown of Zenica to move with his family to Germany. In 1999, he and his family emigrated to the United States (Colorado Springs, Colorado). Since 2004, he has been working for El Paso County Public Health. He proudly became a U.S. citizen in 2005.

The Role Of Emergency Services in Emergency Scenarios

By Eyal Harel

Source: <http://i-hls.com/2016/05/the-role-of-emergency-services-in-emergency-scenarios/>



May 19 – Last Tuesday a dangerous substance leaked from a vehicle in a main street of one of the neighborhoods in Jerusalem. The incident caused great panic and uncertainty as to how to conduct. The incident took place during the morning, where there is much traffic with private vehicles, the

light rail passing nearby, schools and shopping centers around. Instructions were to stay home and turn off the air conditioning – and we should remember that these are very hot days. Unfortunately the incident did not occur the day before, when Jerusalem saw a



CBRNE-TERRORISM NEWSLETTER – May 2016

heat wave. Had it did, an instruction to close the air conditioning would have made the levels of anxiety and chaos rise even higher.

The responsibility for managing such an incident is the Israeli Police, as stated by a law for emergency management in fields in which it is in charge of home security. The incident combines many different services, from the fire department, to medical and rescue services, to the ministry of environmental protection, and of course the local authorities.

When looking at how local authorities are organized to handle such incidents, it's clear that some authorities are more accustomed to different scenarios than others, therefore tools should be given to authorities and their heads to handle different scenarios. Such activity is led by the ministry of defense's national emergency management authority, along with the home front command, which have established the "school for national firmness", which is designed to instruct governmental offices, local authorities and various emergency services who deal with emergency response.

The local authority is the one who knows the terrain and the citizens best, and this is of great importance: The entire force must use the local authority's knowledge and allow its head to play an inseparable part in managing the event.

Terror attacks in the past several years, especially in the city of Jerusalem, have brought about excellent cooperation between emergency services and the local authority.

Of great importance is the clear and immediate instructions to the public in order to save lives and prevent further damage. The issue of spokespersonship and public education has been

led for many years by the home front command, but recently there has been a change in the police and ministry of public security, and with it an understanding that the police, controlling and instructing during such scenarios, should also be the one to issue the instructions to the public. The home front command is not prepared to answer emergency events during routine, as it involves recruiting or transferring forces, but the police is everywhere and is first to arrive and the scene and control the event.

There is great importance in passing on the lessons from different events to different authorities in the country so that they could adjust current protocols of handling various scenarios required from the authority during an incident.

These emergency scenarios erupt into our lives with no warning and require that professionals trained by courses and academic classes will command and manage them. It is important to hold professional conferences which deal with different scenarios alongside the activity led by the national emergency management authority. People in charge of such matters in local authorities, governmental offices, and other organizations must be required to participate in conferences and seminars, and be academically and practically authorized.

In Israel today there is no training at a graduate degree level for emergencies (except in Beit Berl which is offering such training as part of the studies for national security), only post-graduate. This does not offer enough depth and I hope that someday such an initiative will take off and offer professional training for everyone in the field.

Eyal Harel was until recently head of the national security council's division for home and home front security, and was the first manager of the Israeli government's national crisis management center as well as a member of the inter-ministerial committee for earthquake preparedness.





A rising tide of migration

Source: <http://www.homelandsecuritynewswire.com/dr20160503-a-rising-tide-of-migration>

May 03 - **“With sea levels on the rise, several island nations are scrambling to stay above water and ensure citizens will have a place to go when the ocean engulfs their homeland. The humanitarian-crisis phase of climate change has officially begun.”**

Eric Holthaus, a meteorologist who writes about weather and climate for *Slate*, opens a new article written for the *Columbia Law School Magazine* with that dire statement.

Columbia University says that it is not an unforeseen situation. He notes that in 1990, the UN’s Intergovernmental Panel on Climate Change laid out the prospects for environmental change under global warming, if nothing is done to curb the use of fossil fuels. In the panel’s first assessment, the scientists on the panel wrote: “These changes could initiate large migrations of people, leading over a number of years to severe disruptions of settlement patterns and social instability in some areas.”

Here we are in 2016. And not much has improved.

“Not only is it obvious that the UN panel was correct, but it is also indisputable that we have since made things worse,” Holthaus writes. “Four other assessments and more than a quarter-century later, global carbon emissions are still soaring — up more than 60 percent, and in line with what is considered a worst-case scenario.”

Holthaus spoke with several people at the Sabin Center for Climate Change Law, who

have been investigating the impact of these issues on international law — and the ways international law can be brought to bear.

“I think the countries of the world need to start thinking seriously about how many people they’re going to take in,” says Michael Gerrard, director of the Sabin Center. “The current horrific situation in Europe is a fraction of what’s going to be caused by climate change.” And, Gerrard notes, “One thing I’ve learned in the work that I’ve done is that a place becomes uninhabitable well before it’s submerged.”

Gerrard and others in the piece discuss the UN’s role in addressing the issue, and how nations can settle issues like what happens to people’s rights when their country disappears underwater. Even trickier: What responsibility developed nations who have been most responsible for climate change, including the United States, should have for helping out. Who will take in the inevitable climate refugees is a hugely sticky question, especially here in this election year.

Holthaus continues: “In total, **climate change may displace up to a quarter-billion people by 2050**, according to research cited by the Office of the United Nations High Commissioner for Refugees. That means, within our lifetimes, climate change could become a human rights emergency that grinds global governance to a halt. How the global community chooses to address this seemingly inevitable problem will help define international relations for the rest of this century.”

— Read more in Eric Holthaus, “The Rising Tide,” [Columbia Law School Magazine](#) (May 2016).

Climate-exodus expected as temperatures rise in Middle East, North Africa

Source: <http://www.homelandsecuritynewswire.com/dr20160504-climateexodus-expected-as-temperatures-rise-in-middle-east-north-africa>

May 04 – The number of climate refugees could increase dramatically in future. Researchers of the Max Planck Institute for Chemistry and the Cyprus Institute in Nicosia have calculated that the Middle East and North

Africa could become so hot that human habitability is compromised.

The goal of limiting global warming to less than two degrees Celsius, agreed at the recent UN



CBRNE-TERRORISM NEWSLETTER – May 2016

climate summit in Paris, will not be sufficient to prevent this scenario. The temperature during summer in the already very hot Middle East and North Africa will increase more than two times faster compared to the average global warming. This means that during hot days temperatures south of the Mediterranean will reach around 46 degrees Celsius (approximately 114 degrees Fahrenheit) by mid-century. Such extremely hot days will occur five times more often than was the case

daytime they could rise to 46 degrees Celsius (approximately 114 degrees Fahrenheit). By the end of the century, midday temperatures on hot days could even climb to 50 degrees Celsius (approximately 122 degrees Fahrenheit). Another finding: Heat waves could occur ten times more often than they do now.

By mid-century, 80 instead of 16 extremely hot days

In addition, the duration of heat waves in North Africa and the Middle East will prolong dramatically. Between 1986 and 2005, it was very hot for an average period of about 16 days, by mid-century it will be unusually hot for 80 days per year. At the end of the century, up to 118 days could be unusually hot, even if greenhouse gas emissions decline again after 2040. "If mankind continues to release carbon dioxide as it does now, people living in the Middle East and North Africa will have to expect about 200 unusually hot days, according to the model projections," says Panos Hadjinicolaou, Associate

Professor at the Cyprus Institute and climate change expert.

Atmospheric researcher Lelieveld is convinced that climate change will have a major impact on the environment and the health of people in these regions. "Climate change will significantly worsen the living conditions in the Middle East and in North Africa. Prolonged heat waves and desert dust storms can render some regions uninhabitable, which will surely contribute to the pressure to migrate," says Lelieveld.

The research team recently also published findings on the increase of fine particulate air pollution in the Middle East. It was found that desert dust in the atmosphere over Saudi Arabia, Iraq and in Syria has increased by up to 70 percent since the beginning of this century. This is mainly attributable to an increase of sand storms as a result of prolonged droughts. It is expected that climate change will contribute to further increases, which will worsen environmental conditions in the area.

In the now published study, Lelieveld and his colleagues first compared climate data from 1986 to 2005 with predictions from 26 climate models over the same

at the turn of the millennium. In combination with increasing air pollution by windblown desert dust, the environmental conditions could become intolerable and may force people to migrate.

The Max Planck Institute notes that more than 500 million people live in the Middle East and North Africa — a region which is very hot in summer and where climate change is already evident. The number of extremely hot days has doubled since 1970. "In future, the climate in large parts of the Middle East and North Africa could change in such a manner that the very existence of its inhabitants is in jeopardy," says Jos Lelieveld, Director at the Max Planck Institute for Chemistry and Professor at the Cyprus Institute.

Lelieveld and his colleagues have investigated how temperatures will develop in the Middle East and North Africa over the course of the twenty-first century. The result is deeply alarming: Even if Earth's temperature were to increase on average only by two degrees Celsius compared to pre-industrial times, the temperature in summer in these regions will increase more than twofold. By mid-century, during the warmest periods, temperatures will not fall below 30 degrees at night, and during



CBRNE-TERRORISM NEWSLETTER – May 2016

time period. It was shown that the measurement data and model predictions corresponded extremely well, which is why the scientists used these models to project climate conditions for the period from 2046 to 2065 and the period from 2081 to 2100.

Largest temperature increase in already hot summers

The researchers based their calculations on two future scenarios: The first scenario, called RCP4.5, assumes that the global emissions of greenhouse gases will start decreasing by 2040 and that the Earth will be subjected to warming by 4.5 Watt per square meter by the end of the century. The RCP4.5 scenario roughly corresponds to the target set at the most recent UN climate summit, which means that global warming should be limited to less than two degrees Celsius.

The second scenario (RCP8.5) is based on the assumption that greenhouse gases will continue to increase without further limitations. It is therefore called the “business-as-usual scenario”. According to this scenario, the mean surface temperature of the Earth will increase

by more than four degrees Celsius compared to pre-industrial times.

The Max Planck Institute notes that in both scenarios, the strongest rise in temperature in the Middle East and North Africa is expected during summer, when it is already very hot, and not during winter, which is more common in other parts of the globe. This is primarily attributed to a desert warming amplification in regions such as the Sahara. Deserts do not buffer heat well, which means that the hot and dry surface cannot cool by the evaporation of ground water. Since the surface energy balance is controlled by heat radiation, the greenhouse effect by gases such as carbon dioxide and water vapor will increase disproportionately.

Regardless of which climate change scenario will become reality: both Lelieveld and Hadjinicolaou agree that climate change can result in a significant deterioration of living conditions for people living in North Africa and the Middle East, and consequently, sooner or later, many people may have to leave the region.

— Read more in J. Lelieveld et al. “Strongly increasing heat extremes in the Middle East and North Africa (MENA) in the 21st century,” *Climatic Change* (23 April 2016).

Water 4.0—the next revolution in urban water systems

Source: <http://phys.org/news/2016-05-40the-revolution-urban.html>

May 13 – In his 2014 book, *Water 4.0*, UC Berkeley environmental engineer David Sedlak identifies four “revolutions” in the development of urban water systems. The **first revolution** — Water 1.0 — was the Roman innovation of piping potable water in and sewage out of population centers, an advance adopted throughout European and North American cities. The **second revolution** — treating drinking water to kill infectious microbes — protected millions of urban dwellers from cholera, typhoid and other diseases transmitted through the very success of Water 1.0.

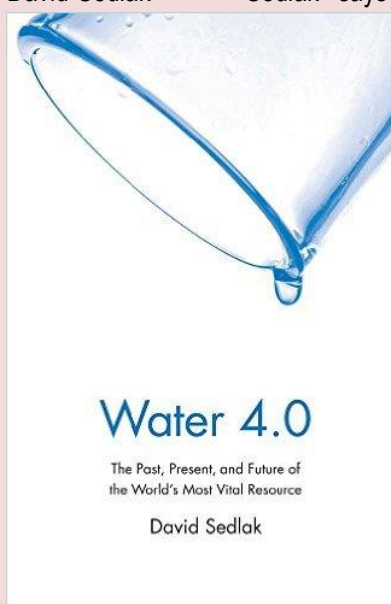
Water 3.0 saw widespread adoption of sewage treatment plants. UC

Berkeley reports that now, half a century later, Sedlak says we need a fourth revolution.

Soaring urban populations and a changing climate create chronic water shortages in some cities and too much water in others. Some contaminants may pose hazards in extraordinarily small concentrations. And aging pipe networks threaten the health of entire communities, as seen this year in Flint, Michigan.

“The current system that we rely upon to manage water in our cities is not up to the challenges of the twenty-first century. The

technologies to make urban water



CBRNE-TERRORISM NEWSLETTER – May 2016

systems more secure already exist. It's up to us to build the next version of the water system."

Sedlak's research tracks the fate of chemical contaminants in wastewater. For the past twenty years, he has led field studies to detect and measure the presence of compounds that are particularly resistant to breakdown by chemical treatment or natural bacteria.

He was one of the first environmental engineers to discover the potential threats posed by natural and synthetic hormones that persist in water after conventional sewage treatment. The hormones are considered

In 1997, Sedlak discovered that hormones that are excreted in urine, such as estradiol, don't break down in sewage treatment plants, or in the rivers downstream of the treatment plants.

Berkeley notes that David Sedlak's popular book explores the serious water treatment, supply and security challenges we now face, and proposes how to meet them.

Pumping treated water into wetland ponds rids the water of most natural and manmade hazards. Cattails and other aquatic plants soak up nitrogen, and bacteria speed decomposition. But Sedlak found that some antibiotics as well as estradiol resist

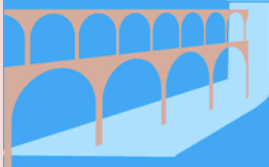
Water 4.0 *The Past, Present, and Future of the World's Most Vital Resource*

From the Yale Press Log's interview with Author David Sedlak

Water 1.0

imported water supply and water as a means of waste disposal

"The dilution of feces and urine made it impossible to capture and reuse the nutrients locked up in the wastes. By discharging sewage above a neighbor's drinking water supply, the first set of innovations also spread waterborne disease to downstream communities."

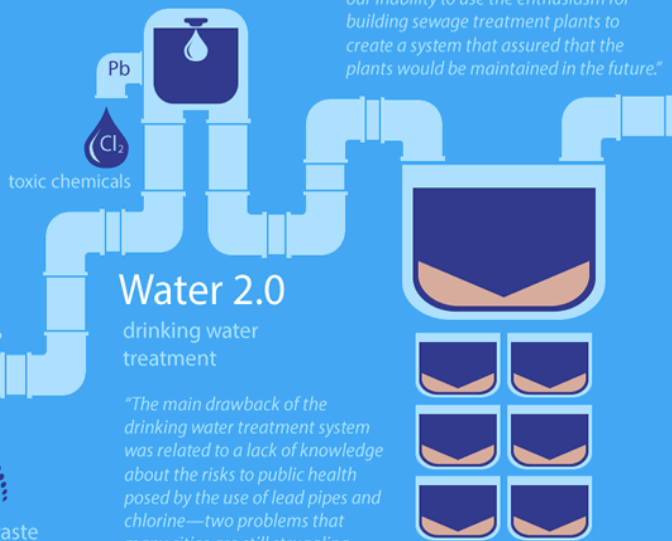


~312 BCE

Water 2.0

drinking water treatment

"The main drawback of the drinking water treatment system was related to a lack of knowledge about the risks to public health posed by the use of lead pipes and chlorine—two problems that many cities are still struggling with today."



~1890 CE

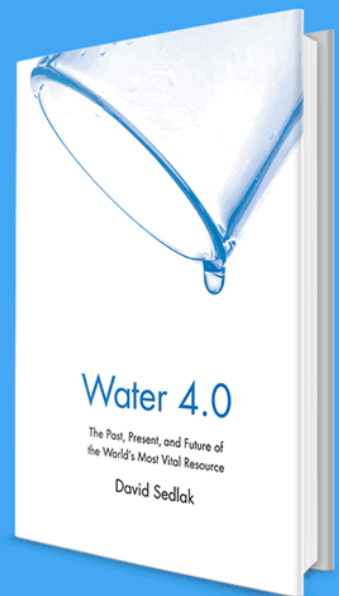
Water 3.0

widespread construction of sewage treatment plants

"Here, the main drawbacks were related to our inability to use the enthusiasm for building sewage treatment plants to create a system that assured that the plants would be maintained in the future."



~1940 CE



The little-known story of the systems that bring us our drinking water, how they were developed, the problems they are facing, and how they will be reinvented in the near future

Yale UNIVERSITY PRESS

endocrine disruptors. In concentrations as low as a few part-per-trillion, they have been shown to derail normal development in fish, causing males to be feminized. For this and other pioneering research he was elected this year to membership in the National Academy of Engineering.

Removing hormones from water supplies

decomposition. He recognized that the natural wetlands vegetation shaded much of the ponds' surfaces, blocking sunlight that could otherwise speed decomposition of remaining contaminants.

He and his Berkeley colleague Alexander Horn designed what they call open wetlands to add a new stage of water treatment. Sheets of plastic line the bottom of



CBRNE-TERRORISM NEWSLETTER – May 2016

the manmade ponds, preventing aquatic plants from proliferating.

“The water gets blasted by sunlight, which breaks up the most compounds,” he says. As a side benefit, algae and bacteria grow on the plastic liner beneath the ponds and degrade otherwise-resistant chemicals.

Three years ago, Sedlak was part of a team that built a 40-acre scale model open wetland pond along the Santa Ana River in Southern California, designed to break down hormones and other contaminants before the water was released to the river. Early data show that the demonstration-scale system works as well as the smaller systems that his team had studied near the Berkeley campus.

Taking on complex water problems from several angles

Sedlak co-directs the Berkeley Water Center, along with Isha Ray, a professor in UC Berkeley’s Energy and Resources Group.

Leaders are always drawn from faculty in engineering as well as the social sciences or natural resources fields to assure the center will attack complex water problems with expertise from very different disciplines.

Center researchers will take on some of CERC-WET’s challenges. Sedlak will focus on the minerals and salts that form a concentrated residue as they are extracted in the treatment process.

“We have amazing technology for removing salts and minerals both from drinking water and water used for cooling at power plants. But we end up creating a waste stream of these chemicals. The management of this concentrate is becoming a real challenge. It turns out to be a huge volume.

“We hope that our collaboration with Chinese researchers in CERC-WET can help us find better ways to remove and maybe even recover valuable materials.

— *Read more in David Sedlak, [Water 4.0: The Past, Present, and Future of the World’s Most Vital Resource](#) (Yale University Press, 2015).*

Addressing global food system challenges

Source: <http://www.homelandsecuritynewswire.com/dr20160510-addressing-global-food-system-challenges>

May 10 – **Agriculture now produces more than enough calories to meet basic human dietary needs worldwide. Despite this seeming abundance, one out of eight people do not have access to sufficient food.**

A new study, “Realizing Resilient Food Systems,” published in the journal *Bioscience* and led by Meagan Schipanski, assistant professor of soil and crop sciences at Colorado State University, presents a set of strategies to address these complex challenges of producing food for a growing global population, while reducing environmental impacts and increasing resilience in the face of climate change.



CSU says that Schipanski led a collaborative team of researchers from the United States and Canada to produce the study, which was supported by funding from the U.S. Department of Agriculture and CSU’s School of Global Environmental Sustainability.

“Addressing our food system challenges requires so much more than increasing food production,” Schipanski said. “We hope that highlighting real world examples that connect food production with positive outcomes for human health will encourage more work across traditional disciplinary lines and direct engagement with communities.” Food systems

“Addressing our food system challenges requires so much more than increasing food production,” Schipanski said. “We hope that highlighting real world examples that connect food production with positive outcomes for human health will encourage more work across traditional disciplinary lines and direct engagement with communities.” Food systems



CBRNE-TERRORISM NEWSLETTER – May 2016

include consideration of how food is produced, how it is distributed, what is consumed, and who influences these different activities.

Food access disparities

Although there have been significant increases in global crop production, the number of undernourished people in undeveloped countries has not declined. Food prices are more variable in less developed countries, and there are simultaneous diet-related health challenges of malnutrition and over-consumption both within the United States and around the world. The root causes of many of these challenges are often less about having enough food and more about poverty and access to resources, particularly women's access to education and resources.

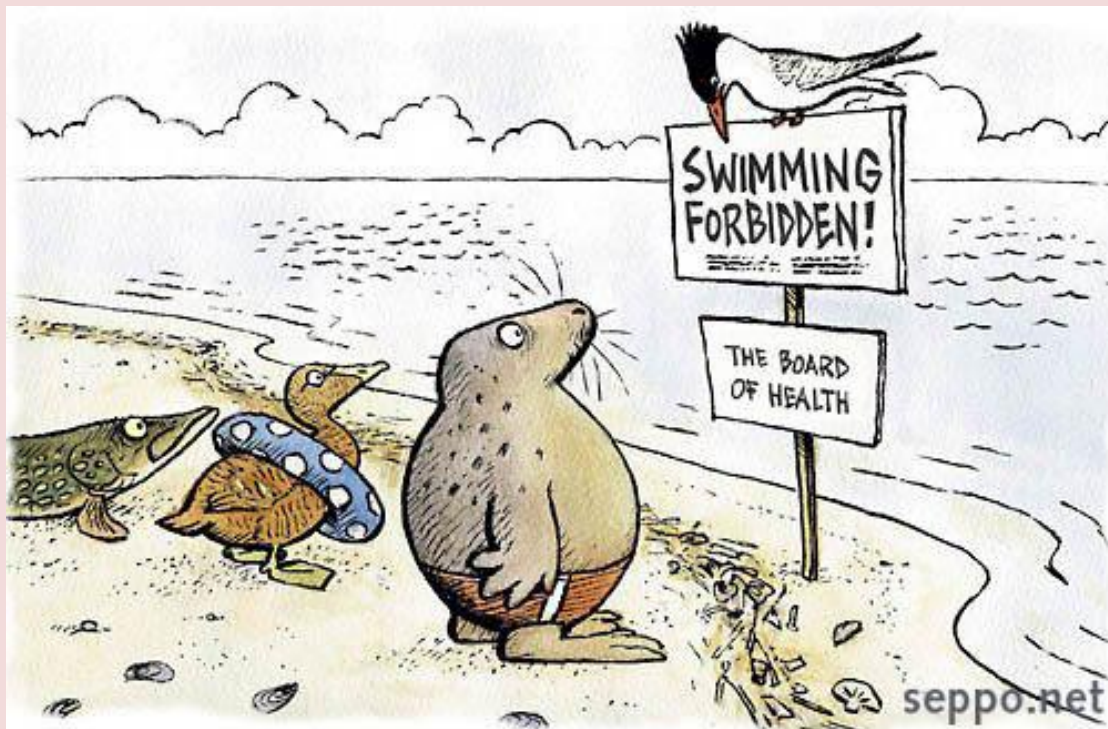
Global case studies

Using case studies from Africa, India, and Brazil, the study highlights the importance of integrated food system strategies. For example, efforts in Malawi have improved human nutrition by integrating more legumes in crop production practices with health and nutrition education. Brazil implemented national

programs in 2003 that link rural producers to low-income urban consumers, improving farmer incomes and access to nutritious foods in urban areas. In India, increasing women's access to land and other resources has resulted in benefits for family health and education.

"Meagan's food system study is a clear example of global knowledge converging from the three dimensions of sustainability: economics, society and the environment. It is a novel and useful effort by her integrating team," said Diana Wall, director of the School of Global Environmental Sustainability and a professor in CSU's Department of Biology.

CSU notes that the Food Systems Research Group is one of several interdisciplinary teams funded and supported by the School of Global Environmental Sustainability. The team facilitates systems-based research to address the challenge of improving global food accessibility while reducing agriculture's environmental impacts.





Risk & Costs of **Not Having** a Business Continuity Management Program

By Chris Britton

Source: <http://www.rockdovesolutions.com/blog/risk-costs-of-not-having-a-business-continuity-management-program>



May 18 – Considering the number of threats that organizations face today, it may be surprising to learn that the majority of companies are not prepared for a business-affecting emergency. Unfortunately, it's true: The Disaster Recovery Preparedness Council found that [nearly three quarters of organizations worldwide](#) aren't properly protecting their data and systems.

The potential consequences of not having a business continuity management program are extremely grave. Consider the many risks that your company faces: network outages, natural disasters, active shooter events, data breaches and more. However, if your organization doesn't take business continuity seriously, you're facing even greater risks, including the following:

1) Business failure.

Many companies that aren't effectively prepared for disaster situations simply cannot bounce back from a significant crisis. In fact, up to 80 percent of businesses fail within 18 months after a major disaster, according to the Business Continuity Institute. The good news is that [research shows](#) companies with business continuity planning recover faster and more effectively following an emergency.

2) Injury and death.

In natural disasters, violent incidents and other dangerous emergencies, the safety of your employees, visitors, customers and other individuals becomes a very real concern. This is particularly true in organizations without an effective business continuity plan. Companies that use traditional, hard-copy planning methods often fail to effectively communicate with stakeholders during an emergency, which

leaves them ill equipped to respond to the situation at hand.

3) Financial loss.

Data breaches, server downtime, weather emergencies and other crises can be extremely costly, especially when you haven't made a plan to mitigate unnecessary financial damage. Over a five-year period, [businesses lost more than \\$70 million](#) due to downtime alone—and that doesn't take into account the other causes of financial loss, such as insurance claims, lost product and public relations efforts.

4) A tarnished reputation.

A company's response to a crisis can have a huge impact on the way their customers and the public views it. Following a data breach, people may perceive it as unsecure. In the wake of a social media gaffe,



CBRNE-TERRORISM NEWSLETTER – May 2016

they might feel that the company is untrustworthy. There are a million ways in which crisis can alter your public perception, and it's important to be prepared.

A major component of reputation management is your [communications plan](#) and seamless communication with stakeholders. As a crisis unfolds, a breakdown in communication such as rapid and responsive announcements to the press can make it more difficult to manage and recover your reputation. Your brand can come out of the crisis with a positive reputation if you stay ahead of the media and shape the conversation. Your stakeholders need to be armed with the most up-to-date information—especially if they will be making announcements to the press, posting on social media or communicating with other stakeholders.

5) Lost productivity.

[In a 2014 study](#), 78 percent of companies reported losing one or more mission-critical applications at some point—and 28 percent lost the use of a data center for more than a week. This kind of significant disruption has a trickle-down effect throughout an organization, slowing down productivity and damaging various aspects of the business. Sales are no longer converted, customer service suffers and the impact of the crisis continues to grow.

Even if a company is able to keep its doors open following this type of event, the impact would be significant. That's why it is important to empower your employees and other stakeholders with the most up-to-date, relevant information possible. One of the best ways to do this is to use a [mobile app for business continuity](#) management and emergency communications.

6) Improved Communication for Greater Continuity

It's clear that organizations require a business continuity plan in order to recover from the myriad of threats they may encounter. But it's not enough to simply create a plan and then store it on a shelf where no one can make full use of it.

[In a recent study](#), IBM found that business continuity professionals thought only about 60 percent of their employees would know what to do during a crisis. However, by leveraging newer plan distribution and emergency communications techniques, your organization can be better equipped to thrive through any crisis.

Today, a growing number of organizations have incorporated mobile technology into their business continuity planning, which enables them to more effectively reach their employees and other stakeholders through their smartphones or tablets. All business continuity planning information, such as contact lists, protocol files and maps, are available through a mobile app. The crisis response team can send alerts and updates in real time, as the crisis unfolds, which helps to protect individuals from dangerous situations, direct them to safety and streamline crisis response.

Since information is more readily available for each stakeholder, the company is able to return to normalcy more quickly and more effectively, without experiencing the risks mentioned above.

**How prepared is your company for a business-disrupting event?
Would you say your employees know what to do in a crisis?**

