Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

CBRNE-Terrorism Newsletter

December 2017

Happy New Year

www.cbne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

National Progress Report: United Arab Emirates

Source: http://www.nss2016.org/document-center-docs/2016/3/31/national-progress-report-united-arab-emirates

March 2016 – Since the 2014 Nuclear Security Summit, the UAE has strengthened nuclear security framework and its implementation in the country while contributing to the development of global nuclear security architecture by…

Strengthening Nuclear and Other Radioactive Material Security

The Government of the UAE has developed an effective nuclear security regime in line with the development of its peaceful nuclear power programme. UAE will host an International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) Mission in 2016, which will review the physical protection system in the UAE and compare it with international guidelines and internationally recognized best practices.

Nuclear Security

UAE has endorsed the Amendment of the Convention of the Physical Protection of Nuclear Material (CPPNM). Although the amendment has not yet entered into force, UAE regulation and regulatory guides have been developed in compliance with the Convention's amended requirements.

The regulation for the Physical Protection of Nuclear Materials and Nuclear Facilities, issued in 2010, and its associated regulatory guides have been established in accordance with the IAEA Nuclear Security Series publications, in particular the Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities publication (INFCIRC/225/Rev.5).

Since 2014, two new regulatory guides were developed and issued in regards to the security of the transport of nuclear material and to the contingency plan required at a nuclear facility.

In 2014, UAE hosted an IAEA workshop on the security of transport of nuclear materials.

Radiological Security

The UAE regulation for the security of radioactive sources has been developed in accordance with the Code of Conduct on the Safety and Security of Radioactive as well as the related IAEA safety and security standards, which the Government of the UAE endorsed

After the issuance of the regulation (FANR regulation 23) in 2011, licensees managing category 1 to 3 radioactive sources in the UAE were required to implement it immediately. Since then all required nuclear security plans were reviewed and approved by the regulator, and inspections of all concerned licensees were achieved to verify the implementation and conformance with the new regulation.

Information Protection and Cyber Security

The Information Protection Program Operating Manual (IPPOM), defining the management of sensitive nuclear information in the UAE, was updated and is currently implemented by relevant entities in the nuclear sector such as Federal Authority for Nuclear Regulation (FANR), Emirates Nuclear Energy Corporation (ENEC) and Critical Infrastructure and Coastal Protection Authority (CICPA).

UAE Regulation and the associated regulatory guides are based on the IAEA publication, Protection against cyber-attack has been taken into account in various FANR regulations developed between 2009 and 2015.

The UAE hosted an IAEA national workshop on cyber security in 2014.

Countering Nuclear Smuggling

To meet the requirements of import and export control rules, the UAE nuclear regulator, FANR has issued in 2014 an updated Regulation on the Export and Import Control of Nuclear Material, Nuclear Related Items and Nuclear Related Dual-Use Items.

The Government of the UAE is an active member in the international information sharing on the illicit trafficking of nuclear materials through its participation of the IAEA Incident and Trafficking Database (ITDB).

The UAE participated and supported the convening of IAEA sub-regional meeting on nuclear security information exchange and coordination in October 2015 in Kuwait. This meeting, aimed at strengthening national, regional and international capacity to prevent and combat illicit trafficking in nuclear and other radioactive material through enhanced information cooperation.

Supporting Multilateral Instruments

The Government of the United Arab Emirates strongly supports the universal implementation of the International Convention on Suppression of Acts of Nuclear Terror (ICSANT), as well as the Convention on Physical Protection of Nuclear Materials (CPPNM) and its 2005 Amendment.

The UAE provided to the United Nations (UN) 1540 Committee, its national report as well as the associated matrix.

The UAE law, regulations and regulatory guides which are enforced have been established in accordance with the amended CPPNM, UAE continues to promote the entry into force of amended CPPNM at international and regional venues.

Collaborating with International Organizations

The Government of the UAE supports the activities of the IAEA through ongoing participation at workshops, Nuclear Security Guidance Committee meetings and by providing experts to meetings regarding the development of Nuclear Security Series publications.

UAE is an active promoter and participant of the (IAEA) Network for Nuclear Security Training and Support Centres - NSSC Network. UAE hosted a Regional Training Course on Introduction to Nuclear Forensics in Dubai in October 2015.

An Integrated master Working Plan (IWP) was signed in 2013 between the UAE and the IAEA, which aims to enhance, for the period of 2013-2017, the efficiency and effectiveness of the partnership between the UAE and the IAEA, including in the nuclear security domain.

For ensuring the sustainability of its nuclear security regime, an Integrated Security Support Plan (INSSP) for UAE was signed in August 2012 between the UAE and IAEA and continued to be implemented through 2016

The UAE has received an IAEA International SSAC Advisory Service (ISSAS) in May 2014 and an Emergency Preparedness Review (EPREV) mission in March 2015. The ISSAS mission covers all aspects of nuclear material safeguards implementation including export control, and nuclear material accounting.

The UAE hosted in Abu Dhabi, the Inter-Arab Nuclear Detection and Response Exercise, FALCON, in February 2016, which aimed at promoting regional approaches in matters of nuclear detection and response to nuclear and other radiological threats and enhancing national and regional interagency coordination and cooperation. The exercise has been developed under the framework of the European Union (EU), Chemical Biological Radiological Nuclear (CBRN) Centers of Excellence (CoE) Initiative by the United Nations Interregional Crime and Justice Research Institute (UNICRI), in partnership with the UAE, the Hashemite Kingdom of Jordan, the Kingdom of Morocco, the European Commission and the Global Initiative to Combat Nuclear Terrorism (GICNT).

Partnering with External Stakeholders

With regard to bilateral agreements on nuclear security, the UAE has concluded a number of nuclear cooperation agreements in support of its civil nuclear power programme. To date, 9 bilateral agreements have been concluded. In addition, multiple MoUs have been signed between FANR, the nuclear regulator and several foreign entities. Such arrangements allowed for further cooperation in areas including nuclear security and continued to be valuable interface for cooperation and knowledge exchange in relation to nuclear security.

The UAE in cooperation with USA entities established the Gulf Nuclear Energy Infrastructure Institute (GNEII) in Abu Dhabi, an educational institution that

provides classroom instruction and hands-on experience in nuclear energy safety, security, safeguards and non-proliferation. GNEII is associated with Khalifa University of Science Technology and Research.

Coping after a big nuclear accident

By Philip Thomas and John May

Process Safety and Environmental Protection; Volume 112, Part A, November 2017, Pages 1–3

Source: http://www.sciencedirect.com/science/article/pii/S0957582017303166

Society's extensive figurative vocabulary of nuclear terms demonstrates just how far atomic energy has permeated the public's consciousness and imagination, in a way matched by few other scientific discoveries. Hence we can understand perfectly well a news report saying that the stock market has had a "meltdown" and we grasp immediately that the political "fallout" could be significant if the number of firms affected has reached a "critical mass". But how do we cope when an actual nuclear reactor melts down and deposits a significant amount of radioactive fallout over the surrounding area? Exactly this happened at Chernobyl in April 1986, where to make matters worse, the reactor went super prompt critical for a few seconds[1], depositing a large amount of additional heat into the core. A quarter of a century later, another very large radioactive release occurred at the Fukushima Daiichi nuclear power station. Here the operating reactors were shut down as soon as the Tohoku Earthquake was detected but the tsunami following on close behind knocked out the reactor cooling systems needed to remove decay heat. The fuel assemblies overheated and reacted with steam to produce hydrogen gas, which led to explosions in the reactor buildings and the release of radionuclides into the environment.

In both cases, the authorities' principal response for protecting the public was to move large numbers of people away from the surrounding area. A total of 335,000 were relocated after Chernobyl, never to return. Meanwhile after the accident at Fukushima Daiichi, 111,000 people were required to leave areas declared as restricted and an additional 49,000 joined the exodus voluntarily; about 85,000 had not returned to their homes by 2015. Were these sensible policy reactions? Was there an alternative? How should we respond to a big nuclear accident in the future? These were the questions behind the multi-university NREFS research study – Management of Risk Issues: Environmental, Financial and Safety – carried out for the Engineering and Physical Sciences Research Council as part of the UK-India Civil Nuclear Power Collaboration (NREFS, 2015). This Special Issue carries the 10 closing papers from that project.

The NREFS approach is predominantly quantitative, and Thomas (2017a) outlines the methods used and the results obtained, and recommends such mathematically based methods as aids to penetrating the fog of uncertainty and confusion following a major nuclear accident. They should, Thomas suggests, provide the basis for making decisions that will do more good than harm. He calls for the demystification of nuclear accidents and specifically for decision makers to be aware in advance that they should not adopt blindly the strategies used to manage past severe nuclear accidents. Using available data on the health consequences of the two severe nuclear events discussed above, the NREFS project has shown these strategies to be excessive in view of the actual, as opposed to feared, level of radiological risk faced by the public.

Waddington et al. (2017a) find that the numbers relocated after both the Chernobyl and Fukushima Daiichi accidents were very much too high. (They use the term "relocation" to imply that the people concerned will live away from a designated exclusion zone for a substantial period of time, after which return to the original location starts to become problematical.) Based on the Judgement- or J-value method, between 5 and 10 times too many people were moved away from the Chernobyl area between 1986 and 1990, and the authors find it difficult to justify moving anyone away from Fukushima Daiichi on grounds of radiological protection. The analysis is retrospective, and so blame is not apportioned to the authorities concerned. However, the authors suggest that the findings should be taken into account in future decision making. They go further and suggest that

more comprehensive radiological data collection could be fed 'on the fly' into the analysis during an accident to assess the potential effectiveness of candidate decisions. Some thought-provoking comparative statistics on life expectancy are also provided between the Chernobyl region after the world's worst nuclear accident and the UK in the 21st century. The authors suggest that the 900 people most under threat from radiation if they had not moved out in the 2nd relocation from Chernobyl in 1990 would have lost just 3 months' life expectancy if they had stayed in situ. Meanwhile the 6800 people who faced the highest radiation dose, had they not been moved out in the 1st Chernobyl evacuation of 1986, would have lost 3 years or more of life expectancy, with 5.6 years constituting the average reduction. These numbers are then compared with

- the 4½ months life expectancy lost by the average Londoner to air pollution (9 months for infants);
- the 3¼ years difference in life expectancy between the average person living in Harrow, North London and his/her counterpart in Manchester; and
- the 8.6 years of life that baby boys born in Blackpool lose compared with those born in London's Kensington and Chelsea.

The J-value is a new approach (validated for 90% of the world's nations during the course of the NREFS study) that balances safety spending against the extension of life expectancy it brings about. It improves on currently used methods by introducing greater objectivity as a result of its incorporation of the life-quality index (Nathwani and Lind, 1997) at its core. This allows the monetisation of future years of life using GDP per head plus an appropriate value of risk-aversion (Thomas, 2016, gives a discussion of risk-aversion and its development as an economic parameter over the past 300 years). The J-value is found by dividing the actual cost of the safety measure by the maximum that can be spent before life quality declines, implying that the expenditure is justified when J is less than 1.0. The J-value possesses the considerable advantage in the nuclear context that, unlike other approaches, it allows loss of life both in the short and in the long term (as a result of radiation exposure, for example) to be measured on the same scale.

The broad thrust of the J-value findings is backed up by two other NREFS studies that employed different and diverse assessment methods. Yumashev et al. (2017) apply Bellman's principle of optimality to determine the best decisions to be taken after a large range of big nuclear accidents. They find relocation not to be a sensible policy measure in any of the hundreds of base case scenarios they examined; it is rarely optimal in any of their sensitivity cases. See also Yumashev and Johnson (2017). Meanwhile, after carrying out a review of current UK planning for a big nuclear accident (Ashley et al., 2017a), Ashley et al. (2017b) examine, using Public Health England's PACE-COCO2 program suite, the likely effects on the public of a severe accident on a fictional nuclear reactor located on the South Downs of England. Even after applying a rather strict safe-return criterion, they find that the expected number of people needing to be relocated is only 620, orders of magnitude below the figures for Chernobyl and Fukushima Daiichi.

By contrast with relocation, the J-value method provides strong support for remediation after a big nuclear accident (Waddington et al., 2017b). Similarly, remediation and temporary food bans are quite likely to be components of an optimal economic strategy (Yumashev et al., 2017). Meanwhile PACE-COCO2 (Ashley et al., 2017b) quantifies the expected cost of lost agricultural production as £130M, within an overall total expected accident cost of £800M (excluding reactor damage and lost electricity sales).

Waddington et al. (2017c) also use the J-value to examine the UK's response to Chernobyl of imposing restrictions on lamb produced on hill pastures in Cumbria, Wales, Scotland and Northern Ireland. The study endorses the Government's decision to remove the controls in 2012, but finds that the positive effect of the curbs had fallen to such a low level (equivalent to increasing the life expectancy of UK consumers by 8 s) at the time they were dropped as to call into question why the restrictions were not taken away much earlier.

The caution displayed on hill sheep controls finds an echo in the approach of those regulating nuclear energy in the UK. Nuttall et al. (2017) report on a structured discussion involving a panel of experts drawn from risk specialists, insurance specialists, lawyers concerned with nuclear law, and, in addition, safety and environmental regulators. The authors contrast the "stoicism" of those closest to implementing policies and procedures to counter nuclear risks

with the greater sense of uncertainty evident amongst those charged with regulating nuclear energy.

While the loss of life expectancy for an exposed population may be rather small after a big nuclear accident, as noted above, what about those people, fortunately few in number, who actually contract a fatal, radiation-induced cancer? How much life will they lose? These are the questions addressed in Thomas (2017b). Based on the model for mortality period devised by Lord Marshall of Goring in the 1980s and the linear, no-threshold model for radiation risk endorsed by the International Committee for Radiological Protection (ICRP), he finds that the average radiation cancer victim will live into his/her 7th or 8th decade and lose between 8 and 22 years of life expectancy. This implies that, on average, a UK citizen has twice as much or more to lose from being killed outright in a road or rail accident as opposed to dying as result of a radiation cancer induced at the same moment. The author draws attention to the limitation this finding exposes in the thinking behind the one-size-fits-all "value of a prevented fatality" (VPF), currently used widely in the UK for cost-benefit analysis.

The final paper (Thomas and Waddington, 2017) provides validation for the J-value method by using it to give the first theoretical explanation of the regular shape found in the Preston curve, which charts life expectancy at birth against GDP per head for all the nations of the world. The paper also proposes the life expectancy ratio (population-average life expectancy divided by life expectancy at birth) as a measure of national development, predicting and then corroborating that its starting value for a very poor county will be ⅔, but that this figure will decrease towards ½ as the country progresses from undeveloped to highly developed. The authors have also provided the first objective estimation of an important economic variable, the pure time discount rate, used, for example, in Lord Stern's analysis of the economic effects of climate change (Stern, 2007 ; Stern, 2009) and, in fact, key to its results.

The results from the NREFS project presented here are based on a diverse set of methods but show a significant scientific and economic convergence on how best to respond to a big nuclear accident. Although it was treated as the prime policy choice at both Chernobyl and Fukushima Daiichi, mass relocation emerges as unlikely to be a good policy option. The NREFS papers indicate that indiscriminate implementation of relocation after a big nuclear accident in the future would very likely transgress the ICRP's fundamental "principle of justification", namely that any measure adopted should do more good than harm.

It is understandable that decision makers react to socio-political pressures but it is very important that decision making takes place against the best available analysis of the impact of the actions to be undertaken, given the very considerable human and monetary consequences that result from over-reaction. Quantitative analyses such as those considered above can provide a "baseline" for the guidance of those who need to judge the best course of action. If a decision is taken that goes further than warranted by the results of the baseline analysis, decision makers should justify why resources are being employed significantly beyond what is cost beneficial.

Investigating the effectiveness of nanoscale nuclear waste filter

Source: http://www.homelandsecuritynewswire.com/dr20171121-investigating-the-effectiveness-of-nanoscale-nuclear-waste-filter

Nov 21 – Researchers at The University of Texas at Dallas are investigating the effectiveness of a **nanoscale "sponge"** that could help filter out dangerous radioactive particles from nuclear waste.

Effectively capturing these byproducts of nuclear power would dramatically increase recycling efforts and enhance the safe storage of radioactive materials, said Dr. Yves Chabal, head of the Department of Materials Science and Engineering at the Erik Jonsson School of Engineering and Computer Science.

UTDallas says that researchers **used tiny metal-organic frameworks, or MOFs, to trap radioactive molecules.** They are composed of metal ion centers and organic molecules that link together parts of the structure. This creates a microscopic scaffold, or trap, that can capture specific gases and

other molecules. The current work focused on testing the adsorption capacity of specific MOFs to remove radioactive iodine more efficiently.

While porous materials have been used to capture radioactive molecules, the capacity of existing adsorbents remains insufficient. Adsorption is the process by which a thin layer of molecules clings to the surfaces of solid bodies or liquids — in this case, the internal surfaces of MOFs.

"In a spent radioactive fuel rod, there are several elements that decay at different rates. Radioactive iodine is one of the primary byproducts," said Dr. Kui Tan, a UT Dallas research scientist and one of the authors of the study recently published in the journal *Nature Communications*. "By attaching a nitrogen-containing molecule to the MOFs, our colleagues showed they could capture these radioactive molecules very efficiently."

Nuclear power accounts for roughly 11 percent of the world's electricity, and researchers are examining more efficient and less expensive methods of capturing radioactive iodine and other common byproducts from the reactors. Some MOFs imbued with silver perform well at high temperatures, but are expensive and difficult to recycle.

"Professor Jing Li and her team at Rutgers University designed and synthesized the MOF molecular traps," Tan said. "They demonstrated that the MOFs can be functionalized by adding nitrogen-containing molecules to form strong chemical bonds with organic iodides, thereby trapping them in the pores. But they needed help to fully understand the binding mechanism. This is where our team and the team at Wake Forest came in."

Using spectroscopy to determine the interaction of molecular iodine and organic iodide within the functionalized lattice, Tan and his colleagues uncovered how the binding occurred and why the capacity for iodine capture was so high.

While the Rutgers team found that the molecular traps captured more than 340 percent more radioactive material than current industrial adsorbents, the UT Dallas and Wake Forest teams determined why and how, which greatly increases the impact of the work. With this knowledge, there is a basis to consider other materials and molecules for a wide range of applications.

"Synthesis of these MOFs is scalable, and they have the potential of being produced on an industrial scale," Tan said. "We really understand better how these processes work, and we hope it opens up the possibility of finding new applications."

Both Chabal and Tan noted that the collaboration between Rutgers, UT Dallas and Wake Forest University was crucial in finding this new potential method for trapping radioactive materials. Researchers from the Massachusetts Institute of Technology, King Abdullah University of Science and Technology in Saudi Arabia, and Jilin University in China also contributed to the study.

Radioactive material, leaked from a Russian nuclear complex, detected over Europe

Source: http://www.homelandsecuritynewswire.com/dr20171121-radioactive-material-leaked-from-a-russian-nuclear-complex-detected-over-europe

Nov 21 – Responding to an access to information request from Greenpeace, the Russian state meteorological agency Roshydromet today (Tuesday, 21 November) published data that show that the agency had found last September the highest concentration of ruthenium-106 in the area where the Rosatom Mayak nuclear complex, located in the Southern Urals. Roshydromet's findings coincide with earlier findings from the French nuclear research agency IRSN and the German agency for radiation protection BfS.

Greenpeace Russia says that based on these data, Greenpeace Russia will send a letter to the office of the public prosecutor to request an investigation into possible concealment of a radiation accident and for the release of information on the status of the environment in the affected area and beyond. It also demands a check whether the atmospheric radionuclide monitoring system is sufficiently prepared for possible accidents, and whether public health issues related to a possible release of Ruthenium 106 were considered, and public healths sufficiently protected.

According to previously published IAEA data, in late September –

early October, **Ruthenium-106** was found in the atmosphere in many European countries. The German radiation protection agency BfS came to the conclusion that the source of the emissions of the radioactive substance was most likely located in the Southern Urals. The French nuclear research and safety agency IRSN confirmed this conclusion.

Rosatom called the conclusions of the German and French nuclear agencies inconsistent. The Russian energy company said that in the period of 25 September – 7 October, according to the results of aerosol sampling done by Roshydromet, Ruthenium-106 was not found anywhere except in one single area – Saint-Petersburg. Today (Tuesday), however, Roshydromet published a more complete set of data in response to an access to information request by Greenpeace Russia.

The agency's report for September shows that the highest concentrations of ruthenium-106 were found in localities around the Mayak complex in the Chelyabinsk region in the Southern Urals. Mayak is a dual-purpose military/civilian nuclear complex which, among other things, reprocesses spent nuclear fuel and processes different forms of radioactive waste.

Roshydromet has also indicated that in that in late-September – early-October, the atmospheric conditions enhanced the transfer of big air masses with pollutants from the Southern Urals to the Mediterranean and up to Northern Europe. Until now, this had officially been denied.

Due to its relatively short half-time of one year, Ruthenium-106 only exists as a human-made substance which is normally not present in the atmosphere. Even small concentrations, therefore, indicate an accidental release. Roshydromet assessed the Ruthenium-106 rate in the air and fall-out samples as "extremely high" and "high contamination."

The French IRSN estimated that the initial discharge could be as high as 100-300 TeraBequerels, 10,000 times the annual allowed limit of emissions of ruthenium-106 and its decay product rhodium-106 combined. IRSN indicated that such a release should lead to protective measures for people in a radius of several kilometers.

An emergency discharge of ruthenium could be connected with the process of nuclear waste vitrification. Another possibility is that materials containing ruthenium-106 were placed in a metal remelting furnace. Both these activities take place in the Rosatom complex at Mayak.

Evacuating a nuclear disaster area is often a waste of time and money, says study

By Philip Thomas

Source: http://www.homelandsecuritynewswire.com/dr20171122-evacuating-a-nuclear-disaster-area-is-often-a-waste-of-time-and-money-says-study

Nov 22 – Over 110,000 people were moved from their homes following the Fukushima nuclear disaster in Japan in March 2011. Another 50,000 left of their own will, and 85,000 had still not returned four-and-a-half years later.

While this might seem like an obvious way of keeping people safe, my colleagues and I have just completed research that shows this kind of mass evacuation is unnecessary, and can even do more harm than good. We calculated that the Fukushima evacuation extended the population's average life expectancy by less than three months.

To do this, we had to estimate how such a nuclear meltdown could affect the average remaining life expectancy of a population from the date of the event. The radiation would cause some people to get cancer and so die younger than they otherwise would have (other health effects are very unlikely because the radiation exposure is so limited). This brings down the average life expectancy of the whole group.

But the average radiation cancer victim will still live into their 60s or 70s. The loss of life expectancy from a radiation cancer will always be less than from an immediately fatal accident such as a train or car crash. These victims have their lives cut short by an average of 40 years, double the 20 years that the average sufferer of cancer caused by radiation exposure. So if you could choose your way of dying from the two, radiation exposure and cancer would on average leave you with a much longer lifespan.

How do you know if evacuation is worthwhile?

To work out how much a specific nuclear accident will affect life expectancy, we can use something called the CLEARE (Change of life expectancy from averting a radiation exposure) Program. This tells us how much a specific dose of radiation will shorten your remaining lifespan by on average.

Yet knowing how a nuclear meltdown will affect average life expectancy isn't enough to work out whether it is worth evacuating people. You also need to measure it against the costs of the evacuation. To do this, we have developed a method known as the judgement or J-value. This can effectively tell us how much quality of life people are willing to sacrifice to increase their remaining life expectancy, and at what point they are no longer willing to pay.

You can work out the J-value for a specific country using a measure of the average amount of money people in that country have (GDP per head) and a measure of how averse to risk they are, based on data about their work-life balance. When you put this data through the J-value model, you can effectively find the maximum amount people will on average be willing to pay for longer life expectancy.

After applying the J-value to the Fukushima scenario, we found that the amount of life expectancy preserved by moving people away was too low to justify it. If no one had been evacuated, the local population's average life expectancy would have fallen by less than three months. The J-value data tells us that three months isn't enough of a gain for people to be willing to sacrifice the quality of life lost through paying their share of the cost of an evacuation, which can run into billions of dollars (although the bill would actually be settled by the power company or government).

The three-month average loss suggests the number of people who will actually die from radiation-induced cancer is very small. Compare it to the average of 20 years lost when you look at all radiation cancer sufferers. In another comparison, the average inhabitant of London loses 4.5 months of life expectancy because of the city's air pollution. Yet no one has suggested evacuating that city.

We also used the J-value to examine the decisions made after the world's worst nuclear accident, which occurred 25 years before Fukushima at the Chernobyl nuclear power plant in Ukraine. In that case, 116,000 people were moved out in 1986, never to return, and a further 220,000 followed in 1990.

By calculating the J-value using data on people in Ukraine and Belarus in the late 1980s and early 1990s, we can work out the minimum amount of life expectancy people would have been willing to evacuate for. In this instance, people should only have been moved if their lifetime radiation exposure would have reduced their life expectancy by nine months or more.

This applied to just 31,000 people. If we took a more cautious approach and said that if one in 20 of a town's inhabitants lost this much life expectancy, then the whole settlement should be moved, it would still only mean the evacuation of 72,500 people. The 220,000 people in the second relocation lost at most three months' life expectancy and so none of them should have been moved. In total, only between 10% and 20% of the number relocated needed to move away.

To support our research, colleagues at the University of Manchester analyzed hundreds of possible large nuclear reactor accidents across the world. They found relocation was not a sensible policy in any of the expected case scenarios they examined.

More harm than good

Some might argue that people have the right to be evacuated if their life expectancy is threatened at all. But overspending on extremely expensive evacuation can actually harm the people it is supposed to help. For example, the World Health Organization has documented the psychological damage done to the Chernobyl evacuees, including their conviction that they are doomed to die young.

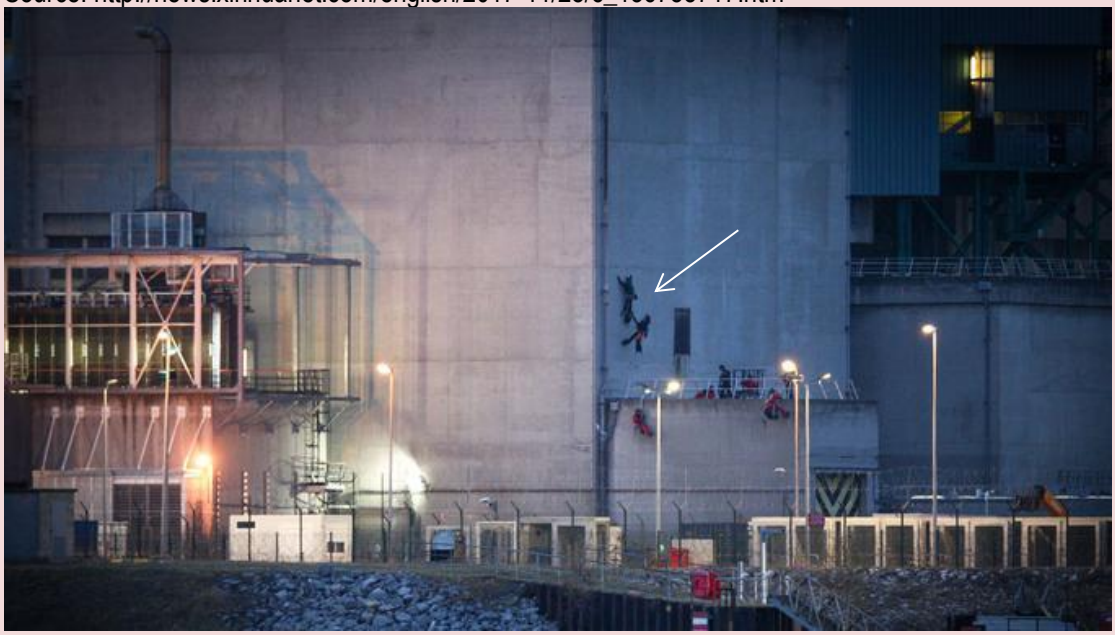
From their perspective, this belief is entirely logical. Nuclear refugees can't be expected to understand exactly how radiation works, but they know when huge amounts of money are being spent. These payments can come to be seen as compensation, suggesting the radiation must have left them in an awful state of health. Their governments have never lavished such amounts of money on them before, so they believe their situation must be dire.

But the reality is that, in most cases, the risk from radiation exposure if they stay in their homes is minimal. It is important that the precedents of Chernobyl and Fukushima do not establish mass relocation as the prime policy choice in the future, because this will benefit nobody.

Philip Thomas *is Professor of Risk Management, University of Bristol.*

Greenpeace activists break into nuclear plant in France

Source: http://news.xinhuanet.com/english/2017-11/28/c_136785717.htm



Nov 28 – **A group of Greenpeace activists entered a nuclear plant in Ardeche, southeastern France on Tuesday to highlight the danger of atomic power and related security problems, the environmental group said.**

Earlier on Tuesday morning, about 20 Greenpeace campaigners broke into Cruas-Meysse nuclear power plant in Ardeche **"to warn about the extreme vulnerability of spent fuel storage pools."**

Some of them climbed one of the buildings containing pools used to cool highly radioactive spent fuel rods and set off flares to show that "they are not sufficiently protected against the risk of external attacks."

"Greenpeace France demands that Electricite de France (EDF) take charge of this nuclear safety problem and undertake the necessary work to secure the most fragile facilities, in particular spent fuel storage pools," the group said in a statement.

EDF, the state-run utility operator which operates the nuclear plan, confirmed the break-in but said that "the intruders remained outside the nuclear zone."
"This intrusion had no impact on the safety of the facilities," it added.
Operating 58 reactors, **France is the most nuclear-reliant country in the world, with more than three quarters of its power coming from nuclear sources.**
The centrist government said it will take more time to meet a pledge to trim reliance on nuclear energy.
As part of its climate plan, the country previously targeted to close up to 17 reactors in order to cut nuclear power generation to 50 percent from 75 percent by 2025.

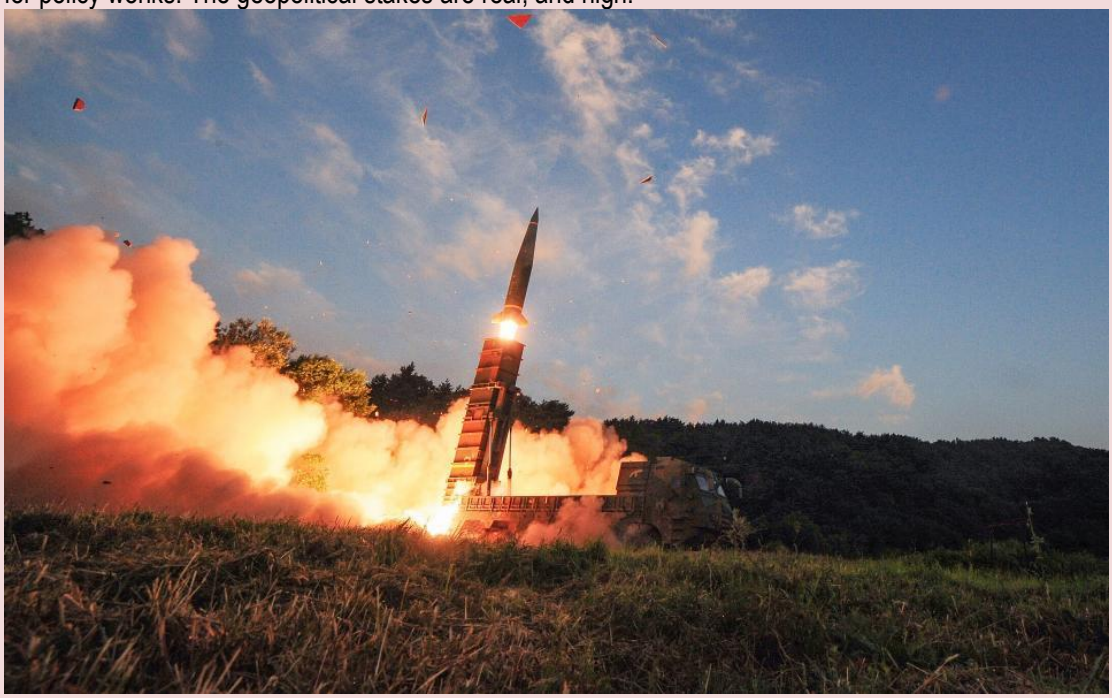
EDITOR'S COMMENT: Never heard of "war games"? Gov should test security of nuclear plants the way Greenpeace illegaly entered nuclear premises. Is the director of security still in place? Most probably YES…

We Can't Attack North Korea. It's Against the Law

By John Burroughs
Source: http://www.newsweek.com/we-cant-attack-north-korea-its-against-law-727009

Nov 30 – Responding to North Korea's test of an intercontinental ballistic missile that could threaten the United States' mainland, Secretary of State Rex Tillerson said in a press release: "Diplomatic options remain viable and open, for now."
At an emergency meeting of the U.N. Security Council on Wednesday, U.S. Ambassador Nikki Haley said while the U.S. does not seek war, "if war comes, make no mistake, the North Korean regime will be utterly destroyed."
But diplomacy is not just viable, as Tillerson says; it's legally required by the Charter of the United Nations, which, as a treaty ratified by the United States, is the law of the land under the Constitution. This dimension of the North Korean crisis is not getting the attention it deserves.
The charter prohibits the threat or use of force except when authorized by the U.N. Security Council or in self-defense against an armed attack. The Security Council is intensively addressing the crisis, including in Wednesday's meeting, and it's significant that it has not seen fit to authorize the use of force.
Unless and until it does, the U.S. is bound by law to seek a diplomatic solution. Seeking a military one, in addition to its horrific humanitarian consequences, would violate the charter and put the U.S. on the wrong side of the law.
We're currently operating under Resolution 2375 of September 11, 2017, which tightened sanctions on North Korea after it tested a powerful nuclear bomb. It was adopted pursuant to U.N. Charter Article 41, which covers measures not involving the use of force, such as economic sanctions.
Neither 2375 nor previous Security Council resolutions on North Korea contain any indication whatever that force is authorized. In fact, they emphasize the need for a peaceful settlement, which is also mandated by the charter.
Article 2(3) obligates all members to "settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."
There is a reason Security Council resolutions on North Korea are written this way. China and Russia are implacably opposed to a military strike, and have the power to veto resolutions they oppose.

They learned their lesson in the run-up to the 2003 U.S. invasion of Iraq, when the United States interpreted ambiguous language in Security Council resolutions to authorize the invasion.
That interpretation was incorrect, but since then China, Russia and other members of the council have taken extreme care to prevent the U.S. from making similar maneuvers.
Those inclined to scoff at the idea that the U.N. or international law could restrain the U.S. from using its military might haven't really understood the situation. This is not just a matter of international legalisms for policy wonks. The geopolitical stakes are real, and high.



In this photo released by the South Korean Defense Ministry, South Korea's Hyunmoo-2 ballistic missile is fired during an exercise aimed to counter North Korea's nuclear test on September 4. South Korean Defense Ministry via Getty
China might well intervene militarily if the United States started a war with North Korea. In negotiations on Resolution 2375, China and Russia supported including a provision forbidding military action north of the 38th parallel dividing South and North Korea.
That provision was refused by the U.S., but it shows how opposed Russia and China are to use of force in the region. Their position is backed by law, which, as permanent members of the Security Council, they shape by refusing any authorization of force.
Article 51 of the U.N. Charter does recognize "the inherent right of individual or collective self-defense *if an armed attack occurs* … until the Security Council has taken measures necessary to maintain international peace and security."
But since the George W. Bush administration, U.S. doctrine has permitted preemptive attacks against serious threats, particularly weapons of mass destruction. While the term is usually avoided, this is essentially a doctrine allowing preventive war.
This August, Trump's chief of staff, General H. R. McMaster, broke protocol and referred to a possible "preventive war" against North Korea.
That U.S. position is not backed by law. Preventive war is plainly illegal under the U.N. Charter, which permits military action as a matter of self-defense only in response to an actual armed attack. At most, military action might be allowed in response to the early stages of an attack.
Again, this is no wonkish, legalistic fine point of parsing the charter; it's of vital practical importance. Preventive war proved profoundly destabilizing and destructive in the Middle East, and would again on the Korean Peninsula.
Amid Trump's incendiary "fire and fury" rhetoric, Congress is also beginning to debate the legality of a conventional or nuclear strike against North Korea, and the limits of the president's power to order one.

At a November 14 hearing of the Senate Foreign Relations Committee, Brian McKeon, former committee lawyer and former Pentagon official, testified that the Constitution requires any war with North Korea to be authorized by Congress. Two bills were recently introduced in Congress requiring its specific approval of war with North Korea, and two others require Congressional approval of the first use of nuclear weapons or rule it out altogether.
Also at the Senate hearing, former Commander of Strategic Command Robert Kehler pointed out that the U.S. military is duty-bound to refuse a president's order to use nuclear weapons if it's illegal.
He testified that to be legal, use of nuclear weapons must comply with requirements of necessity, proportionality and discrimination under the international law of armed conflict.
What Kehler did not say is that given their uncontrollable and indiscriminate effects, an order to use nuclear weapons would fail those tests, and be illegal.
There was zero discussion at the hearing of the illegality of the U.S. attacking North Korea under the U.N. Charter.
Yet as we learned from the Iraq War, there is great wisdom in the charter requirement that peaceful solutions, however difficult to achieve, take precedence over resorting to force.

***John Burroughs** is Executive Director of the New York City–based Lawyers Committee on Nuclear Policy.*

Yemen's Houthi group says fires missile toward Abu Dhabi nuclear reactor

Source: https://www.reuters.com/article/yemen-security-emirates/update-1-yemens-houthi-group-says-fires-missile-toward-abu-dhabi-nuclear-reactor-idUSL8N1O3065

Dec 3 – Yemen's Houthi group has fired a cruise missile towards a nuclear power plant in Abu Dhabi in the United Arab Emirates, the group's television service reported on its website on Sunday, without providing any evidence.
There were no reports of any missiles reaching the UAE.
The Iran-aligned Houthis control much of northern Yemen and had said Abu Dhabi, a member of the Saudi-led coalition fighting against them since 2015, was a target for their missiles.
"The missile force announces the launching of a winged cruise missile ... towards the al-Barakah nuclear reactor in Abu Dhabi," the website said. It gave no further details.

The Barakah project, which is being built by Korea Electric Power Corporation (KEPCO), is expected to be completed and become operational in 2018, the UAE energy minister has said.
It is the second time this year the Houthis have said they have fired missiles towards the UAE. A few months ago they said they had "successfully" test fired a missile towards Abu Dhabi.

EDITOR'S COMMENT: Might be fake news – war propaganda as usual. Might be a reality but I doubt it although technically is possible (there are Iranian cruise missiles covering the range from Sanaa area all the way to Bakarah (~1500km), BUT the missile must esape the Patriot system of S. Arabia and that of the Emirates. Nevertheless, the point is that a nuclear power plant in steadily unstable neighborhood is a risky business and all related preparedness measures should be taken well in advance and before the completion of the project – special focus on population awareness!!!

NBC: Microwave Weapons Could Disable N. Korean Missiles

Source: http://world.kbs.co.kr/english/news/news_In_detail.htm?No=132174

Dec 05 – The United States could disable North Korean missiles with microwave weapons, according to a report by NBC on Monday.

The U.S. broadcaster revealed that White House officials had discussed the development of microwave weapons, called CHAMPs, in August. The weapons would be fit into an air-launched cruise missile and delivered from B-52 bombers into enemy airspace to emit sharp pulses of microwave energy that could disable electronic systems.

The CHAMP project began in April, 2009 at the Air Force Research Laboratory in Albuquerque, New Mexico. A document that the broadcaster attained shows that the weapons could be used on weapons of mass destruction.

As missile control centers have many devices that are weak to microwave signals, CHAMPs could be used to disable North Korea's ballistic missiles, according to the NBC report.

U.S. medical profession unprepared for nuclear attack: Study

Source: http://www.homelandsecuritynewswire.com/dr20171206-u-s-medical-profession-unprepared-for-nuclear-attack-study

Dec 06 – Escalating tensions between Washington and Pyongyang over North Korea's nuclear program have fueled concerns about the possibility of nuclear warfare, and a study from the University of Georgia has found that American medical professionals are woefully unprepared to handle the needs of patients after a nuclear attack.

The researchers analyzed survey responses from over 400 emergency medical personnel in the U.S. and Asia to find out if medical professionals would show up to the site of a nuclear attack and, if they did, whether or not they know the appropriate treatment protocols. They published their findings recently in *Frontiers in Public Health*.

"I was not surprised that the responses from the emergency medical community were relatively poor in terms of knowledge and attitudes, because that's what you get with radiation-myths versus reality," said the study's lead author, Cham E. Dallas, a professor of health policy and management and director of the Institute for Disaster Management at UGA's College of Public Health.

Over half of the respondents hadn't received any formal education on issues related to radiation, and many thought that the immediate medical need after a Hiroshima-sized nuclear detonation would be thermal burns when, in fact, patients are more likely to need treatment for lacerations.
When asked to rank what type of disaster event would make them unwilling to come to work, respondents chose nuclear bomb.

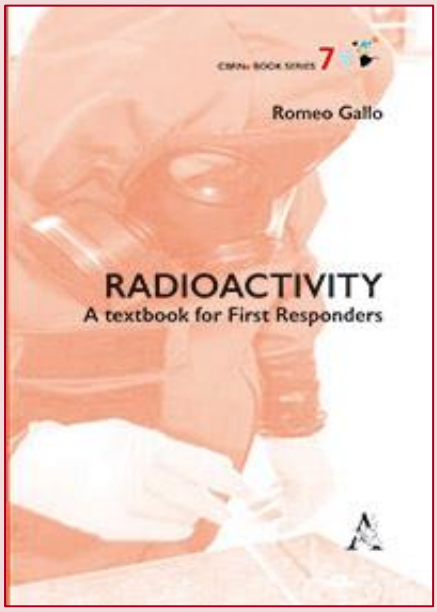
"What we found was that medical personnel were actually more afraid of radiation than they were of biological or chemical events," said Dallas.

Ironically, responding to radiological or nuclear events has historically presented no risk to health care providers.
UGA says that this study suggests that emergency medical personnel, despite access to nuclear disaster training, view nuclear events with the same fear and misunderstanding as the general public. Dallas believes this may be because nuclear events are rare, and most providers have no firsthand experience. They fear what they don't know.
"The interesting thing is these are tough characters. These are people who see trauma and death all the time," said Dallas. "They're tough, but not with radiation."
Dallas also points to Hollywood's treatment of nuclear events. Most of what people see on television or in movies, he says, is incorrect and reinforces a view that little can be done in the face of a nuclear event. That's the key assumption Dallas wants to correct.
"As terrible as it might be," he said, "it's far more manageable than emergency professionals realize."
Yet, Dallas is concerned that deep-seated fears may override any disaster training medical personnel might receive. "Even when emergency medical personnel get a minimum amount of training, I'm not certain we're breaking these patterns," he said.
Experts agree that a radiological or nuclear event is inevitable, so health care professionals can't afford to be unprepared, said Dallas, and he urges medical community leaders to offer more radiation and nuclear disaster training addressing the myths related to these events before the threat of attack becomes a reality.
"We're about to turn the corner on this into a far more likely landscape of nuclear events, and we are not ready," said Dallas. "It's a problem."

— Read more in Cham E. Dallas et al., "Readiness for Radiological and Nuclear Events among Emergency Medical Personnel," Frontiers in Public Health (18 August 2017)

Radioactivity – A textbook for First Responders

By Romeo Gallo
Source:http://www.aracneeditrice.it/aracneweb/index.php/pubblicazione.html?item=9788825508055



CBRN risk can not be addressed without adequate knowledge. Thought for the First Responder, the book confront in particular the radiological risk, which can be manifested in civil defense as well as in the most typical of civil protection. Only an accurate analysis of the event that may occur time after time, proper use of appropriate instrumentation and knowledge of radiation protection measures can ensure the safety of rescuers and the population. The paper addresses both theoretical and practical aspects (radioprotection, dosimetry, detectors, contamination, transport) and has over 60 exercises carried out.

***Romeo Gallo**, ingegnere civile, è funzionario del Corpo Nazionale VVF presso il Comando Provinciale di Matera. Per il Corpo si è occupato di formazione CBRN, contribuendo alla stesura di apposite dispense, e della pianificazione delle specifiche emergenze.*

Ha conseguito il titolo di Master di II Livello in Protezione da eventi CBRNe, collaborando successivamente come docente nell'ambito del programma radiologico/nucleare. Esperto qualificato di secondo livello, è membro della Commissione per la Radioprotezione per la Provincia di Matera.

Engaging North Korea II: Evidence from the Clinton Administration

Source: https://nsarchive.gwu.edu/briefing-book/korea/2017-12-08/engaging-north-korea-ii-evidence-clinton-administration

Dec 08 – The Clinton administration made plans for war against North Korea during the 1994 nuclear crisis. While U.S. officials believed they could "undoubtedly win," however, they also understood "war involves many casualties," according to documents posted today by the George Washington University-based National Security Archive.

President Bill Clinton's negotiators took a tough stance in meetings with North Korean leaders, including warning of "serious, negative consequences" if Pyongyang continued to pursue its "unacceptable" missile program. At the same time, the administration decided flexibility was critical given the unpredictability of events, including the prospect that a "starving North Korea" might create a "dangerously chaotic situation."

Today's posting features declassified cables, background papers, and reports of meetings involving former Defense Secretary William Perry, other senior Americans, and North and South Korean officials. Together, the documents describe key moments and thinking during the course of the complex negotiations of the 1990s. Perry and others had hopes the incoming Bush team would carry the effort forward (as Colin Powell indicated they would), but President Bush quickly informed President Kim he would be terminating all talks with the North.

Engaging North Korea II: The Clinton Administration's Experience

By Robert A. Wampler, Ph.D.

The current deepening crisis driven by North Korea's nuclear weapons and missile programs makes understanding prior efforts to resolve this long-standing security threat on the peninsula all the more urgent. An earlier National Security Archive Electronic Briefing Book posted documents that dealt with efforts of the George H. W. Bush administration to engage Pyongyang in talks that could lead to a Korean peninsula free of nuclear weapons. As that posting discussed, the early hopes engendered by this U.S. initiative were eventually dashed as suspicion grew that North Korea did not intend to abide by its commitments to open its nuclear facilities to international inspection.

The documents posted here take up the story as it unfolded during the second Clinton administration (1997-2000), which witnessed another period of promises unmet. Among the important points made by these documents:

1. William Perry, Clinton's special envoy for North Korea and former secretary of defense told South Korean President Kim Dae Jung that during the 1994 nuclear crisis the U.S had planned for war. "Of course, with the combined forces of the ROK and U.S., we can undoubtedly win the war," Perry added. "But war involves many casualties in the process." [Document 7]
2. In Pyongyang in 1999, Perry told North Korean leaders their missile program, whose longer-range missiles could already reach U.S. territory and threatened South Korea and Japan, posed an "unacceptable" threat, and that if continued would bring "serious, negative consequences" for U.S.-DPRK relations. [Documents 9 and 10]
3. Pyongyang's economic situation raised worries in Washington that a "starving North Korea" could become unstable and create a "dangerously chaotic situation," according to a 1997 State Department document. The U.S. approach to the Four-Party Talks therefore had to be "flexible enough to encompass a wide range of options," from "a collapse of the North" to "meaningful reforms which would give the DPRK regime renewed vitality." [Documents 1and 3]
4. The State Department advised that the U.S. and its negotiating partners "be prepared for the long haul and keep expectations low" in talks with the North Koreans, whose style was described as "being obstreperous, applying pressure, and then relenting in the end." [Documents 1 and 2]
5. The U.S. warned Seoul that "If Pyongyang senses we will betray our commitments to them, they will look for a reason to betray their commitments to us." This risked "fueling hard-line arguments in Pyongyang that the DPRK was deceived by the U.S., and that the nuclear program should be restarted." [Documents 2 and 5]
6. A number of documents address the need to engage China fully in the Four Party Talks and other discussions, given Beijing's presumed influence with North Korea and China's national interest in resolving the security dilemmas on the Korean peninsula. [Documents 5, 9, and 13]
7. Kim Jong Il's relatively positive debut on the world stage in the summer of 1999 persuaded many South Koreans, at least temporarily, that he might not be "the dissipated, degenerate 'playboy madman'" depicted "deliciously and maliciously" for many years by South Korean media. Conservatives, however, continued to see Kim as "the devil incarnate," according to a State Department cable. [Document 16]

These and other points made by the documents need to be viewed in light of current events. North Korea continues to be a crucial security concern for the U.S., with recent developments underscoring the stakes. North Korea tested an intercontinental ballistic missile on November 28th that experts say demonstrated the range to reach Washington, D.C. and other parts of the U.S. eastern seaboard (though many expressed doubt the missile would have this range carrying a nuclear warhead). Following the launch, North Korean officials told CNN that Pyongyang was not interested in diplomacy until after it had "fully demonstrated its nuclear deterrent."

With President Trump and North Korean leader Kim Jong Un trading personal attacks, and reports that Trump plans to fire Secretary of State Rex Tillerson, whose effort to engage North Korea in talks was torpedoed by a tweet from President Trump, there seems to be little chance diplomacy can resolve this deepening crisis on the Korean peninsula.[1] Instead, the U.S. has sought new sanctions against North Korea, warned China to cut off oil exports to North Korea or the U.S. will take matters into its own hands, and U.S. Ambassador to the UN Nikki Haley warned at an emergency UN National Security Council meeting that while the U.S. did not desire war, "if war comes, make no mistake, the North Korean regime will be utterly destroyed." [2]

These documents show how the Clinton administration, like the earlier Bush White House, harbored no unrealistic hopes about a quick and easy resolution of the Korean security challenge. The vital stakes were clearly recognized, with the U.S. underscoring for North Korea that its nuclear and missile programs presented an "unacceptable threat," and that the U.S. goal was a mechanism that would provide the U.S. and its allies "complete and verifiable assurances that North Korea had no nuclear weapons program."

The range of outcomes for the Four Party talks that began in December 1997 ranged from the collapse of North Korea due to economic failures to the possible, though unlikely, adoption of reforms that would give the DPRK new vitality. The U.S. held modest expectations for the talks, knowing they would be "tedious and subject to constant tensions," exhibiting the usual North Korean modus operandi: "being obstreperous, applying pressure, and then relenting in the end." There was also appreciation of the risk that, if North Korea felt the U.S. and its allies were failing to carry out their commitments to Pyongyang under the 1994 Framework Agreement, they may seize on this as an excuse to resume their nuclear weapons program. Throughout, the U.S. gave high priority to consultations and coordination with South Korea and Japan, and to engaging China to bring its influence to bear on North Korea.

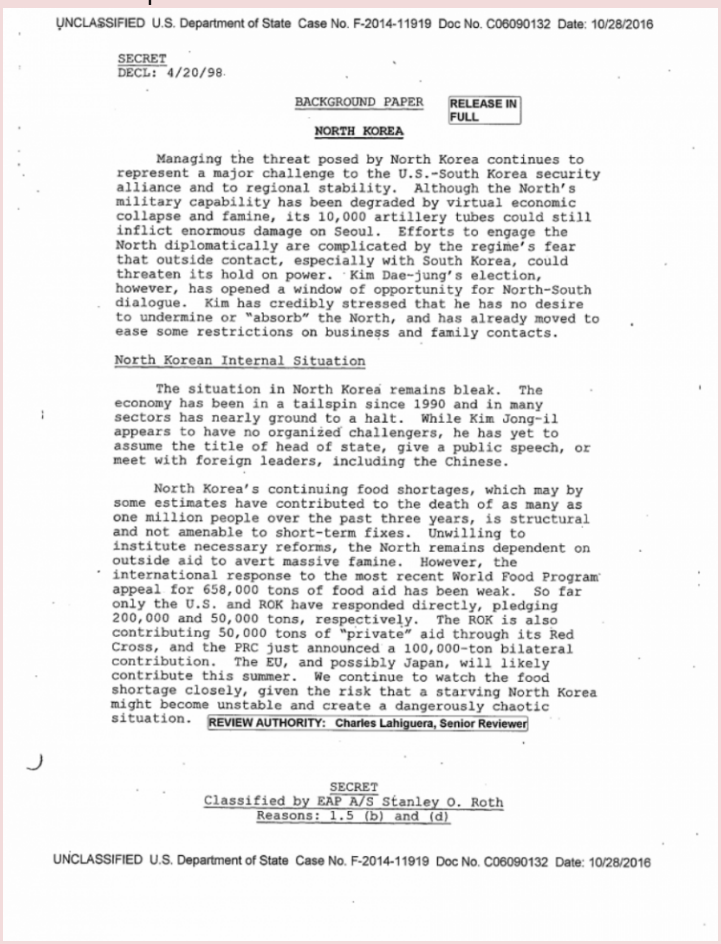
Finally, though U.S. policy included sanctions as both carrot and stick, there is little discussion of military options. Possibly this is the result of the Clinton administration's examination of such options against North Korea during the 1994 nuclear crisis. As former Secretary of Defense William Perry told Kim Dae Jung, while its war planning showed that the U.S. and South Korea would prevail in a war, there would be many casualties.

A brief sketch of the historical backdrop to the documents posted today can provide the necessary context.[3] The mounting concerns at the end of the Bush administration about North Korea's nuclear weapons program reached a head during the first Clinton administration, leading to the 1994 crisis during which the U.S. gave serious consideration to military action to take out Pyongyang's nuclear facilities, only to reach agreement with North Korea on the 1994 Framework Agreement. Under this agreement, North Korea agreed to halt its nuclear weapons program and open its nuclear facilities to inspection, while the U.S. and other nations agreed to supply North Korea with heavy fuel oil to meet near-term needs, and international financing would be provided, under the aegis of the Korean Peninsula Energy Development Organization (KEDO), for construction of light-water reactors.[4]

Seeking to build on this progress, President Clinton and South Korean president Kim Young Sam at their meeting in April 1996 proposed Four Power talks (the U.S., South Korea, North Korea and China) to negotiate a peace treaty to replace the armistice that ended the Korean War.[5] These talks would be complemented by bilateral discussions between the U.S. and North Korea on nuclear weapons and missiles, and by the ongoing North-South dialogue that sought to make progress on issues such as economic cooperation and reuniting families divided by the Korean War. A key concern of the U.S. and South Korea was that their North Korea policies should be coordinated so that these inter-related negotiations could have a synergistic effect, with success in one venue serving to build momentum and confidence in the others.

Movement on all these fronts was hindered by several factors. Following the death of North Korean leader Kim Il Sung in July 1994, it took time for his son and successor, Kim Jong Il, to consolidate his control of the regime. North Korean provocations such as the infiltration of commandos into South Korea via submarine (they were either killed or captured) in September 1996, and the seizure of a DPRK submarine in South Korean waters in June 1998, tested South Korean resolve to engage with Pyongyang. Bilateral U.S.-DPRK talks aimed at stopping the latter's missile program, which saw five rounds between 1996 and 2000, made little headway. North Korea continued to develop and deploy long-range missiles capable of striking South Korea and Japan, and furthermore engaged in the sale of Scud missiles to Iran and Syria, actions which brought new U.S. sanctions against the DPRK. It was not until late 1997 that China agreed to take part in the Four Party Talks.

Other obstacles arose along the way. Direct talks between the two Koreas, prompted in part by North Korea's need for chemical fertilizers from South Korea to address its food shortages, collapsed quickly when North Korea rejected Seoul's desire to use the talks to arrange for the reunion of families divided by the partition of the country. Intelligence reports in 1998 indicated that North Korea might have built an underground complex to secretly resume its nuclear weapons program. Finally, the economic crisis that hit Asia in 1997 put in doubt South Korea's ability to meet its commitments to provide financing for the construction of light-water reactors in North Korea, a critical component of the 1994 Framework Agreement.



UNCLASSIFIED U.S. Department of State Case No. F-2014-11919 Doc No. C06090132 Date: 10/28/2016

SECRET
DECL: 4/20/98

BACKGROUND PAPER RELEASE IN FULL

NORTH KOREA

Managing the threat posed by North Korea continues to represent a major challenge to the U.S.-South Korea security alliance and to regional stability. Although the North's military capability has been degraded by virtual economic collapse and famine, its 10,000 artillery tubes could still inflict enormous damage on Seoul. Efforts to engage the North diplomatically are complicated by the regime's fear that outside contact, especially with South Korea, could threaten its hold on power. Kim Dae-jung's election, however, has opened a window of opportunity for North-South dialogue. Kim has credibly stressed that he has no desire to undermine or "absorb" the North, and has already moved to ease some restrictions on business and family contacts.

North Korean Internal Situation

The situation in North Korea remains bleak. The economy has been in a tailspin since 1990 and in many sectors has nearly ground to a halt. While Kim Jong-il appears to have no organized challengers, he has yet to assume the title of head of state, give a public speech, or meet with foreign leaders, including the Chinese.

North Korea's continuing food shortages, which may by some estimates have contributed to the death of as many as one million people over the past three years, is structural and not amenable to short-term fixes. Unwilling to institute necessary reforms, the North remains dependent on outside aid to avert massive famine. However, the international response to the most recent World Food Program appeal for 658,000 tons of food aid has been weak. So far only the U.S. and ROK have responded directly, pledging 200,000 and 50,000 tons, respectively. The ROK is also contributing 50,000 tons of "private" aid through its Red Cross, and the PRC just announced a 100,000-ton bilateral contribution. The EU, and possibly Japan, will likely contribute this summer. We continue to watch the food shortage closely, given the risk that a starving North Korea might become unstable and create a dangerously chaotic situation. REVIEW AUTHORITY: Charles Lahiguera, Senior Reviewer

SECRET
Classified by EAP A/S Stanley O. Roth
Reasons: 1.5 (b) and (d)

UNCLASSIFIED U.S. Department of State Case No. F-2014-11919 Doc No. C06090132 Date: 10/28/2016

Engagement with North Korea received a new impetus in 1998. First, newly-elected South Korean president Kim Dae Jung, a political reformer and former political prisoner, looked to reengage with North Korea through his "Sunshine Policy," as part of which he called on the U.S. and other countries to ease sanctions against North Korea and show greater flexibility in pursuing political and economic engagement with the regime. In the U.S., President Clinton named former Secretary of Defense William J. Perry to serve as North Korea policy coordinator in November 1998 (a position established by Congress) and to prepare a study setting forth recommendations for U.S. policy toward the DPRK.[6] As Perry carried out his review, one obstacle to progress was removed when North Korea agreed in late 1998 to U.S. inspection of the suspected nuclear site at Kumghang-ri; these inspections in 1999 discovered no covert nuclear facility. Then Perry, following consultations with South Korea and Japan (who joined with the U.S. in creating the Trilateral Coordination and Oversight Group, or TCOG, to coordinate their policies regarding North Korea, went to Pyongyang in May 1999 to present his ideas on improving U.S.-DPRK relations to high level North Korean officials. As Perry told the North Koreans and elaborated in his report, submitted to President Clinton in September 1999, the U.S. was prepared to accelerate diplomatic and economic relations with North Korea in exchange for DPRK steps to curb its nuclear weapons and missile programs, but also stood ready to adopt more coercive measures, i.e., sanctions, if North Korea proved unwilling to take the steps required to assure the U.S. and its allies.

President Clinton moved quickly to act on Perry's recommendation, ordering a broad easing of economic sanctions against the DPRK as a first step in a long-term plan to persuade Pyongyang to give up its nuclear and missile programs. Then, in March 2000, Kim Dae Jung gave a speech in Berlin in which he called for bilateral official talks between the two Koreas. This led to the historic summit meeting between Kim Dae Jung and Kim Jong Il in Pyongyang in June 2000. The summit raised new hopes for reconciliation on the peninsula, as cordial and productive meetings resulted in a joint declaration in which the two leaders agreed to work together to resolve reunification issues, address humanitarian issues such as exchange visits by divided families, and cooperation on economic initiatives. This in turn led to the further easing of sanctions by the U.S. The U.S. also moved to reenergize bilateral talks. In July 2000, Secretary of State Albright met with North Korean Foreign Minister Paek Nam Sun in Bangkok for talks that were more symbolic and substantive. This was followed by U.S.-DPRK talks in Washington, D.C. in September on nuclear issues, missiles and terrorism, which led to Pyongyang sending Vice Marshal Jo Myong Rok to Washington as a special envoy to meet with Clinton and Albright. These meetings in turn laid the basis for Secretary Albright's visit to Pyongyang in October, where she met with Kim Jong Ill and discussed U.S. proposals to curb North Korea's missile program, in return for which the U.S. would provide financial assistance and arrange a visit by Clinton to North Korea.[7]

In late December, President Clinton announced he would not be able to visit North Korea, a decision probably made in light of perceived opposition from the incoming George W. Bush administration. Still, there was hope that the outgoing administration would hand off North Korean relations in much better shape than when Clinton entered office. Perry recalled that he briefed incoming Secretary of State Colin Powell on the Clinton administration's negotiations with North Korea, and Powell told Perry that he planned to follow up on these talks and work to bring them to a successful end. Powell also gave similar reassurance to Kim Dae Jung when he visited Washington soon after President Bush's inauguration. However, when Kim met with Bush that same day, the president told him that he was ending all talks with North Korea, a step that Perry deeply regretted.[8]

So, once again, a period of cautious hope in U.S.-Korean affairs would fail to live up to its promise. It would be several years before the U.S. sought to reengage with North Korea, time which the communist regime used to press ahead with its nuclear and missile programs. The reasons for North Korea's decision to break its commitments are still subject to debate, and this history colors all current efforts to address the regime's security threat to the peninsula and the region.

▶▶ Read the documents at source's URL.

A Yemeni rebel claim highlights the risk of nuclear power in the Middle East

By Ali Ahmad

Source: https://thebulletin.org/yemeni-rebel-claim-highlights-risk-nuclear-power-middle-east11335

Dec 08 – Earlier this week, Yemen's Houthi rebel group claimed it had launched a missile at the Barakah nuclear power plant in the western region of Abu Dhabi, in retaliation for the Saudi-led blockade imposed on Yemen. Abu Dhabi is part of the United Arab Emirates (UAE), a member of the coalition that has been targeting the Houthis.

UAE officials immediately denied that the attack had taken place, and the Houthis have not provided any evidence to support their claim. However, regardless of the claim's validity, and despite the lack of evidence, **the incident is emblematic of the dangers of nuclear power in the Middle East.** The UAE should take it very seriously. Even if this "attack" was merely a propaganda ploy, nuclear power facilities will always be potential targets for enemy states and non-state actors, including terrorist groups. In the Middle East, in particular, there is a history of attacks on nuclear sites during regional conflicts.

The Barakah plant, being built by the Korea Electrical Power Corporation at an estimated cost of $20 billion, will be the UAE's first nuclear power facility. **The behemoth plant, with four 1,400-megawatt reactors and a total capacity of 5,600 megawatts, is the world's largest single nuclear construction project.** Once completed, it is projected to contribute about 25 percent of the UAE's energy. **The first reactor is expected to be online next year and the rest by 2020.**

The UAE's nuclear power program has been widely applauded as an intelligent investment that will help the country achieve energy security by reducing its reliance on imported natural gas. The UAE relies on natural gas not only to supply its population's growing demand for electricity, but also to power the desalination plants that provide the majority of the country's potable water. Officials have also touted the potential for the shift to nuclear power to reduce carbon dioxide emissions.

But the rosy projections about nuclear power's benefits gloss over the major security vulnerability the plant will create.

The fact that the population of the UAE and other Gulf countries is concentrated in some major urban centers exacerbates this vulnerability. At Fukushima, the site of Japan's infamous 2011 nuclear disaster, the population living on the coast near the plant could be evacuated inland. In contrast, evacuation from the UAE coast would be difficult, and there are few suitable sites to which the coastal population could be removed in the event of a disaster.

In an interview with the *Telegraph*, Japan's Prime Minister at the time of the Fukushima disaster revealed that his government came within a "paper-thin-margin" of deciding to

evacuate Tokyo and its 50 million people. The distance between Fukushima and Tokyo is comparable to the distance between Al-Barakah and Abu Dhabi, the nearest major city on the Gulf coast.

The country's National Emergency Crisis and Disaster Management Authority has said that "the UAE's air defense system is capable of dealing with any threats." But downplaying the vulnerability of the site and the security risks of nuclear power could prove to be very costly. Nuclear power plants are natural targets in armed conflicts, particularly with the emergence of non-state actors such as Yemen's Houthis.

After 9/11, the United States' security apparatus went on high alert over the possibility of a terrorist attack on one of the nation's nuclear reactors. Al Qaeda training materials found in Afghanistan reportedly contained diagrams of American nuclear power plants. In February 2002, the US Nuclear Regulatory Commission issued an advisory to the nation's 103 nuclear power plants warning that terrorists might attempt a 9/11-style attack on some of them by flying hijacked planes into the reactors. **Security officials also warned of potential attacks via boat or truck bombs, ground assaults by commando teams, and the possibility of sabotage by insiders**. Such attacks could target not only the reactors themselves, but also the spent fuel pools where radioactive waste is stored.

The issue of security is one of the reasons Israel has refrained from building nuclear power plants on its territory, although it has two small reactors, ostensibly for research. There is reason for caution, as the Middle East has a history of attacks on nuclear facilities, including one launched by Israel itself: **In 1980, Iran bombed the under-construction Osirak nuclear reactor in Iraq but failed to destroy it; a year later, an attack by the Israeli air force succeeded in reducing the reactor to rubble.** Likewise, Iraq repeatedly bombed the partially-completed Bushehr nuclear plant in Iran during the Iran-Iraq War in the 1980s.

Because these reactors were still under construction, the attacks did not lead to a release of radiation, but there have also been attacks on Israel's Dimona reactor in the southern Negev desert. In 1991, Iraq fired Scud missiles at the reactor, but missed the target. Today, the facility is in missile range from Iran, Syria, and Hezbollah in Lebanon. Although the site is heavily protected, in 2012 the Israel Atomic Energy Commission announced that the reactor would be shut down should war break out, to minimize danger from attacks.

Given this history, and the potentially catastrophic consequences of a successful attack on a nuclear facility, the UAE and other Middle Eastern countries should seriously consider the risks when deciding whether to pursue their own forays into nuclear power.

__Ali Ahmad__ is a scholar-in-residence and director of the Energy Policy and Security Program at the Issam Fares Institute for Public Policy and International Affairs at the American University of Beirut. His work covers nuclear security, energy policy, and economics, with a focus on the Middle East. Prior to joining AUB, Ali was a research fellow at Princeton University's Program on Science and Global Security, where he studied prospects for nuclear energy in the Middle East and nuclear diplomacy with Iran.

Newly declassified videos of nuclear tests

Source: http://www.homelandsecuritynewswire.com/dr20171215-newly-declassified-videos-of-nuclear-tests

Dec 15 – Researchers at Lawrence Livermore National Laboratory (LLNL) released sixty-two newly declassified videos today of atmospheric nuclear tests films that have never before been seen by the public.

The videos are the second batch of scientific test films to be published on the LLNL YouTube channel this year, and the team plans to publish the remaining videos of tests conducted by LLNL as they are scanned and approved for public release.

LLNL nuclear weapon physicist Gregg Spriggs is leading a team of film experts, code developers and interns on a mission to hunt down, scan and reanalyze what they estimate to be 10,000 films of the 210 atmospheric tests conducted by the United States between 1945 and 1962. With many of the films suffering from physical decay, their goal is to preserve

this priceless record before it's lost forever, and to provide more accurate scientific data to colleagues who are responsible for certifying the stockpile every year.

"We've received a lot of demand for these videos and the public has a right to see this footage," Spriggs said. "Not only are we preserving history, but we're getting much more consistent answers with our calculations.

"It's been 25 years since the last nuclear test, and computer simulations have become our virtual test ground. But those simulations are only as good as the data they're based on. Accurate data is what enables us to ensure the stockpile remains safe, secure and effective without having to return to testing."

"The data must be off"

LLNL says that ten years ago, Spriggs was asked to write a computer code related to nuclear weapons effects, but his calculations didn't agree with what was published in the 1950s and 1960s. When he dug in to find out why there was a discrepancy, he discovered that the manual measurements made in the 1950s and 1960s were off, in some cases by 20 percent to 30 percent. His new mission had become clear: reanalyze all the nuclear test films to ensure future computer simulations would be validated.

"It was driving me nuts," Spriggs said. "No matter what I did, I couldn't get my calculations to agree. Eventually, I came to the conclusion that the data must be off. To prove our simulations are correct, we rely on quality benchmark data. That's why this project is so important. It is providing the data our physicists need to ensure our deterrent remains viable into the future."

Nuclear detonations are tremendously extreme events. To record the action, each test was captured by upward of fifty cameras, providing different vantage points and providing backup in case one of the cameras malfunctioned. Some cameras were designed to zip through hundreds of feet of film within a couple seconds, capturing every detail of massive fireballs in stunning slow motion. Others captured a frame or two every minute in order to record how mushroom clouds evolved over longer periods of time. The common thread between these films is that they contain a great deal of quality scientific data, data that can never be reproduced.

For rare film expert Jim Moye, the goal when scanning the films is simple: Create as exact a copy of the data as possible. To do so, Moye preps and cleans the film before scanning it with a customized Hollywood film scanner. Because much of the film is black and white, it contains a greater range of optical density (shades of dark and light) than the scanner can record in one pass. So Moye scans the film twice, first capturing the rich details of the darker shades before adjusting the scanner software to capture the lighter shades.

"It's fascinating to watch film that hasn't been seen in more than 50 years," Moye said. "This may be our one and only chance to preserve this historical record. It's critical that we capture as much of the data as possible. I truly feel like we're preserving history."

What a physicist looks for in a nuclear test

While the team certainly is preserving history, the driving purpose behind the project is to reanalyze the films to get a more accurate measurement of the yield (amount of energy released) of each test. To ensure accuracy, the team takes multiple measurements of a handful of different physics phenomena that independently correlate to test yield. Some films provide four to five different ways a scientist like Spriggs can calculate the yield, and agreement between these measurements means they have a number they can trust.

Nuclear detonations show two characteristic light pulses. This double-pulse phenomenon is evident in the video of the "Harlem event," a 1.2 megaton test that took place 13,645 feet above the Christmas Island area of the Pacific on 12 June 1962. The first pulse peaks almost

immediately as the shockwave first forms (0:09 in the video). The brightness then decreases as the superheated air, which is opaque when heated to above 3,300 degrees Kelvin — or 5,480.33 degrees Fahrenheit — shields the light from inside the fireball (0:10 in the video). As the shockwave cools to below 3,300 Kelvin, the air becomes transparent and the hot gasses begin to show through, creating the second pulse (0:21 in the video). Software developed by LLNL computer scientist Jason Bender scans each frame of the films to automate the measurement process. Bender's software notes the timestamp of both pulses of light, as well as the darkest frame between them. With this data, Spriggs can calculate the test's yield.

Tests like the "Bighorn event" display the mechanisms that lead to the formation of the iconic mushroom-shaped cloud. Bighorn was a 7.65 megaton test that took place 11,810 feet above the Christmas Island area of the Pacific on 27 June 1962. The fireball is spherical, almost sun-like, until the shockwave "outruns" the fireball, bounces off the ground, then smacks back into the bottom of the fireball, flattening it into the shape many have come to associate with a nuclear blast. The speed at which the mushroom cloud rises and the height of the cloud can be used to calculate yield.

The glow time of the fireball itself, as well as the speed at which it grows, also can be used to calculate yield. These measurements can be taken from the video of the "Turk event," a 43-kiloton test that took place 508 feet above the desert floor of the Nevada Test Site on 7 March 1955.

Measurements taken in the '50s and '60s focused on the rate of growth of the fireball. These measurements were done manually by projecting each frame onto a grid, with an analyst jotting down the eyeballed measurement before the projector's heat began to melt the frame.

"It's really amazing how close they got back in the '50s and '60s," Spriggs said. "The measurements they got for most of their tests were pretty accurate. But when it comes to ensuring the stockpile, we need to be certain. These are devastating weapons, and I hope they're never used in war. But the stockpile has been an effective deterrent for more than seventy years. My hope is that this project can help to make sure it stays viable into the future."

Playing at nuclear war

By Timothy Westmyer

Source: https://thebulletin.org/playing-nuclear-war11351

Dec 14 – The hallmark of a Norman Rockwell Christmas morning is gathering around the fireplace to drink hot chocolate and open gifts with your loved ones. Depending on what you find in your stockings this year, you might come face-to-face with nuclear war like you never have before. Virtually speaking, that is.

On the Christmas gift list of many children (and geeky grown-ups) these days are the latest virtual reality, or VR, systems for use with a video game console, computer, or smartphone. The PlayStation VR, HTC

Vive, Facebook's Oculus Rift, Samsung Gear VR, Google Cardboard, and others give enthusiasts many options to explore the rapidly emerging catalog of virtual reality games and applications.

In a way, this marks the latest iteration of a trend that has been around since the advent of the atomic age. Nuclear science and nuclear weapons have occupied a dominant position in mainstream popular culture, so it should be no surprise that VR has gone nuclear as well.

But virtual reality systems contain something inherently different: They use technology to create realistic images and surround sound to make a person sense that they are physically present in a simulated environment. This feature has the potential to make VR ideal for immersive storytelling and for professional training for emergency situations, as well as for documentaries and for what some refer to as nuclear disaster tourism.

And don't forget video games.

What remains to be seen is whether this brave new VR world could be harnessed to reduce the danger of nuclear weapons—or if it will remain an entertaining gimmick, destined to go the way of drive-ins and hula hoops.

To find out where the technology stood, I decided to try out the different virtual reality applications myself. After telling my wife that it was essential for vital research for an article I was working on, she let me buy a PlayStation VR. What follows is not an exhaustive compendium of all that is out there, but a few highlights—though it does take in virtual reality applications that have been created from around the globe.

Playing nuclear war in virtual reality

A great piece of art—whether it is a film, a painting, or even a video game—has the ability to provoke emotions and push the viewer to see an issue from a new perspective. During the Cold War, the anti-nuclear weapon movement used painting, music, poetry, and film to comment on nuclear risks. Now, that medium may be virtual reality.

First, some background. The VR setup uses a camera to track movements of a headset and two handheld controllers, so that when I turned my head or moved my arms, the 360-degree environment displayed on the visors moved in nearly perfect unison. Though a long way from the holodeck virtual reality environment featured in *Star Trek*, it is nevertheless extraordinary how riveting the visuals look and how strong a reaction they evoke.

There are certainly technical limitations in VR systems today. It can be difficult to focus the lens, and the graphics are a step down from what you see on high-definition televisions or the latest gaming consoles. There is a noticeable lack of tactile feedback and some people suffer from motion sickness after using VR for long periods of time. And while there are cheaper options available, high-tech VR systems are still largely cost-prohibitive for the average household.

But these constraints are unlikely to hold back VR systems as long as there is a steady demand for content. And the technology is sure to improve.

In my pursuit of what VR has to say about nukes, I tried out a handful of video games and several VR applications that are akin to interactive documentaries. The first game I tried was *Megaton Rainfall*, a "superhero simulator" designed by a company in Spain that gives you nearly unlimited power—but also the global responsibility of stopping an alien invasion. Inspired by the movies *War of the Worlds* and *Independence Day*, the game allows the player to fly around Earth to fight off intruders with powers such as a "Megaton blast" that can destroy massive spaceships but also inflict city-leveling collateral damage. The first time I missed an enemy and accidentally hit a city center, I was forced to listen to thousands of digital screams as a fireball destroyed people and collapsed buildings, with imagery torn straight from the most iconic nuclear detonations on film. No matter where I turned my head in real life, I was confronted with the verisimilitude of megadeath and needed to take a long break to regain my composure. This was not a situation that I found myself in playing Super Mario Bros.

Using a Google Cardboard VR headset and my smartphone, up next was the mobile game *Cold War Nuclear Strike VR*, made by a consortium of educators using technology to enrich teaching in schools across London. The game puts you in the backyard of an average early-1980s British home, enjoying your day before the radio advises you to seek shelter in a nuclear fallout bunker because World War III has just started. You only have a couple of seconds to head inside your bunker before the game declares you dead.

There is not much to do once you are underground, but players can look at the piles of recommended bunker supplies and at a survival checklist on the wall that has a reminder to stock the shelter with board games for your family. I suddenly noticed that I was standing alone; my virtual family apparently did not make it into the shelter with me. This realization

left me fearing for the safety of my virtual loved ones and feeling a creeping sense of survivor's guilt—something which the National Academies of Sciences' study, *Psychological Consequences of Disaster: Analogies for the Nuclear Case*, had said might happen. According to the game's creators, the stimulation of such feelings was intentional; their mission was to "create a scenario that presented pupils with a realistic experience of the genuine level of fear" during the Cold War and to "portray how life could change dramatically and instantly in the case of a nuclear strike." They also promised, however, to not "leave students traumatized" and instead "provide just enough jeopardy and threat to leave them feeling they have just experienced something significant."
(It's worth noting that the incredibly popular video game *Fallout 4*, about life after nuclear war, is also available this holiday season. The *Bulletin* already delved into the popularity of this game, but playing the expansive story in a VR environment promises to be an entirely different adventure.)

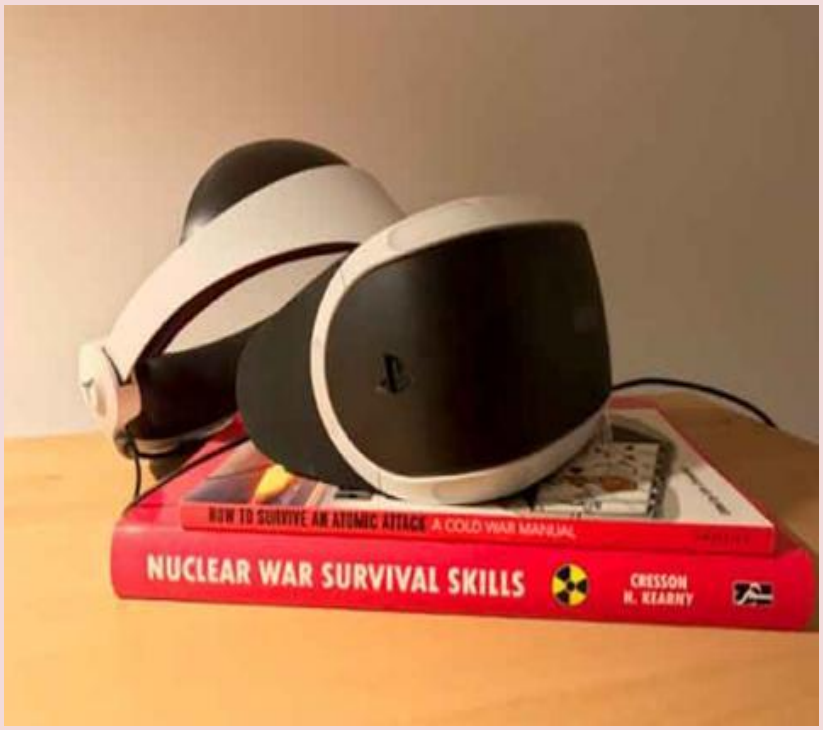
Nuclear tourism with a VR passport

Several virtual reality programs brought me on a tour of the same two key locations in nuclear history. The first was *Atomic Ghost Fleet*, an application developed by a UK-based company that lets you tag along with a marine research crew as they use 360-degree underwater cameras to film naval vessels sunk at Bikini Atoll by US nuclear tests in 1946. The story starts with you standing on a beach looking at the ocean as an immense atmospheric nuclear test mushroom cloud fills the screen. You then dive further into the narrative as a submarine visits ships that survived World War II, only to later be used as target practice in nuclear tests to measure the impact of atomic weapons against navies. Edited together with contemporary World War II footage, there were several moments where I forgot for a moment that I was not actually there, floating mesmerized past corals as big as the 44mm guns on the sunken *USS Lamson* destroyer itself, amid abundant schools of fish—showing the resiliency of life in the waters of Bikini Atoll after being laid waste by a nuclear test more than 70 years ago. I involuntarily swayed on my couch with the imaginary ocean current—which seemed as real to me as the sight of the massive submerged aircraft carrier right in front of me.
I turned next to a pair of virtual trips to Pripyat in Ukraine to witness a once-bustling community now largely abandoned in the aftermath of the 1986 Chernobyl Nuclear Power Plant disaster. *Frontline* partnered with New York University to film a tour of the exclusion zone with a guide who had been evacuated as a child but who now brings visitors to the site to share his experience and teach about what happened. *Return to Chernobyl* is an amazing look at the human toll of the nuclear disaster that displaced upwards of 300,000 people.
In contrast, the *Chernobyl VR Project* was a more interactive experience, designed by a studio in Poland, that "combines video games with educational and movie narrative software" to allow players to freely walk around locations and interact with objects on-site. Locations include the nuclear plant, a dilapidated school, an abandoned amusement park, the radiation containment shelter, and others. Players can hear from survivors of the accident and deploy Geiger counters to measure radiation levels at specific areas. The *Chernobyl VR Project* also lets you visit the Duga-1 radar, an over-the-horizon early warning system built to allow the Soviet Union to detect incoming ballistic missiles and heavy bombers from the US Eastern seaboard—before the system was contaminated by the nuclear accident.
The *Chernobyl VR Project* is a good example of how virtual reality systems could be used as an interactive learning tool. Walking around the 3D-rendered environment of a music room at the school, you can hear faded memories of instruments and children's laughter, alongside wind blowing through broken windows and the sounds of creaking floorboards. "Playing"—if it may be called that—a piano in the music room cues a narrator to begin talking about what life was like for average schoolchildren in the Soviet Union. These two virtual tours of Chernobyl leave the viewer with a deeper understanding of this tragic event in nuclear history beyond what even the best writers can describe on paper. I felt the sadness of the citizens of Pripyat in being uprooted from their homes, and their frustrations with the government's response to the accident—along with a sense of optimism about what Pripyat citizens were trying to build today.

Possibilities and pitfalls in using VR to teach about nukes

From my own immediate responses to the technology, I got the impression that virtual reality truly does have the potential to let people engage with nuclear topics in innovative ways. A well-made VR application can offer the closest thing to a real-life nuclear accident—making it a great hands-on training tool. Apparently, I am not alone in coming to this conclusion; an

official with the International Atomic Energy Agency's Incident and Emergency Center said that VR enabled his team to "conduct large scale [nuclear] emergency simulations" and let participants train "in environments impossible to simulate otherwise, such as emergencies with very high radiation exposure scenarios." Similarly, the Nuclear Futures Laboratory at Princeton University and the nonprofit corporation *Games for Change* are working together on using VR to demonstrate verification techniques for future nuclear arms control treaties, as well as helping the public understand the risks of keeping large nuclear arsenals ready to launch at a moment's notice.



Virtual reality applications may also be able to update how civil defense planners prepare for a nuclear attack. Instead of Civil Defense pamphlets and public service announcements, VR could help people visualize how to prepare to survive fallout, or what to do in the event of terrorists exploding a radiological dirty bomb. Of course, participating in a virtual reality experience in the comfort of your living room does not approach the horror of a nuclear detonation, but its immersiveness may help bring home the consequences of what happens when large quantities of radiological material or nuclear weapons are left vulnerable around the world.

Once you go beyond using VR as a training tool, however, and start to think about how it can be used in storytelling or as a call to action, the situation becomes much more complicated. It is not enough to just simulate the sights and sounds of nuclear horror. As I discovered, this exposure can leave you feeling overwhelmed and without the ability to do anything about it. I may have sensed a tiny fraction of what it is like to be near ground zero for a nuclear detonation, but what am I to do with this observation? The Doomsday Clock is at two-and-a-half minutes to midnight and my atomic anxieties are already dialed to eleven.

There are several endeavors that use virtual reality to try to deal with this problem of feeling helpless.

One is the *Ways of Knowing* project undertaken by Lovely Umayam, a research analyst with the Stimson Center and founder of *Bombshelltoe*, a blog featuring stories about nuclear history, politics, art, and media. This multimedia project uses 360-degree cameras and other VR technologies to better understand the Navajo people's health and traditions via their enduring, traumatic encounters with uranium mining. By sharing these narratives, the project seeks to ask whether there are "steps we can take as individuals or communities to support environmental rehabilitation and remediation caused by nuclear weapons production."

Another, similar project is the Australian VR movie *Collisions*, which tells the story of indigenous elder Nyarri Morgan, whose first interactions with the outside world were during the Maralinga nuclear tests in the state of Western Australia during the 1950s. Released in 2016 and featured at Sundance Institute, the story tries to come to grips with an often-overlooked part of the history of the land down-under, when British atomic bombs were tested on Australian soil.

What all these projects have in common is that they use the technology of virtual reality to tell powerful, nuanced stories that inspire people toward important causes. They are also evidence of how it is possible to keep the immersive nature of VR from devolving the player experience into atomic voyeurism. (For example, the popular DEFCON series—a real-time strategy game inspired by "the big board" of *Dr. Strangelove* and *WarGames*—lets users

play a game of global thermonuclear war. Earlier this year, a VR update was added, that allows players to sit in a simulated war room as spectators to the end of the world.)

On a similar note, disaster tourism—travel by curiosity seekers to sites of major catastrophes—can be a real dilemma for those seeking to better the public's understanding of these events. I would enjoy interacting with a simulated missile launch facility or a demonstration of how the president can authorize an attack with the nuclear football, but the application would need to be designed properly to work as an educational tool instead of just a game. Artists are free to create whatever art they wish, of course, and there is definitely a place for escapist entertainment in video games. But if they aim to inspire people to do more than sit in their Adirondack chairs to watch the spectacle of a nuclear bomb exploding, the creators of VR applications will need to think carefully about their craft.

Virtual reality is a cutting-edge technology that empowers storytellers and nuclear policy wonks alike so they can talk about nuclear weapons in imaginative ways. It can help people visit faraway destinations and engage on topics that remain largely inaccessible to the average person. If nuclear VR is handled irresponsibly, we will miss out on the broader possibilities. In the words of Lovely Umayam, "we need to widen the aperture" on what we envision that VR can accomplish.

As Edward R. Murrow once said about the disruptive new technology of television back in 1958: "This instrument can teach, it can illuminate; yes, and it can even inspire. But it can do so only to the extent that humans are determined to use it to those ends. Otherwise, it's nothing but wires and lights in a box."

***Timothy Westmyer** is a project manager in nuclear security at CRDF Global. He also hosts the Super Critical Podcast, which explores the portrayal of nuclear weapons in film, television, and other pop culture outlets.*

Is That Airport Security Scanner Really Safe?

Source: https://blogs.scientificamerican.com/observations/is-that-airport-security-scanner-really-safe/

The holiday season is upon us, and with millions of Americans expected to be traveling over the next few weeks there will be many more airport body scans than usual done by the U.S. Transportation Security Administration (TSA). Gone are the days of metal detectors and baggage screening alone as the means for airport security: The TSA introduced advanced imaging technology (AIT), better known as full-body scanners, as a primary screening modality in 2009. The widespread use of this technology across the U.S. ramped up after a passenger flying to Detroit successfully smuggled explosives in his underwear onto a U.S.-bound flight on Christmas Day of that year.

But AIT was introduced to airports across the country with very little transparency for passengers. As a result, most of the general public probably does not realize there is minimal proof these technologies actually prevent terrorist attacks, and there have been no long-term studies about their safety and efficacy. As a physician, I cannot help but question the risk/benefit balance involved. I have worried about risk ever since their initial implementation, and I have never set foot in a body scanner despite extensive air travel over the years—I always choose to "opt out" instead. The lack of clear benefit with no complete absolution of risk begs the question: Why is the TSA expanding the distribution of body scanners instead of getting rid of them?

The History of TSA Body Scanners

When AIT was initially rolled out, the TSA had two modes of screening: backscatter x-ray scanners and millimeter wave body scanners. Backscatter x-ray scanners used low doses of radiation in order generate a computerized image of the entire body These scanners came under significant fire by several different groups, including physicians and experts in the field of radiological research, due to their use of ionizing radiation—the kind that can break apart molecules. In a special report in 2011 for the *Archives of Internal Medicine* (now *JAMA Internal Medicine*) radiologists helped the public understand dose equivalents to the backscatter machines—with 50 TSA scans being equivalent to the exposure of one dental x-ray, a thousand scans roughly equivalent to a single chest X-ray, and so on.

Estimating the actual health risks that came with this added exposure, however, was more challenging. And despite the fact

backscatter machines use only low doses of radiation when compared with the exposure from routine medical procedures, the argument held strong that humans should not be exposed to ionizing radiation without clear medical benefit.

This argument formed the basis for a ProPublica and PBS NewsHour story that decried the nonchalance with which the government introduced this new method of security screening without reliable scientific testing of the risks involved. Despite these public concerns, backscatter x-ray scanners were deemed to provide only a "negligible individual dose" (pdf) of ionizing radiation in a special report on radiation protection issues prepared by the National Council on Radiation Protection & Measurements (NCRP) for the U.S. Food and Drug Administration.

According to the NRCP, a passenger would have to undergo 2,500 backscatter body scans in one year before exceeding the annual limit for ionizing radiation exposure from nonmedical devices. And although these minimal health risks did not faze the TSA, the European Union banned backscatter machines in 2011 due to health and safety concerns. The machines were also widely believed to violate passenger privacy, given the graphic nature of the images they produced. Ultimately the TSA began shelving the backscatter scanners in 2012 due to an issue with the manufacturer's privacy software (pdf).

With the shuttering of backscatter x-ray scanners, the TSA shifted to millimeter wave body scanners. These use electromagnetic waves to generate high-resolution images of unusual objects that might be concealed by passenger clothing; these anomalies are then superimposed on the image of a mannequin to protect privacy. The frequencies of the waves used by these scanners are measured in tens of gigahertz (GHz), and at these frequencies the radiation is considered high-frequency non-ionizing radiation—the kind of that heats up molecules.

Millimeter wave body scanners avoided many of the controversial issues that took down the backscatter x-ray machines, until the TSA issued a surprise update to their policy in early 2016, allowing agents to deny the right of passengers deemed to be security risks to opt out of the scans. Several privacy advocates spoke out (pdf) against this move, but the TSA pushed forward with their updated regulations.

Has AIT Been Effective?

The TSA blog regularly posts roundups of weapons discovered during TSA screening procedures. More often than not these posts make no mention of items detected with AIT. Body scanners have detected the occasional knife, underwear full of ecstasy, a plastic dagger and a loaded gun—yet everything but ecstasy and the plastic dagger would likely have been picked up by metal detectors, without exposing passengers to radiation.

What the TSA has not publicized is the high false-positive rates of millimeter wave body scanners, with a ProPublica report citing a 54 percent false-positive rate in Germany due to the machine picking up even sweat as a potential cause for concern. And whereas the backscatter x-ray scanners have been shelved, a team of researchers obtained their own backscatter body scanner and demonstrated multiple vulnerabilities in the scanners—from allowing weapons to be smuggled through to the machines' susceptibility to malware.

To date, there has not been a single report of aviation terrorism that was thwarted thanks to AIT. Even in the immediate aftermath of the underwear bomber's failed attack, statistical journalist Nate Silver placed the odds of being on any given flight with terrorist activity at less than one in 10 million in the decade preceding that incident. Nevertheless, nearly eight years after that pivotal moment in U.S. aviation security history, we are still scanning passengers with potentially harmful machines every day. A spring 2016 report from the TSA defends AIT—justifying the over $2.1-million cost of the scanners from 2008 to 2017 by arguing the machines "deter would-be attackers."

But when it comes to what AIT can or cannot actually detect, the TSA claims the information is classified. Even a former TSA agent spoke out against body scanners in an op-ed for *TIME*, arguing they are expensive and ineffective. The conservative the Heritage Foundation's compilation of 60 terrorist plots since 9/11 also notes no post-2009 events were foiled by AIT. And still the TSA firmly stands by the nearly 800 machines at over 150 airports across the country. My requests for comments from aviation security experts have gone unanswered.

The Facts about Health Risks of Millimeter Wave Body Scanners

To understand potential health effects from the millimeter wave body scanners, it is critical to understand non-ionizing radiation, which encompasses everything from high-frequency ultraviolet solar radiation to very-low-frequency radiation from electric and magnetic fields. The millimeter wave body scanners emit radiation that falls in the microwave range of the non-ionizing radiation spectrum. Other technologies in this category include cell phones, microwave ovens, radar, wi-fi signals and cordless phones. The International Commission on Non-Ionizing Radiation Protection (ICNIRP) issued a statement (pdf) regarding potential health issues associated with millimeter wave body scanners in 2012, making it clear that higher-frequency waves will lead to more energy absorption. Guidelines for exposure limitations are set for all non-ionizing forms of radiation to prevent problems from localized heating and, per the ICNIRP, the TSA millimeter wave body scanners provide only a tenth of the radiation limit for the general public.

So does this mean we are safe? According to the World Health Organization's current electromagnetic field project, there is really no way to know at this point. Ivan Brezovich, a professor of radiation physics at The University of Alabama at Birmingham's Department of Radiation Oncology, agrees these millimeter wave body scanners may not be 100 percent risk free and could have a biological effect. Brezovich explains that microwaves such as those from the millimeter wave body scanners can interact with the entire body, individual organs or with large molecules, thus having a potentially measurable effect. And although Brezovich was involved in experiments that demonstrated effects on cancer cells with radio frequency non-ionizing radiation exposure, he deems the risk of the millimeter wave body scanners as acceptable due to the low intensity and low penetration depth of the millimeter waves during the short scan duration.

In a world where we are all exposed to non-ionizing radiation every single day, its amount in our environment is only going to increase as technologies advance. As an example, even our cell phones have been deemed "potentially carcinogenic" by the International Agency for Research on Cancer (IARC). Couple this with our existence in modern society today and we are all living in bubbles of potential carcinogens that we cannot rid ourselves of. So although there is no proof of long-term detrimental health effects from chronic exposure to non-ionizing radiation, we have also not been able to prove there is an absence of risk from these regular exposures. Recent *Business Insider* analysis demonstrated Americans are millions of times more likely to die from heart disease or cancer than at the hands of terrorist attacks carried out by foreigners. And so, until there is proof that the machines either prevent terror attacks or are 100 percent safe even with long-term chronic exposure, I will continue to opt-out of AIT screenings.

Perhaps you should, too.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

Homemade Explosive Characterization Program helps keep Americans safe

Source: http://www.homelandsecuritynewswire.com/dr20171121-homemade-explosive-characterization-program-helps-keep-americans-safe

Nov 21 – **Each day almost two million Americans travel on commercial aviation domestically and internationally, and in addition tens of millions use America's mass transit systems.** In recent months, several significant plots to take down commercial aircraft and attack public spaces have been thwarted due to the mitigation efforts of law enforcement and government counter terrorism agencies across the globe. In August of 2017 Australian Police uncovered a plot to use explosives to bring down an Etihad Airways flight from Sydney. Throughout 2016 and 2017 there have been major bombings in Istanbul, Paris, Brussels and Manchester targeting airports, mass transit systems, concerts and other public venues. In addition, there have been dozens of foiled attempts by our adversaries to kill Americans and their allies as they travel, work and go about their daily lives. The Department of Homeland Security Science and Technology Directorate (S&T) says it is at the forefront of the response to, and mitigation against, such plots against the homeland.

S&T says that DHS S&T's Homeland Security Advanced Research Projects Agency (HSARPA), Explosives Division's Homemade Explosives (HME) Characterization Program directly addresses this threat environment by providing mission critical data collection, measurement of physical properties of threat materials, risk mitigation and modeling, and support for first responders against the terrorist threat. In fact, the explosive detection signatures data used by algorithms for the machines at the screening checkpoints at the airport were developed through the HME Program to keep the traveling public safe. S&T's HME Program has taken a leading role in several rapid responses regarding intelligence about terror plots and in the aftermath of successful terror attacks. Specifically, following the Australia plot the HME Program transitioned data to TSA which allowed them to enhance their mitigation strategies.

"The HSARPA HME Characterization Program is a key partner in assisting TSA to leverage screening technologies to their fullest potential in mitigating the highest and most credible threats to aviation," noted a TSA Senior Advisor Domenic Bianchini.

To accomplish the program's principal goal – mitigating terrorist threats to commercial aviation and other targets – the HME Program leverages extensive interagency relationships to conduct counter HME and threat mitigation research and development utilizing the best and brightest from across the explosives community, explained HME Program Manager Elizabeth Obregon. For instance, the HME Program's research and development (R&D) efforts in support of National Protection and Programs Directorate (NPPD) are using science to inform regulatory policy.

Three DHS S&T assets support the HME Programs goal of mitigating terrorist threats to commercial aircraft and other targets: The Transportation Security Laboratory (TSL) in Atlantic City, New Jersey; the Tyndall Reactive Materials Group (TRMG) in Panama City, Florida; and the Detection 'Technology Center (DTC) in Huntsville, Alabama.

TRMG conducts testing to provide critical characterization data and is indispensable in dealing with rapid responses to intelligence and/or new threat information as the unit is able to deliver data collection within days of threat identification. They also collect and store explosives too hazardous to be handled at TSL. TSL, an explosives community leader for certification and qualification testing, works in conjunction with TRMG, assisting with characterization work including synthesis, material property calculations, and detection system measurements. At S&T's DTC Facility the HME Program will partner with the FBI's Terrorist Explosive Device Analytical Center (TEDAC) Improvised Explosives Detection and Synthesis Center (TIEDS) to carry out a range of specialized characterization duties when the facility is scheduled to come fully online by the end of 2017.

S&T says that the data from the characterization efforts and the HME Program's other R&D projects enables decision makers to understand the full spectrum of HME threats and better respond to plots and

intelligence to ensure they do not evolve into successful terror attacks. When a new issue of Al-Qaeda's Inspire magazine is released advertising their latest strategies for attacking the American public, or a new terror plot is uncovered, the HME Program is ready to respond and assist its partners across the government to effectively counter and defeat the threat. Intelligence information on new threats can only lead to the development of effective mitigation techniques when it is assessed in conjunction with the R&D efforts of teams like the HME Program and its partners. The HME Program researches areas of detonability based on the physical properties of materials. This allows the development and maturation of security screening technology to keep the traveling public safe by enhancing checkpoint security and mitigating against evolving threats. Characterization data gathered by the HME Program is essential to the Transportation Security Administration (TSA) and other government end users, as it strengthens the explosives detection capabilities of the equipment and counters efforts by America's adversaries to defeat detection technologies. The HME Program has also developed a wide range of tools for law enforcement and first responders whose functions run the gamut from training, situational awareness and incident response to facility and force protection. These tools include the law enforcement and first responder DHS version of the Vulnerability Assessment and Protection Option (VAPO) from Defense Threat Reduction Agency as well as the Incident Management Preparedness and Coordination Toolkit (IMPACT).

"The S&T HME Program works with our partners to use actionable intelligence and data collection to inform and develop mitigation strategies and strengthen our detection, deterrence and response abilities in order to prepare for, and prevent an attack against American Citizens and our allies," said Obregon.

"The information generated from this program directly impacts the TSA Detection Standards, law enforcement and first responder training and preparedness, HME testing safety, the development of new detection methods and a host of other initiatives" Obregon concluded.

S&T notes that the work of the HME Program involves continuous collaboration with partners across the federal government including the Department of Defense, various national laboratories from the Department of Energy, the Department of Justice, the Department of State, and other U.S. and international public and private sector organizations.

Reducing IED threats: Commercially available precursor chemicals should be better monitored

Source: http://www.homelandsecuritynewswire.com/dr20171127-reducing-ied-threats-commercially-available-precursor-chemicals-should-be-better-monitored

Nov 27 – Policymakers' efforts to reduce threats from improvised explosive devices (IEDs) should include greater oversight of precursor chemicals sold at the retail level – especially over the internet – that terrorists, violent extremists, or criminals use to make homemade explosives, says a new report from the National Academies of Sciences, Engineering, and Medicine. While retail sales of these precursor chemicals present a substantial vulnerability, they have not been a major focus of federal regulations so far.

"The bombings of the Murrah Federal Building in Oklahoma City and the World Trade Center in New York City in the 1990s and those over the past few years in Paris, Brussels, and Manchester, in New York and New Jersey, and in many other communities around the world starkly demonstrate the long lived and persistent threat posed by IEDs," said Victoria Greenfield, chair of the committee that wrote the report, and a visiting scholar in the department of criminology, law and society at George Mason University. "The report stresses the importance of engaging in an ongoing deliberative process to reduce this threat."

The NAS says that the report, which was requested by the U.S. Department of Homeland Security, identifies, lists, and prioritizes precursor chemicals that can be used to make homemade explosives, using criteria on utility and use to separate them into Groups A, B, and C. The 10 chemicals in Group A constitute the greatest current threat and should be the highest priority for policymakers' attention, the report says.

Precursor chemicals enter the supply chain as imports or through manufacturing and make their way to industrial, agricultural, and other end users. Industry tracks the movement of

chemicals through much of the supply chain, but visibility and oversight appear to diminish as chemicals approach the end of the line. Data suggest that a terrorist can acquire enough precursor chemicals to manufacture homemade explosives through legal purchases from retail outlets. While the Oklahoma and New York City bombings employed thousands of pounds of precursor chemicals, many contemporary incidents have involved much smaller quantities that are readily available to consumers.

Conscious of the need to address this vulnerability yet minimize the burden on legitimate commerce, the committee assessed four general types of control strategy, directed at a subset of retail sales to noncommercial end-users, that is, the general public. Each strategy could include different combinations of mandatory and voluntary policy mechanisms, but three would feature a new control—a ban, a licensing requirement, or a registry for non-commercial purchases—and one would augment existing controls with increases in related outreach, training, and reporting.

Of the four types of strategy, none emerged as the best choice during the committee's deliberations on security, economic, and other trade-offs, the report says, noting that the committee lacked the time, resources, and directive from DHS to do an in-depth analysis of these policy options and that such an endeavor would require greater specificity about the terms of proposed actions. The report calls on DHS to use the committee's assessment as a starting point for engaging in a more comprehensive, detailed, and rigorous analysis of specific provisions for mandatory and voluntary policy mechanisms.

In examining possible policy options, policymakers and private-sector entities should consider strategies that would address multiple chemicals, rather than just a single chemical, the report says. Historically, terrorists' have modified their tactics by using alternative chemicals in response to single-chemical controls. The federal government also should provide more support for voluntary measures and programs that can help restrict access. Regardless of the path chosen, the report calls for re-evaluating priorities among chemicals and re-visiting policy responses regularly, in light of changing threats.

In addition, federal, state, local, and private-sector entities should explore strategies for harmonizing oversight of the sale and use of commercially available exploding target kits that are designed to produce homemade explosives, the report says. Some states have implemented rules independently, but no federal agency has explicit authority from Congress to oversee the sale of these kits.

NAS notes that the committee also identified opportunities for future research, including work to identify chemicals that could replace precursor chemicals in commercial products and to better understand how terrorists might respond to possible controls.

Former Staten Islander is one of 12 females in elite Navy unit

Source: http://www.silive.com/news/2017/11/post_1844.html

Nov 28 – Brianne "Brie" Coger first joined the U.S. Navy after graduating college because she was looking for a challenge.

Ten years later, the 34-year-old from West Brighton is now one of just 12 women enlisted as an Explosive Ordnance Disposal (EOD) technician.

After graduating from the University of Miami with a degree in theater in 2005, Coger looked for jobs as an actress and stuntwoman.

That was until she received an email about joining the Army reserve. She knew if she was going to do anything in the military, it was going to be in the Navy because of her experience in the water.

Coger spent most of her high school and college career on swim teams. She was a three-time Advance All Star during her swimming career at Curtis High School.

"The job looked like it would be an adventure, and that's what I was ready for," she recalled.

What is an EOD tech?

An EOD technician is responsible for protecting personnel and property from explosives. The Navy EOD is an elite combat force for countering Improvised Explosive Devices, Weapons of Mass Destruction and other types of weaponry.

Technicians are on call to respond to any type of ordnance, and investigating and demolishing natural and man-made underwater obstructions.

"The Navy's EOD techs are the only ones who take care of all explosives found in the water," Coger said. "We are the only ones who are able to dive and clear the way for ships, and protect infrastructure that happen to be near explosive devices."

Coger said she is trained to deal with chemical, biological, homemade and nuclear devices. What she likes most about her position is that she knows she isn't serving in the Navy to hurt anyone, but to protect United States forces.

Becoming an EOD tech

To become an EOD technician in the elite Naval Special Warfare/Naval Special Operations community, you must go through what is considered to be one of the most physically and mentally demanding military programs in existence.

"My community is very small and male-dominated," Coger said.

After serving in Spain and the United States, she went back to school to become a Navy instructor to work at the EOD Training and Evaluation Unit 1 in San Diego, Calif. She teaches explosive ordnance neutralization techniques to military members and civilians from around the world.

"Once I had served that time, learned my job better, became a subject matter expert in the fields in five different mission areas, it was time to pay back in the community and teach others how to do their job when deployed," she said.

Coger is living in Rhode Island for the next three months as she goes through boot camp to learn how to lead as an EOD officer.

Normal day

Every day is an adventure as an EOD technician. Coger's days can range from working in an office, going out on a boat blowing things out of the water or jumping out of an airplane during an investigation.

"The whole job is amazing, I think that's why these 10 years have flown by so quickly," she said. "I'm always traveling and doing something different. The main thing that stands out is the life the navy gave me and what it has provided me. I couldn't have asked for anything better."

Military dog awarded 'animal Victoria Cross' for sniffing out bombs under fire

Source: https://news.sky.com/story/military-dog-awarded-animal-victoria-cross-for-sniffing-out-bombs-under-fire-11129926

A courageous canine has been honoured for his bravery during a military operation in Afghanistan and awarded the prestigious PDSA Dickin Medal – the

"animal Victoria cross".

Mali, a Belgian Malinois attached to the Royal Army Veterinary Corps (RAVC), was presented with the accolade in London following the operation in 2012.

The eight-year-old dog, trained to sniff out explosives and detect insurgents, assisted in securing a key enemy stronghold.

He was twice sent through direct fire to conduct searches for bombs and continued to work despite being injured after three grenades went off.

PDSA director general Jan McLoughlin praised his "awesome ability and determination" and declared the animal "an incredibly worthy recipient" of the accolade. **He is now the 69th winner.**

The Manchester bombing: unknown unknowns and "hindsight bias"

By Dan Lomas

Source: http://www.homelandsecuritynewswire.com/dr20171206-the-manchester-bombing-unknown-unknowns-and-hindsight-bias

Dec 06 – The May 2017 Manchester Arena bombing could have been prevented, a report by the former Independent Reviewer of Terrorism Legislation has revealed. The 22-year-old attacker Salman Abedi, who killed 22 people and injured

512 others, had been a "subject of interest" to Britain's Security Service (MI5) in 2014 and 2015 but was classed as a "low residual risk" to national security and his case was closed.

David Anderson QC's report suggests there were opportunities to reopen the case, raising the possibility the attack could have been stopped. MI5 twice received intelligence reports which – had their significance been "properly understood" – would have reopened the investigation into Abedi. The intelligence was not "fully appreciated" and judged to "relate not to terrorism" but possible "nefarious activity or criminality". Abedi was just one of a number of closed subjects of interest (SOI) whose case needed "further consideration". A meeting to review the evidence was scheduled for 31 May 2017 – nine days after the Manchester Arena bombing.

MI5 had also missed the opportunity to place a port alert on Abedi following a visit to Libya in April 2017. Had they done so, Abedi could have been questioned and searched by counter-terror police four days before the attack. As with the Westminster Bridge attacker, 52-year-old Khalid Masood, Abedi was judged to pose little threat, yet struck with devastating results.

The findings form part of a review requested by Home Secretary Amber Rudd to provide "independent assurance" of internal reviews by the police and MI5, to assess intelligence and decisions before the attacks, and to "identify whether the processes and systems … can be improved".

Greater Manchester Mayor Andy Burnham said Anderson's report would be a "difficult read" for Mancunians, adding: "It is clear that things could, and perhaps should, have been done differently and that wrong judgements have been made."

The report led to a series of headlines suggesting MI5 had been caught napping. BBC News claimed the attack "could have been stopped," The Financial Times ran with the story that Abedi could have been "prevented", while The Daily Mail suggested MI5 had missed a series of red lines and were "alerted months" before the Manchester Arena blast. One commentator concluded that Anderson's conclusions are "damning for MI5." The implication being a so-called "intelligence failure" had occurred.

Yet headlines like these are misleading, neglecting the nuance in Anderson's report that the decision to ignore or misinterpret the intelligence on Abedi was "understandable" in the circumstances, overlooking the complex nature of counter-terror investigations. So, could the Manchester bombing really have been prevented?

Unknown unknowns

For the security services, piecing together the intelligence jigsaw is a difficult process. Post-mortem reviews often suffer from hindsight bias. Complex issues become easy to interpret. Intelligence previously considered irrelevant, becomes suddenly important. Knowing the end result often provides clarity where there was none at the time.

"Hindsight can sometimes see the past clearly – with 20/20 vision," concludes the 9/11 Commission report. In her classic study of the attack on Pearl Harbor, intelligence academic Roberta Wohlstetter found it "easier after the event to sort the relevant from the irrelevant signals." Intelligence before an event is "obscure and pregnant with conflicting" messages.

Intelligence agencies are far from the all-seeing and all-knowing entities of popular imagination. The very nature of intelligence means that the information available to the security services is often incomplete. Remember this classic bit of intelligence speakfrom U.S. Defense Secretary Donald Rumsfeld in February 2002? "We know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know."

Lord Butler's review of intelligence on Iraqi Weapons of Mass Destruction (WMD) also makes it clear that "intelligence seldom acquires the full story." When collected, the information is "sporadic and patchy". In these circumstances, intelligence gaps are to be expected.

Talk of failure also overlooks the growing tempo of counter-terror operations in the U.K. On Tuesday, MI5's Director General Andrew Parker told ministers that his service had prevented "nine terrorist attacks" in the previous 12 months. Since the 2013 killing of Fusilier Lee Rigby, 22 attacks had been foiled. MI5 and counter-terrorism police continue to be inundated with potential threats.

Amber Rudd revealed to parliament there were over 500 live operations – up by a third since the start of the year – with a further 3,000 extremists categorized as "subjects of interest". A further 20,000

individuals have been investigated and may pose a threat in future. The security services have to prioritize threats – sometimes with tragic results.

Intelligence failure?

In 2004, MI5 surveillance of the ringleaders of a fertilizer bomb plot, known as Operation Crevice, picked up two of the future July 7 suicide bombers – Mohammed Sidique Khan and Shehzad Tanweer. At the time, both were marginal figures. Continued surveillance of the Crevice cell led to successful prosecutions of others but Khan and Tanweer remained off MI5's radar until the 7/7 attacks. The pair killed 52 commuters on the London transport network with their co-conspirators. Questions were again asked as to how two terrorists fell through the gaps of an inquiry and went on to kill. But hindsight made it easier to connect the dots that MI5 had missed.

Anderson's report highlights that problems continue with the security services' strategies for dealing with "low level" subjects of interest that may suddenly pose a threat, a concern raised by the Parliamentary Intelligence and Security Committee in 2013. But claims that the Manchester Arena bombing could have been stopped are too simplistic.

The report acknowledges the "inherent uncertainty" of whether more could have been done, while, on the balance of probability, a "successful pre-emption… would have been unlikely." Abedi could have been stopped, for Anderson, had "the cards fallen differently." In reality, they rarely do. Simplistic headlines that the attack could have been prevented fail to understand the complicated situation facing the security services and do little to bolster public confidence in the U.K.'s counter-terror effort.

***Dan Lomas** is Program Leader, M.A. Intelligence and Security Studies, University of Salford*

What One (Badly Made) Bomb Can Do

Source: https://clarionproject.org/badly-made-bomb/

Dec 13 – At first glance, Monday's terrorist attack was truly pathetic. The terrorist, identified as Akayed Ullah, an immigrant from Bangladesh living in Brooklyn, detonated a homemade pipe bomb at the Port Authority Bus Terminal in midtown Manhattan. Ullah told police he carried out the attack in the name of ISIS.

No one was killed in the attack, although three people suffered minor injuries. The terrorist also injured himself. He has now been arrested and will face criminal charges.

The Islamic State and other terrorist groups gain legitimacy among their followers through their ability to carry out successful terrorist strikes against the West. Today's attack merely underscored the stupidity and incompetence of the would-be-killer.
Whilst it may be tempting to gloat at just how bad terrorists are at terrorism, we shouldn't feel too smug about it. The attack succeeded in three main ways.

1. It Put ISIS Back in the News

Terrorism is primarily a psychological tactic. The death count is viewed by the terrorist group as a bonus, but ISIS doesn't genuinely expect to kill all 323 million Americans one by one. They want to push their ideological agenda by making people scared that an attack could take place anywhere and any time.
A big part of that is media driven. The Islamic State's stated goal is to force a backlash against Muslims through repeated terrorist attacks and thereby forcing Muslims to accept ISIS as the defenders of Islam. So far it isn't working. Despite a minor rise in anti-Muslim hate crime, America and Western countries in general remain remarkably tolerant places.
Yet, every time ISIS is in the news carrying out an attack, it chips away at societal unity and advances their agenda.

2. It Inconvenienced Thousands of New Yorkers

As soon as the bomb went off, police evacuated and closed the Port Authority Bus Terminal on West 42nd street. For several hours, all trains skipped that stop while police held it on lockdown. They also evacuated several nearby subway stations.
This is part of the jihadist strategy of "death by a thousand cuts." The plan is to wear America down by repeated low-level attacks, until it eventually gives up, exhausted. The mass inconvenience caused by terrorist attacks is part of this. When people are late for work, forced to wait or reroute their journeys or otherwise made to suffer, this too is part of terrorism.

3. It Costs the State (A LOT) of Money

Both the FBI and the NYPD are involved in the Joint Terrorism Task Force, which is investigating the attack. There are a lot of people involved. Investigating something like this is a huge operation. The officers who physically shut down the Port Authority Bus Terminal, the detectives carrying out investigations, extra support teams called in for backup, all of these people have to be paid.
What about the trial? Judges and lawyers are not cheap. This is not even to mention the costs of incarcerating the suspect.
All of that money is coming straight out of your pocket, the taxpayer. With a bomb that costs no more than a few hundred dollars, a terrorist can drain the coffers of the state by hundreds of thousands, if not millions of dollars.
Monday's terrorist was an incompetent loser. But even without killing anyone, his attack still damaged America.

'Text message from boat' triggered bomb that killed Maltese journalist Caruana Galizia

Source: https://news.sky.com/story/text-message-from-boat-triggered-bomb-that-killed-maltese-journalist-caruana-galizia-11159533

Dec 15 – A bomb that killed a Maltese anti-corruption journalist was detonated by one of the suspects sending **a text message from a boat,** prosecutors believe.
Daphne Caruana Galizia's car was blown up as she drove from her home on the island on 16 October.
The assassination sparked outrage in Malta and among

many journalists and politicians in Europe and worldwide, who view it as an attack on free speech.
Three men, two of them brothers, were charged with her murder on Tuesday.
Seven other men were released on bail.
Police sources said it was suspected that George Degiorgio sent the text after getting a signal from his brother Alfred, who they think acted as a lookout.

A boat has been impounded and the sources say mobile phones have been recovered from the sea in Valletta harbour.
Vincent Muscat, 55, George Degiorgio, 54, and Alfred Degiorgio, 52, all deny murder.
They were also charged with manufacturing the bomb which killed the journalist, taking part in organised crime, as well as possessing explosives.
Caruana Galizia's family have released a statement saying that she was not investigating any of the 10 men arrested.
Witnesses to her murder describe seeing two explosions coming from her car and the vehicle skidding down the road, before ending up on fire in a field.
Her son, Matthew Caruana Galizia, said he found his mother's body in pieces.
Evidence suggests the bomb was placed in her rented car while it was parked in an alley outside her house.
The journalist's articles probed issues such as government officials named in the Panama Papers leaks, Malta's reputation as a tax haven, and links with Libya.
Malta's prime minister, Joseph Muscat, often a target of Caruana Galizia's articles, vowed no stone would be left unturned in finding the killers and has offered a €1m (£890,000) reward to bring her killers to justice.

How ISIS Produced Its Cruel Arsenal on an Industrial Scale

Source: https://www.nytimes.com/2017/12/10/world/middleeast/isis-bombs.html

Dec 15 – Late this spring, Iraqi forces fighting the Islamic State in Mosul discovered three unfired rocket-propelled grenades with an unusual feature — a heavy liquid sloshing inside their warheads. Tests later found that the warheads contained a crude blister agent resembling sulfur mustard, a banned chemical weapon intended to burn a victim's skin and respiratory tract.

The improvised chemical rockets were the latest in a procession of weapons developed by the Islamic State during a jihadist arms-manufacturing spree without recent analogue.
Irregular fighting forces, with limited access to global arms markets, routinely manufacture their own weapons. But the Islamic State took the practice to new levels, with outputs "unlike anything we've ever seen" from a nonstate force, said Solomon H. Black, a State Department official who tracks and analyzes weapons.

Space heaters that the Islamic State modified into improvised bombs. They could be set off in multiple ways and were most likely meant to target families returning home. Credit Craig McInally/Norwegian People's Aid

Humanitarian de-miners, former military explosive ordnance disposal technicians and arms analysts working in areas captured from the Islamic State provided The New York Times with dozens of reports and scores of photographs and drawings detailing weapons that the militant organization has developed since 2014, when it established a self-declared caliphate in Syria and Iraq.

The records show the work of a jihadist hive mind — a system of armaments production that combined research and development, mass production and organized distribution to amplify the militant organization's endurance and power.

The resulting weapons, used against the Islamic State's armed foes on many fronts and against civilians who did not support its rule, were variously novel and familiar. At times they were exceptionally cruel.

One report noted that before being expelled from Ramadi, Islamic State fighters buried a massive explosive charge under a group of homes and wired it to the electrical system in one of the buildings.

The houses were thought to be safe. But when a family returned and connected a generator, their home was blown apart in an enormous blast, according to Snoor Tofiq, national operations manager for Norwegian People's Aid, which is clearing improvised weapons from areas that the Islamic State left. The entire family, he said, was killed.

Craig McInally, also an operations manager for the Norwegian demining organization, described indiscriminate inventions elsewhere — including four seemingly abandoned space heaters and a generator recovered near Mosul.

The heaters and generator, useful to displaced civilians and combatants alike, were packed with hidden explosives. The bombs had been configured, Mr. McInally said, so that if a person approached them or tried to move them, they would explode.

A series of shoulder-fired, recoilless launchers made by the Islamic State, shown with a variety of repurposed projectiles. ISIS weapons engineers took Soviet-era munitions and made Western-style disposable launchers for them, even affixing written instructions for their use. Credit Damien Spleeters/Conflict Armament Research

Taken together, the scope and scale of Islamic State production demonstrated the perils of a determined militant organization allowed to pursue its ambitions in a large, ungoverned space.

Some weapon components, for example, were essentially standardized, including locally manufactured injection-molded munition fuzes, shoulder-fired rockets, mortar ammunition, modular bomb parts and plastic-bodied land mines that underwent generations of upgrades. Many were produced in industrial quantities.

The findings also included apparent prototypes of weapons that either were not selected for mass production or were abandoned in development, including projectiles loaded with caustic soda and shoulder-fired rockets containing blister agent.

While the Islamic State has been routed from almost all its territory in Iraq and Syria, security officials say that its advances pose risks elsewhere, as its members move on to other

countries, its foreign members return home and veterans of its arms-production network pool and share knowledge and techniques online.

"They're spreading this knowledge all over the world," said Ernest Barajas Jr., a former Marine explosive ordnance disposal technician who has worked with ordnance-clearing organizations in areas occupied by the Islamic State. "It's going to the Philippines, it's in Africa." He added, "This stuff's going to continue to grow."

An Islamic State weapons experiment that failed: a 120-millimeter mortar projectile filled with caustic soda, also known as lye. The fill is highly corrosive and can burn a victim's skin and respiratory tracts. It caused the munition to rust so badly that it could not be fired. Credit Ernest Barajas Jr.

Born of Insurgency

One reason for the Islamic State's level of sophistication was clear: Its armaments programs grew out of the insurgencies fighting the American occupation of Iraq from 2003 through 2011.

Sunni and Shiite militant groups became adept at making improvised bombs, both from conventional munitions abandoned in 2003 by Iraq's defeated military, and with ingredients that bomb-makers prepared themselves. American officials say certain Shiite groups received technical assistance and components from Iran.

Sunni bomb makers also fielded chemical weapons, sometimes by combining explosive devices with chlorine, a toxic substance with legal applications, and other times in bombs made from degraded chemical rockets or shells left from Iraq's defunct chemical warfare program.

An Islamic State improvised explosive device disguised to look like a rock, top, is triggered by a passive infrared sensor. The militants produced weapons like this by the thousands. At bottom, a sample of the Islamic State's signature homemade explosive mixture, prepared for testing after removal from a similar I.E.D. Credit Ernest Barajas Jr.

The Islamic State, which evolved from Al Qaeda in Iraq, built upon its predecessors' lethal industry.

The group's larger success since also played a role. When the Islamic State seized swaths of territory and major cities in 2014, it took control of shops and factories with hydraulic presses, forges, computer-driven machine tools and plastic injection-molding machines. It also moved into at least one technical college and university lab. This infrastructure positioned the Islamic State for an arms-production breakout.

Behind the capacity was an armaments bureaucracy that supervised product development and manufacture, said Damien Spleeters, head of operations in Iraq and Syria for Conflict Armament Research, a private arms-monitoring and investigative firm that has done field work in both countries during the war.

The system was resilient, Mr. Spleeters said. One of the Islamic State's projects, a series of recoilless launchers that gained prominence late in the battle for Mosul, in northern Iraq, was built from the ground up even while militants were pressured in combat from multiple foes on multiple fronts.

"It just kept going," Mr. Spleeters said of the technical advancements. "They could develop stuff even as they lost territories."

The Islamic State's arms bureaucracy was also disciplined. Detonating cord used in improvised explosive devices was measured and allotted down to the centimeter, Mr. Spleeters said. When a stock ran out, management would fill out a request form for more. The material would be resupplied.

Mr. McInally said the group's armament production appeared centralized and carefully considered.

As de-miners have found weapons, he said, they have routinely encountered improvised devices with a modular design that allowed for the Islamic State's fighters to choose from uniform parts and assemble devices quickly. The separate parts were issued distinctly, to be combined before use.

One of the suicide belts mass-produced by the Islamic State, top. For these weapons, ISIS engineers preferred to use the more powerful and reliable explosives scavenged from conventional ordnance the group had captured. At bottom, the granular explosive from one of the suicide belt's charges. Spectral analysis identified it as TNT, one of the most common military high explosives. Credit Ernest Barajas, Jr.

"It's a collection of pressure plates, a collection of charges, a collection of switches," Mr. McInally said. "Components that can be connected as necessary. It's clever. It's impressive."

The New York Times is withholding technical details of weapons and explosive mixtures described in this article to prevent the spread of information useful to copycats.

Mr. Barajas said the explosive charges themselves were further standardized — via a so-called homemade explosive with a recipe the group tweaked and produced at an industrial scale.

The mixture, he said, is a widely known combination of ammonium nitrate fertilizer and aluminum with a long history of use in many conflicts, including in Iraq. But the Islamic State improved the explosive with the addition of another material that makes it easier to detonate.

The Times previously documented the Islamic State's importation of large amounts of ammonium nitrate from Turkey, along with sections of heavy pipe.

Mr. McInally said the group also standardized other items: supplemental charges for mortar rounds to extend their range; a common fuze with a spring-loaded striker assembly machined from an over-the-counter bolt; and an improvised bomb — he said de-miners refer to it as a land mine — that was fielded in a standard-sized plastic tub.

Kurdish de-miners from the Swiss Foundation for Mine Action next to improvised land mines made by the Islamic State. Credit Steve Kosier/Swiss Foundation for Mine Action

The mines resemble an Italian-made antipersonnel mine called the VS-50, though the Islamic State's version is much larger, prompting de-miners to dryly refer to it as the "VS-500."

The components of a complex improvised explosive device made by the Islamic State. In what became a common tactic, ISIS connected multiple means of initiation to a single device. Any of the four pressure plates would have detonated the bomb if stepped on. Credit Steve Kosier/Swiss Foundation for Mine Action

As time passed, newly produced VS-500 mines became increasingly water-resistant, extending their life in the ground. Similarly, the striker fuzes that the Islamic State has fielded show signs of being made resistant to moisture and rust.

The first-generation land mines, Mr. McInally said, were not well made. "They didn't weather well," he said. But by the time the Islamic State was defeated in Mosul, he said, it had improved the design and salted the battlefield and villages with weapons "that last a long, long time."

The Islamic State has also engaged in organized scavenging, including collecting dud American-made bombs dropped by coalition warplanes and repurposing their explosive

power. One set of photos provided by a de-miner show how the group set up an open-air chop shop to cut open unexploded American aircraft bombs and remove the explosive inside.

These explosives tend to be more powerful and more reliable than homemade explosives. Mr. Barajas said the Islamic State put what it had scavenged to priority use — in suicide attacks.

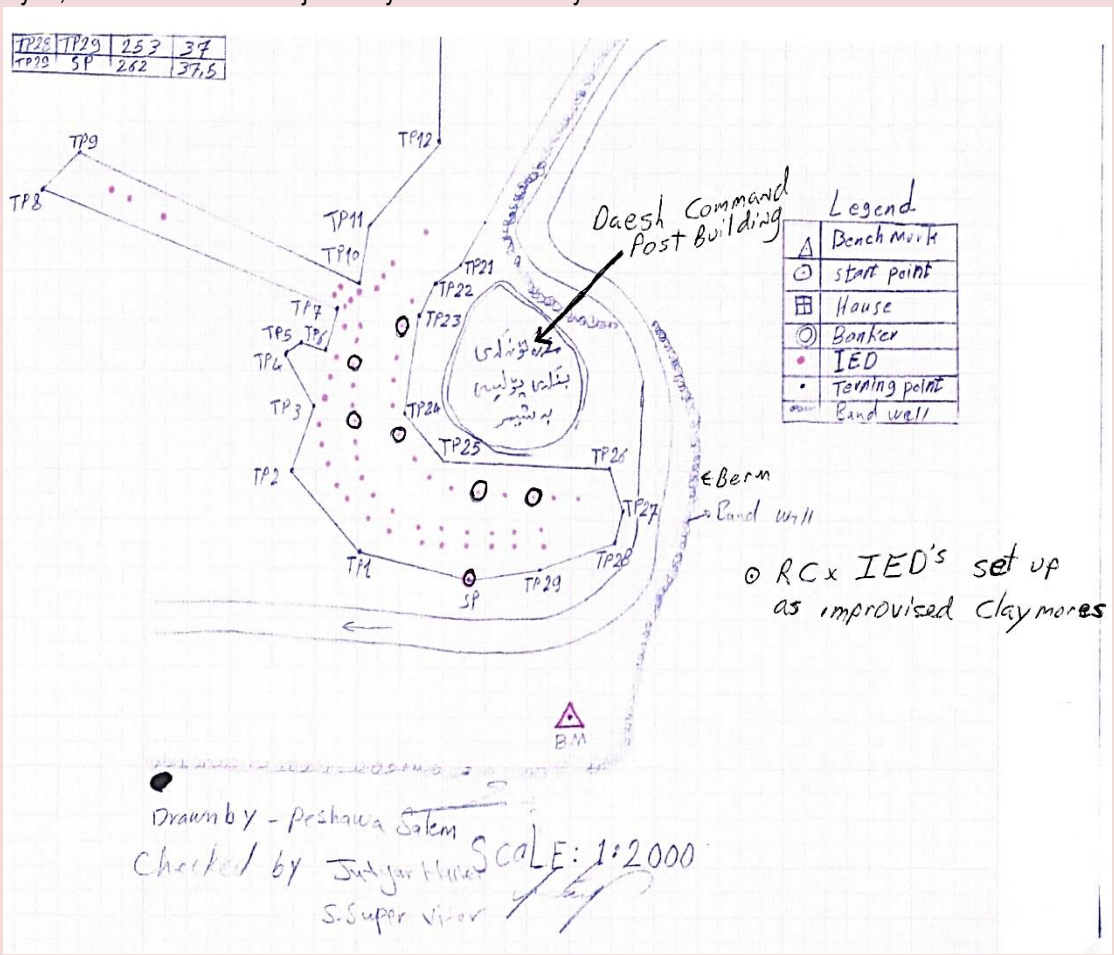
"Every time I'd run an explosive test on the ordnance buried in the ground, if I found it connected to the pressure switches, it would come back as 'homemade explosives,'" he said. But the explosives in suicide vests and belts, he added, were compounds, including RDX and TNT, extracted from conventional ordnance.

Not all of the Islamic State's developments have been effective. When experimental designs failed, Islamic State engineers made changes or moved on.

According to an American government official who examined an analysis of the rocket-propelled grenade filled with blister agent, the weapons would probably not fly a predictable and accurate path. X-rays, he said, showed that they had been only partly filled, and were unbalanced.

Similarly, the Islamic State seemed to struggle with a series of mortars filled with caustic soda, or lye, a strongly alkaline compound that is sold in a heavy flake form and sometimes used as a drain cleaner.

Dozens of locally produced mortar projectiles filled with caustic soda were found by de-miners in Manbij, Syria, in late 2016. Mr. Barajas analyzed the discovery.



A map drawn by a de-miner from the Swiss Foundation for Mine Action shows dozens of improvised explosive devices surrounding an Islamic State command post in northern Iraq. Credit Steve Kosier/Swiss Foundation for Mine Action

"Caustic soda is extremely hazardous. It'll burn your skin," he said. "If you inhale it, it'll cause death." But the material is also corrosive, so much so that it damaged the interior of the shells the Islamic State had used to hold it.

He said that the Islamic State tried loading 120-millimeter mortar rounds with caustic soda, but that the munitions rusted to the point of exuding salts. They could not be safely fired. "I think once they got this bad reaction, they moved away from this," Mr. Barajas said.

Put to Brutal Use

Many of the Islamic State's bombs have been used against the military and police forces fighting it. Aso Mohammed, a Kurdish de-miner with the Swiss Foundation for Mine Action, said that by his estimates, improvised explosive devices have been responsible for 60 percent of casualties of Kurdish pesh merga soldiers in Iraq's north.

But other uses were consistent with the Islamic State's well-documented disregard for international law and humanitarian concerns evident in their abductions, public executions, production of snuff films and bombings of public spaces.

In a prepared statement, the American military in Baghdad noted that coalition forces have recovered and destroyed booby-trapped teddy bears. De-miners and their supervisors in Iraq frequently trade reports and details of other Islamic State-made booby traps, among them dolls, stuffed animals and plastic trucks, as well as teapots, fire extinguishers, flashlights and copies of the Quran.

Two de-miners, Steve Kosier and Mr. Mohammed, of the Swiss demining organization, said that the Islamic State's locally made weapons had evolved in a predictably sinister fashion. Improvised devices that once were connected to a single plate that would cause the bomb to explode were later in the campaign connected to several plates — an adaptation intended to slow de-miners as they cleared buildings, roads and terrain.

Mr. Kosier said he had disabled one makeshift bomb that "had four pressure plates surrounding the container with a 9-volt battery for each plate." Each plate was connected by a separate electrical circuit to a container of homemade high explosives, which in turn had an "anti-lift device" beneath it — essentially a booby trap added to an already complex booby trap.

The ambition behind such a trap, de-miners said, is to kill people trying to make the Islamic State's former turf safe.

Casualties Surge From Land Mines and Improvised Explosives

Source: https://www.nytimes.com/2017/12/14/world/middleeast/land-mines-casualties.html

Sweeping for mines outside Debaltseve in eastern Ukraine. The conflict there contributed to a rise in deaths from land mines.CreditSergey Averin/Sputnik, via Associated Press

Dec 14 – Casualties from land mines and similar booby-trap explosives increased for the second consecutive year in 2016, to the highest level since a treaty banning such weapons of war took effect in 1999, a monitoring group said Thursday.

The group, the International Campaign to Ban Landmines, attributed the increased casualties largely to armed conflicts in Afghanistan, Libya, Ukraine and Yemen.

For 2016, the group recorded 8,605 casualties from land mines, including improvised devices triggered in the same way, as well as from other explosive remnants of war that are inadvertently detonated, often by unsuspecting civilians. The 2015 casualty figure was 6,461.

The figures include deaths and injuries, many of them suffered by children. The total in 2016 was the highest since the 9,228 casualties recorded 18 years ago when the land mine treaty first came into force.

"A few intense conflicts, where utter disregard for civilian safety persists, have resulted in very high numbers of mine casualties for the second year in a row," Loren Persi, an editor of the Landmine Monitor, the group's annual report, said in announcing the findings.

The report by the group, which won a Nobel Peace Prize for its work on the land mine treaty, was released in advance of a meeting of treaty members in Vienna next week.

In an improvement over 2015, the group said international donations for mine clearance and victim assistance rose sharply in 2016.

Thirty-two donors contributed $479.5 million, an increase of $85.5 million from the year before.

The treaty forbids the use of mines and other explosive devices placed on or under the ground, designed to detonate when a person accidentally steps on them.

Such weapons can be deadly for many years, long after a conflict has ended. Roughly four out of five victims are civilians.

The treaty also prohibits production, stockpiling and transfer of land mines. It has been signed by 163 countries — Sri Lanka was the latest, having officially joined on Wednesday.

Disarmament advocates widely regard the treaty as a success. But 34 countries remain outside the treaty, including China, Russia and the United States.

The United States has stated that it will observe the "key requirements" of the treaty except on the Korean Peninsula, where the demilitarized zone separating North and South Korea is heavily mined.

Algeria and Mozambique, which were once heavily mined, declared themselves free of land mines this past year, the Landmine Monitor said. Both are treaty members.

Government forces in Myanmar and Syria — neither of them treaty members — were the only ones known to have planted land mines during the past year, the Landmine Monitor said.

Nonstate militants, it said, planted land mines in at least nine countries: Afghanistan, India, Iraq, Myanmar, Nigeria, Pakistan, Syria, Ukraine and Yemen.

Eight dead and 30 wounded after suicide bomb attack in Pakistan

Source: http://www.telegraph.co.uk/news/2017/12/17/eight-dead-30-wounded-suicide-bomb-attack-pakistan/

Dec 18 – At least eight people were killed and 30 wounded when two suicide bombers attacked a church in Pakistan during a service Sunday, just over a week before Christmas, police said.

Two women were among the dead at a Methodist church in the restive southwestern city of Quetta in Balochistan province, said provincial Home Secretary Akbar Harifal.

Several of the wounded were in serious condition, police added.

Officials said security forces intercepted and shot one bomber outside but the second attacker managed to reach the church's main door where he blew himself up.

"Police were quick to react and stop the attackers from entering into the main hall," provincial police chief Moazzam Jah told AFP.

Balochistan provincial home minister Sarfraz Bugti said around 250 people normally attend the church on Sundays, but the congregation had swelled to around 400 because it was close to Christmas.

"God forbid, if the terrorists had succeeded in their plans more than 400 precious lives would have been at stake," tweeted the home minister.
An AFP reporter at the scene saw shattered pews, shoes and broken musical instruments littered across the blood-smeared floor of the church.

New Mine-Disarming Drones To Be Used In Syria

Source: https://i-hls.com/archives/80266

Dec 18 – New drones were demonstrated by Russia's International Anti-Mining Center's sapper units for mine-disarming.
Dmitry Klochko, director of LocMas who told mil.today: "To neutralize mines, we use small and very small quadcopters. An adapted drone picks up an anti-mine charge and puts it on a detected mine. After a time set by a sapper, an explosion occurs. This method has been already tested in Syria."
He added that experts of the International Anti-Mining Center operating on Syrian territories lately returned under governmental control are using, among other things, the STUPOR anti-drone portable system.

"Sometimes terrorists used drones to drop bombs right on the sappers. These were not fatal accidents, but they led to injuries. So, the military began to apply drone countermeasures", he said.

Denis Fedutinov, a leading Russian expert in unmanned systems, said drones were earlier used only for searching of explosives. "Good example is products of Austrian Schiebel that initially specialized in mine detection. It produced mine locators and other equipment, and then mastered production of unmanned aerial vehicles", the expert commented.

Another new sapper technology recently commissioned by the Russian Army's International Anti-Mining Center was a cooling vest for the OVR-2-02 body armor sets. Wearing such cooling vests, the sappers may work at up to 40°C.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

Hackers Substitute Porn on ISIS Sites

Source: https://clarionproject.org/hackers-substitute-porn-isis-sites/

Participants at the annual Chaos Computer Club computer hackers' congress in Hamburg, Germany (Illustrative photo: Patrick Lux/Getty Images)

Nov 23 – A group of Iraqi hackers placed porn on encrypted message sites used by Islamic State's 'news agency' Amaq.

The hacks are meant to disrupt the flow of communication between ISIS jihadis by creating havoc in the organization and mistrust of supporters for each other.

"Our intention was to flood the market with fake Amaq content in order to dilute the credibility of Amaq – a so-called news agency," one of the anonymous hacker told *Newsweek*.

The hackers call themselves Daeshgram, a play on the name of the encrypted messaging application Telegram that is favored by ISIS supporters. "Daesh" is an derogatory acronym in Arabic used to refer to ISIS.

"Daesh responded by telling supporters not to trust any of the Amaq links. They even had fights among themselves about the topic and deleted each other from various groups," the anonymous hacker said.

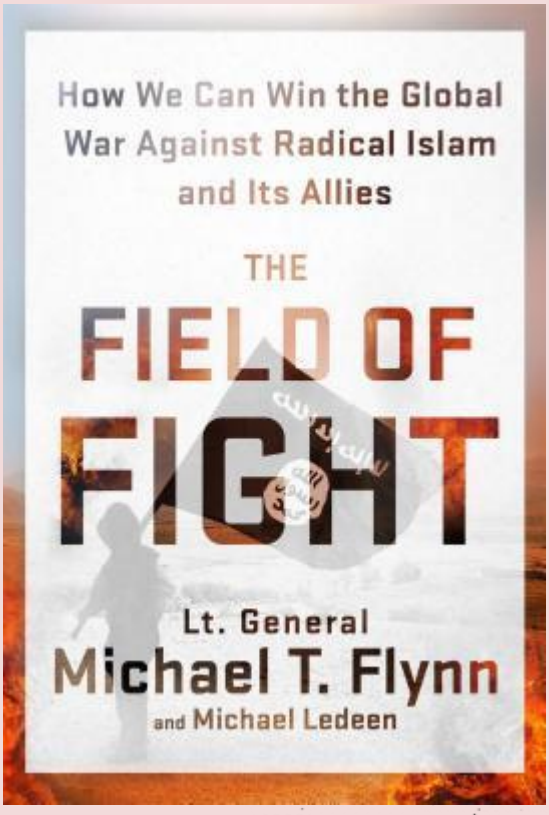
Hacks on other communications networks and apps have forced ISIS to rely only on Telegram in recent weeks.

Recently, another group of Muslim activists hacked into ISIS servers after the terror group announced it had upped its online security following a series of cyber attacks on Amaq.

"In response to recent events, we have imposed more stringent security measures on our systems," ISIS announced. "We can now handle email attacks or any type of hack."

"Challenge accepted" wrote the hacking group on Twitter. Barely three hours later, the hackers tweeted, "Challenge complete – too easy! 2000 email subscribers hacked from Amaq…What is next??"

The hackers then released the email addresses of Amaq subscribers online.



In his latest book, **Lt.-Gen. Michael Flynn**, former head of the U.S. Defense Intelligence Agency, wrote the computers of ISIS jihadis seized by the U.S. were filled with pornography.

"We looked a ruthless enemy in the eye — women and children, girls and boys, raped and exploited, the beheadings stored on a laptop next to pornography," wrote Flynn in ***The Field of Fight: How We Can Win the Global War Against Radical Islam and Its Allies.*** "At one point, we actually had determined that the material on the laptops was up to 80 per cent pornography."
Flynn said the pornographic material brutalized the psyche of the jihadists and enabled them to become desensitized enough to carry out the group's atrocities. He also said that closing down ISIS communication channels combined was the only way to defeat ISIS.
It was also revealed that assassinated al-Qaeda leader Osama bin Laden had an extensive pornography collection, which was seized by U.S. Navy Seals who killed him during a raid on his compound in Pakistan in 2011.

Russia increasingly uses hacker mercenaries for cyberattacks: FBI

Source: http://www.homelandsecuritynewswire.com/dr20171201-russia-increasingly-uses-hacker-mercenaries-for-cyberattacks-fbi
Dec 01 – **FBI director Christopher Wray told lawmakers Thursday that state-actors such as Russia are increasingly relying on hacker mercenaries, blurring the lines between government-backed hackers and cyber criminals.**
The FBI, by indicting two Russian intelligence officers and two criminal co-defendants for a major breach of the Yahoo email service in March, wanted to send the Russian government the message, Wray said.
"We are seeing an emergence of that kind of collaboration which used to be two separate things—nation-state actors and criminal hackers," Wray told the House Homeland Security Committee. "Now there's this collusion, if you will."
DHS is also following the trend, Acting Secretary Elaine Duke told the committee. "What we're having to do is really understand, as the director said earlier, the difference between state actors, people [who are] maybe just looking for financial gain and those hybrid actors and that's become more difficult," she said.

The *Free Beacon* reports that U.S. officials have long feared that cybercriminal networks, which operate with relative impunity in Russia, could be deputized to conduct hacking operations which serve the Kremlin's interests.
Russian President Vladimir Putin even said that it may have been Russian "patriotic hackers" who might have been behind the email breaches of the Democratic National Committee and the Hillary Clinton campaign.
Wray told lawmakers that increasingly, such hybrid government-criminal breaches are becoming a reality.
"You have the blend of a nation-state actor, in that case, the Russian intelligence service, using the assistance of criminal hackers, which you think of almost like mercenaries, being used to commit cyberattacks," the FBI director said.
"Russia is attempting to assert its place in the world and relying more creatively on a form of asymmetric warfare to damage and weaken this country economically and otherwise," he said.
"On a scale of 1 to 10," Acting Secretary Duke told lawmakers, the threat of a cyberattack on U.S. critical infrastructure is "a 7 or an 8." "Because what we know is daunting and we don't know what we don't know," she added.

Five programming languages with hidden flaws vulnerable to hackers

Source: https://www.techrepublic.com/article/five-programming-languages-with-hidden-flaws-vulnerable-to-hackers/

Dec 11 – Writing bug-free software is practically impossible, due to the impracticality of predicting every way in which code might be executed.

But even if developers go above and beyond to avoid flaws that can be exploited by hackers, attackers can often still take advantage of vulnerabilities in the design of the underlying programming language.
At the recent Black Hat Europe conference, IOActive security services revealed it had identified flaws in five major, interpreted programming languages that could be used by hackers in crafting an attack.
"With regards to the interpreted programming languages vulnerabilities, software developers may unknowingly include code in an application that can be used in a way that the designer did not foresee," it writes.
"Some of these behaviors pose a security risk to applications that were securely developed according to guidelines."
These are the five programming languages and the flaws that were identified:

1. Python

Currently enjoying a surge in usage, Python is regularly used by web and desktop developers, sysadmin/devops, and more recently by data scientists and machine-learning engineers.
The IOActive paper found that Python contains undocumented methods and local environment variables that can be used to execute operating-system commands.
Both Python's *mimetools* and *pydoc* libraries have undocumented methods that can be exploited in this way, which IOActive used to run Linux's *id* command.

2. Perl

Popular for web server scripting, sysadmin jobs, network programming and automating various tasks, Perl has been in use since the late 1980s.
IOActive highlights the fact that Perl contains a function that will attempt to execute one of the arguments passed to it as Perl code. It describes the practice as a "hidden feature" within a default Perl function for handling typemaps.

3. NodeJS

NodeJS provides a server-side environment for executing JavaScript, the language commonly used for scripting in web browsers.
IOActive found that NodeJS' built-in error messages for its *require* function could be exploited to determine whether a file name existed on the machine and to leak the first line of files on a system—potentially useful information for an attacker.

4. JRuby

The Java implementation of the Ruby programming language was found to allow remote code execution in a way that isn't possible in Ruby as a base language.
By calling executable Ruby code using a specific function in JRuby, IOActive was able to get the function to execute an operating system command, the Linux command *id*, by loading a file on a remote server.

5. PHP

The venerable server scripting language was used to call an operating system command, again the Linux command *id*, using the shell_exec() function and by exploiting the way PHP handles the names of constants.
"Depending on how the PHP application has been developed, this may lead to remote command execution," say researchers.
That said, many web admins have long known the potential risk posed by PHP's *shell_exec()* function, and how to disable it.
Exploitable flaws in each programming language were identified using a tool called a differential fuzzer, which was designed to automatically find vulnerabilities. The fuzzer works by running through a large array of scenarios in each language, calling each of the languages' native functions with a wide variety of different arguments and observing the results.

CybersecurityCyber trends in 2017: The rise of the global cyberattack

Source: http://www.homelandsecuritynewswire.com/dr20171212-cyber-trends-in-2017-the-rise-of-the-global-cyberattack
Dec 12 – What are the mega-trends across the cyber landscape in the Asia–Pacific?

The Australian Strategic Policy Institute (ASPI) International Cyber Policy Center's new report, Cyber maturity in the Asia–Pacific region 2017, distils the major trends from a year's worth of cyber events and looks at how countries in the region are measuring up to the challenges and opportunities posed by the internet and ever-more-connected IT infrastructure.

In a ASPI blog post, Tom Uren writes that although cyber maturity and cybersecurity generally improved over the past year, the threat landscape worsened. Cybercriminals are investing in more advanced and innovative scams, and nation-states are prepared to launch massively destructive attacks causing huge collateral damage.

The region (like other parts of the world) was affected by two state-sponsored malware attacks that were designed to cause serious damage. The WannaCry ransomware was notable for including EternalBlue (a highly advanced exploit that was reportedly developed by the U.S. National Security Agency), which allowed it to spread rapidly in many Windows environments with poor software update practices. Both the NSA and Britain's National Cyber Security Center attributed the attack to North Korea. Despite its use of sophisticated technology, WannaCry was so poorly executed that it failed to collect significant ransom money. It also contained a readily identified kill switch, which was used to prevent the malware from spreading. Even so, WannaCry affected more than 200,000 computers in over 150 countries, and the victims included factories, universities, and parts of Britain's National Health Service.

The NotPetya incident, attributed to Russia, involved a Ukrainian accounting software firm. Hackers breached the software update process and used it to distribute malware to the firm's clients using the software. The malware then spread through internal networks and wiped victims' machines. Although it targeted Ukrainian businesses, NotPetya caused huge collateral damage:

German pharmaceutical company Merck reported $310 million in direct costs and lost sales; US logistics company Fedex, $300 million; and Danish shipping company Maersk, $200 million. The Cadbury chocolate factory in Hobart was also shut down by NotPetya.

These events show that some states are actively and destructively using cyberweapons to gain advantage—either to raise money or to damage IT infrastructure.

The UN process that was attempting to negotiate limits on state behavior in cyberspace broke down earlier this year without agreement. The way ahead isn't clear. The United States has talked of forming a coalition of like-minded countries that could engage in joint action, and Australia has committed to measures to respond to these threats in its International Cyber Engagement Strategy.

Several countries in the Asia–Pacific have started to talk more openly about military cyber capabilities. The U.S. plans to elevate its military cyber unit, Cyber Command, to a unified combatant command to give it more independence and authority. Australia has established an Information Warfare Division and has declared that it has an offensive cyber capability that it's prepared to use to disrupt and deter cyber criminals targeting Australia. Japan has also proposed greatly expanding its military cyber investment, albeit from a very small base.

Although militaries traditionally shroud their cyber capabilities in secrecy, more transparency and doctrine-sharing would be welcome. Increased openness, collaboration, and other confidence-building measures would help to set expectations of state behavior, clarify how international law applies, and reduce the risk that cyber incidents will result in accidental escalation into armed conflict. Australia has led the way in this area; it is relatively transparent about its cyber offensive capabilities and has consistently emphasized that both international and domestic law applies in offensive cyber operations.

Cybercrime is also a huge issue in the region. With the rise of 'crime as a service', the technical sophistication needed to be a cybercriminal is lower than ever. The rewards are high and the chances of arrest are low. As countries in the region become better connected to the internet, rising levels of cybercrime threaten to undermine progress on economic development enabled by the internet. But government regulation and law enforcement make a difference. Tonga is a shining example—it became the first Pacific island to accede to the Budapest Convention on Cybercrime, a treaty that enables a cross-border approach to tackling cybercrime.

Uren notes that in a third worrying development, many countries use cybersecurity laws to impose or strengthen information control and censorship. Of the twenty-five countries covered in our report, just four—Australia, Japan, the Philippines and the United States—are classified as having a free internet.

Overall, cyber maturity improved across all countries in the region: governance, law enforcement and international engagement are stronger, and the internet is available to more

people. But progress is uneven. The countries that lead in cyber maturity—the US, Australia, Japan, Singapore and South Korea—continue to pull away from less developed countries that struggle to invest in cybersecurity and telecommunications in the face of more pressing economic and human development concerns.

"The spread of the internet provides huge development opportunities, but it also comes with its fair share of challenges," Uren concludes. "Australia and other developed countries in the region must directly address the challenges of dangerous state behavior, the spread of cybercrime, and a constrained and censored internet, by promoting our vision of a free, open and secure internet that will benefit all economies in the region."

"Watershed attack:" Hackers deploy new ICS attack framework, disrupting critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20171215-watershed-attack-hackers-deploy-new-ics-attack-framework-disrupting-critical-infrastructure

Dec 15 – Hackers working for a nation-state recently invaded the safety system of a critical infrastructure facility in what experts call "a watershed attack" that halted plant operations. Cybersecurity firm FireEye disclosed the incident on Thursday, saying it targeted Triconex industrial safety technology from Schneider Electric SE. Schneider confirmed that the incident had occurred and that it had issued a security alert to users of Triconex, which cyber experts said is widely used in the energy industry, including at nuclear facilities, and oil and gas plants. FireEye and Schneider declined to identify the victim, industry or location of the attack.

Mandiant, a unit of FireEye, recently responded to an incident at a critical infrastructure organization where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes. Mandiant says it assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which Mandiant calls TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers.

Mandiant notes it "has not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack."

Mandiant says that TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016. TRITON is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence.

Incident summary

The attacker gained remote access to an SIS engineering workstation and deployed the TRITON attack framework to reprogram the SIS controllers. During the incident, some SIS controllers entered a failed safe state, which automatically shutdown the industrial process and prompted the asset owner to initiate an investigation. The investigation found that the SIS controllers initiated a safe shutdown when application code between redundant processing units failed a validation check — resulting in an MP diagnostic failure message.

Mandiant assess with moderate confidence that the attacker inadvertently shutdown operations while developing the ability to cause physical damage for the following reasons:

- Modifying the SIS could prevent it from functioning correctly, increasing the likelihood of a failure that would result in physical consequences.
- TRITON was used to modify application memory on SIS controllers in the environment, which could have led to a failed validation check.
- The failure occurred during the time period when TRITON was used.
- It is not likely that existing or external conditions, in isolation, caused a fault during the time of the incident.

Attribution

FireEye, the parent company of Mandiant Consulting, says it has not connected this activity to any actor they currently track; however, "we assess with moderate confidence that the actor is sponsored by a nation state." The targeting of critical infrastructure as well as the attacker's persistence, lack of any clear monetary goal and the technical resources necessary to create the attack framework suggest a well-resourced nation state actor. Specifically, the following facts support this assessment:

The attacker targeted the SIS suggesting an interest in causing a high-impact attack with physical consequences. "This is an attack objective not typically seen from cyber-crime groups," says FireEye.

The attacker deployed TRITON shortly after gaining access to the SIS system, indicating that they had pre-built and tested the tool which would require access to hardware and software that is not widely available. TRITON is also designed to communicate using the proprietary TriStation protocol which is not publicly documented suggesting the adversary independently reverse engineered this protocol.

The targeting of critical infrastructure to disrupt, degrade, or destroy systems is consistent with numerous attack and reconnaissance activities carried out globally by Russian, Iranian, North Korean, U.S., and Israeli nation state actors, FireEye notes. Intrusions of this nature do not necessarily indicate an immediate intent to disrupt targeted systems, and may be preparation for a contingency.

Background on Process Control and Safety Instrumented Systems

Modern industrial process control and automation systems rely on a variety of sophisticated control systems and safety functions. These systems and functions are often referred to as Industrial Control Systems (ICS) or Operational Technology (OT).

A Distributed Control System (DCS) provides human operators with the ability to remotely monitor and control an industrial process. It is a computerized control system consisting of computers, software applications and controllers. An Engineering Workstation is a computer used for configuration, maintenance and diagnostics of the control system applications and other control system equipment.

A SIS is an autonomous control system that independently monitors the status of the process under control. If the process exceeds the parameters that define a hazardous state, the SIS attempts to bring the process back into a safe state or automatically performs a safe shutdown of the process. If the SIS and DCS controls fail, the final line of defense is the design of the industrial facility, which includes mechanical protections on equipment (for example, rupture discs), physical alarms, emergency response procedures and other mechanisms to mitigate dangerous situations.

Asset owners employ varied approaches to interface their plant's DCS with the SIS. The traditional approach relies on the principles of segregation for both communication infrastructures and control strategies. For at least the past decade, there has been a trend towards integrating DCS and SIS designs for various reasons including lower cost, ease of use, and benefits achieved from exchanging information between the DCS and SIS. We believe TRITON acutely demonstrates the risk associated with integrated designs that allow bi-directional communication between DCS and SIS network hosts.

Safety Instrumented Systems threat model and attack scenarios

FireEye says that the attack lifecycle for disruptive attacks against ICS is similar to other types of cyberattacks, with a few key distinctions. First, the attacker's mission is to disrupt an operational process rather than steal data. Second, the attacker must have performed OT reconnaissance and have sufficient specialized engineering knowledge to understand the industrial process being controlled and successfully manipulate it.

Even if cyber security measures fail, safety controls are designed to prevent physical damage. To maximize physical impact, a cyber attacker would also need to bypass safety controls.

The SIS threat model highlights some of the options available to an attacker who has successfully compromised an SIS.

Attack Option 1: Use the SIS to shut down the process

The attacker can reprogram the SIS logic to cause it to trip and shutdown a process that is, in actuality, in a safe state. In other words, trigger a false positive.

▶ **Implication:** Financial losses due to process downtime and complex plant start up procedure after the shutdown.

Attack Option 2: Reprogram the SIS to allow an unsafe state

The attacker can reprogram the SIS logic to allow unsafe conditions to persist.

▶ **Implication:** Increased risk that a hazardous situation will cause physical consequences (e.g. impact to equipment, product, environment and human safety) due to a loss of SIS functionality.

Attack Option 3: Reprogram the SIS to allow an unsafe state – while using the DCS to create an unsafe state or hazard

The attacker can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.

▶ **Implication:** Impact to human safety, the environment, or damage to equipment, the extent of which depends on the physical constraints of the process and the plant design.

Analysis of attacker intent

FireEye assess with moderate confidence that the attacker's long-term objective was to develop the capability to cause a physical consequence. The company bases this on the fact that the attacker initially obtained a reliable foothold on the DCS and could have developed the capability to manipulate the process or shutdown the plant, but instead proceeded to compromise the SIS system. Compromising both the DCS and SIS system would enable the attacker to develop and carry out an attack that causes the maximum amount of damage allowed by the physical and mechanical safeguards in place.

Once on the SIS network, the attacker used their pre-built TRITON attack framework to interact with the SIS controllers using the TriStation protocol. The attacker could have caused a process shutdown by issuing a halt command or intentionally uploading flawed code to the SIS controller to cause it to fail. Instead, the attacker made several attempts over a period of time to develop and deliver functioning control logic for the SIS controllers in this target environment. While these attempts appear to have failed due one of the attack scripts' conditional checks, the attacker persisted with their efforts. This suggests the attacker was intent on causing a specific outcome beyond a process shutdown.

Of note, on several occasions, FireEye has observed evidence of long-term intrusions into ICS which were not ultimately used to disrupt or disable operations. For instance, Russian operators, such as Sandworm Team, have compromised Western ICS over a multi-year period without causing a disruption.

Summary of malware capabilities

The TRITON attack tool was built with a number of features, including the ability to read and write programs, read and write individual functions and query the state of the SIS controller. However, only some of these capabilities were leveraged in the trilog.exe sample (for example, the attacker did not leverage all of TRITON's extensive reconnaissance capabilities).

The TRITON malware contained the capability to communicate with Triconex SIS controllers (for example, send specific commands such as *halt* or read its memory content) and remotely reprogram them with an attacker-defined payload. The TRITON sample Mandiant analyzed added an attacker-provided program to the execution table of the Triconex controller. This sample left legitimate programs in place, expecting the controller to continue operating without a fault or exception. If the controller failed, TRITON would attempt to return it to a running state. If the controller did not recover within a defined time window, this sample would overwrite the malicious program with invalid data to cover its tracks.

Recommendations

FireEye recommends that asset owners who wish to defend against the capabilities demonstrated in the incident, should consider the following controls:

- Where technically feasible, segregate safety system networks from process control and information system networks. Engineering workstations capable of programming SIS controllers should not be dual-homed to any other DCS process control or information system network.
- Leverage hardware features that provide for physical control of the ability to program safety controllers. These usually take the form of switches controlled by a physical key. On Triconex controllers, keys should not be left in the PROGRAM mode other than during scheduled programming events.
- Implement change management procedures for changes to key position. Audit current key state regularly.
- Use a unidirectional gateway rather than bidirectional network connections for any applications that depend on the data provided by the SIS.

- Implement strict access control and application whitelisting on any server or workstation endpoints that can reach the SIS system over TCP/IP.
- Monitor ICS network traffic for unexpected communication flows and other anomalous activity.

"Cyberbiosecurity" and the protection of the life sciences

Source: http://www.homelandsecuritynewswire.com/dr20171219-cyberbiosecurity-and-the-protection-of-the-life-sciences

Dec 19 – Biology and biotechnology have entered a digital age, but security policies around such activities have not kept pace.

That's according to Colorado State University's Jean Peccoud, Abell Chair of Synthetic Biology and professor in the Department of Chemical and Biological Engineering. Peccoud is lead author on a new paper in *Trends in Biotechnology*, urging awareness of "cyberbiosecurity" risks for researchers, government and industry.

The paper outlines how the evolving nature of biotechnology should sound alarm bells for new ways to keep life sciences assets safe. This could be from accidental cyber-physical breaches, or more nefarious threats.

"In the past, most biosecurity and biosafety policies were based on sample containment," Peccoud says. "Now, it's so easy to read DNA sequences, for example, or to make DNA molecules out of sequences publicly available from bioinformatics databases. Most projects have a cyber dimension, and that introduces a new category of risk."

CSU notes that Peccoud is a synthetic and computational biology who specializes in the design of new DNA molecules. He has led trainings for federal government agencies interested in increasing security around life sciences infrastructure, and has also helped assess the state of the nation's biodefense infrastructure.

Traditional practices fall short

Peccoud and co-authors explain that security policies in the life sciences fall into two categories: biosafety and biosecurity. Biosafety procedures are designed to prevent exposure to pathogens and accidental release of biological agents. Such measures include protective clothing, sterilization procedures and airlocks.

Biosecurity policies, however, are usually associated with travel, supply chains, or terrorist activities. Breaches of biosecurity can be accidental (a traveler bringing contaminated material from overseas) or intentional (bioterrorism).

Such policies fall short in protecting against threats from "the intricate relationship between computational and experimental workflows," according to the paper.

Nowadays, software tools can design DNA sequences with new properties. Gene synthesis techniques can theoretically be used to develop biological weapons derived from genomic sequences of pathogens. In fact, the federal government has developed new screening guidelines for providers of gene synthesis services.

Peccoud stresses that cyberbiosecurity risks are not always doomsday scenarios. There's a broad spectrum of risks that can start with fairly low-impact mistakes, such as mislabeled samples in a lab. Despite the risks, there is too much naive trust among partners in the biotechnology supply chain. That needs to change, he says, in order to increase productivity around biological research and to limit the risk of a significant incident.

Culture change

Peccoud likens this needed change to today's increasing awareness around cybersecurity, in response to high-profile hacking incidents of credit card and other companies. Decades ago, it was possible to use computer systems without a password, and it was common for several employees of a company to share a computer. Today, most people have at least some sense of how to manage their own cybersecurity. The same should be true for the life sciences, he says, and a major incident shouldn't need to be the impetus for change.

The authors recommend employee training, systematic analyses to examine potential exposure to cyberbiosecurity risks, and the development of new policies for preventing and detecting security incidents.

"Once individuals in a community are aware of cyberbiosecurity risks, they can begin to implement safeguards within their own work environments, and work with regulators to develop policies to prevent cyberbiosecurity breaches," they write.

— Read more in Jean Peccoud et al., "Cyberbiosecurity: From Naive Trust to Risk Awareness," Trends in Biotechnology 36, no. 1 (January 2018): 4-9.

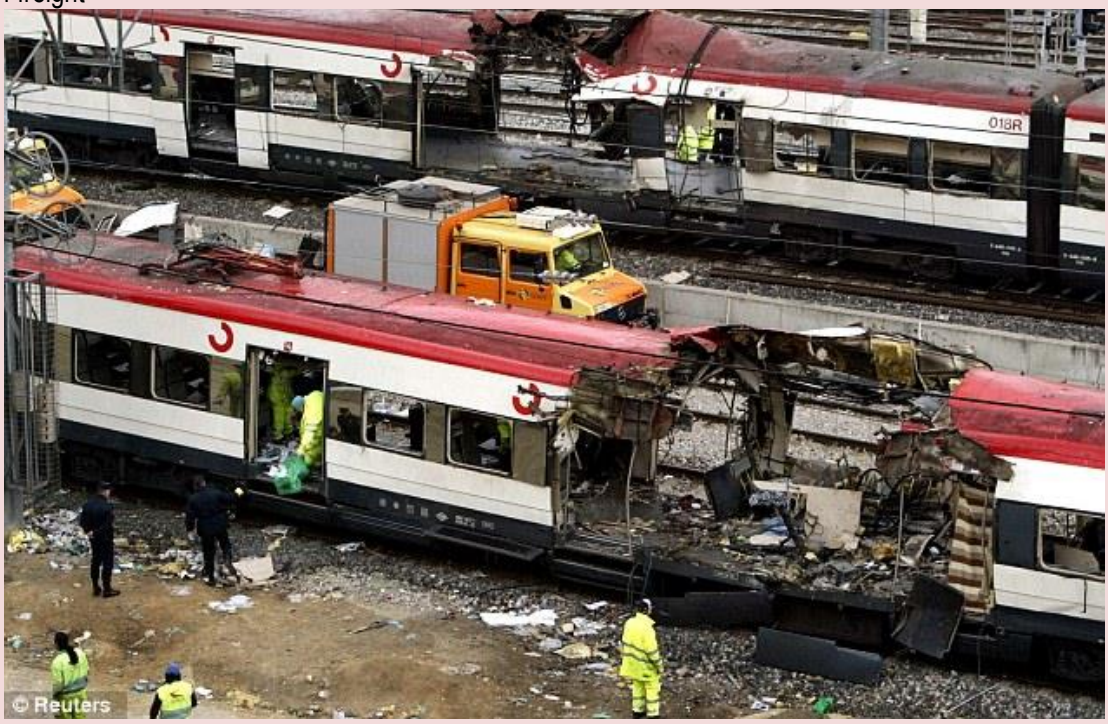

ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
EMERGENCY
RESPONSE

DomPrep Journal
November 2017
https://www.domesticpreparedness.com/journals/november-2017/

Emerging Threats to Rail Infrastructure

By Joseph Trindal

Source: http://www.domesticpreparedness.com/commentary/emerging-threats-to-rail-infrastructure-part-i-freight



Dec 06 – There is a desire for some bad actors to target rail systems, especially the hazardous materials freight rail network. This threat underscores the need for the rail transportation industry to maintain and strengthen partnerships with federal, state, and local authorities. With over 140,000 miles of infrastructure, there are difficult security challenges. For example, the U.S. rail system moves over 1.8 billion tons originated/year of freight, petroleum, chemicals, and military assets, making it a vital lifeline. A recent roundtable examined current issues and progress regarding this important topic from government and private sector experts.

Analysis of terrorist attack and plot trends targeting transportation infrastructure in developed countries demonstrates a growing interest in rail systems. Over the past 13 years, European rail systems infrastructure have been the increased focus of successful terrorist attacks, failed attempts, and disrupted plots. Examples include:

- The March 2016 suicide bombing on board a metro train at a station in the center of Brussels, Belgium, part of a coordinated operation that targeted the city's international airport, killed 32 people and wounded more than 300 others;
- The March 2010 coordinated suicide bombings in Moscow, Russia, subway killed 40 and injured more than 100;
- The July 2005 coordinated suicide bombings on three underground trains and a double decker bus in London, UK, public transport killed 52 people and injured over 700 more;
- The March 2004 coordinated bombings over a period of about four minutes on four commuter trains operating on the same line in Madrid, Spain, killed 192 people and injured over 1,800 others.

Noteworthy terrorist failures include the September 2017 attempt to detonate an improvised explosive device on board a London Underground train at Parsons Green station and the attempt to execute a mass shooting on board a high-speed train operating in northeastern

France in August 2015. In the United States, numerous plots envisioning attacks on domestic rail systems have been disrupted, the most advanced being a plan to detonate suicide explosives on board New York City subway trains foiled in September 2009. More recently, a plot to target a VIA Rail passenger train in the Toronto, Canada, area during the September 2012 to April 2013 period was disrupted by the combined efforts of a joint investigation. The Royal Canadian Mounted Police and the Federal Bureau of Investigation (FBI) monitored the two main plotters and the timely reporting of pre-attack surveillance observed by a conductor on a passing train operating on the targeted rail line.

Certainly, the interest of terrorist groups in targeting rail systems has persisted. In August 2017, al-Qaida published issue 17 of its *Inspire* online publication that focused on inciting attacks against both passenger and freight rail systems in the United States and Europe. On 10 October 2017, Domestic Preparedness moderated a roundtable discussion entitled "Emerging Threats to Freight Rail Infrastructure." The panel was comprised of distinguished speakers representing a board range of stakeholders in the freight rail transportation sector. Representatives from the following agencies and organizations contributed to this discussion on emerging threats and mitigation strategies in the freight rail transportation sector: Transportation Security Administration (TSA), Threat Analysis Division; TSA, Office of Security Policy and Industry Engagement; the FBI's Rail Security Program; the U.S. Department of Defense (DoD) TRANSCOM; National Protection and Preparedness Directorate (NPPD), Protective Security Coordination Division; Amtrak Police, Criminal Intelligence Unit; the Association of American Railroads (AAR); and the Secure Technology Alliance. Many interesting and relevant points were discussed during this important roundtable event.

Holistic Perspectives on Threat Mitigation

The panel acknowledged that, although the trends in terrorists' actions and priorities continuously evolve, so too are integrated measures to disrupt, detect, and mitigate threats to the freight rail industry. Recent events indicate a terrorist focus on the rail sector, but predominately target passenger and commuter rail systems. Attacks such as 2017 Parsons Green bombing in London and the 2016 Brussels bombings targeted urban commuter rail infrastructure during peak hours. TSA's officials made clear that the risks of attack on the freight rail sector are low. The FBI pointed out that their investigative activities still include cargo thefts by criminal actors and gangs, as well as disruptive activities targeting freight rail by environmental activists. The panel identified cyberthreats as an emerging challenge, a common public and private sector threat across customer facing, business, and operational systems.

The panelists agreed that defeating every threat is practically unattainable. However, disrupting plots and creating difficult environments that thwart attacks are key elements of a shared strategy for narrowing risks. It was pointed out during the discussion that, if some of the early indicators of the Parsons Green and Brussels attacks as well as other successful terrorist operations against passenger trains and stations had been recognized, reported, and acted upon, these plots may have been disrupted before the attacks were launched. According to a 16 September 2017 BBC news report, London's Metropolitan Police commissioner, Cressida Dick, stated that police had interdicted six "significant plots" in the months leading up to the Parsons Green attack. A shared challenge across the rail sector is recognition and early identification of threat indicators.

The TSA and FBI both noted that public and private stakeholders in the rail industry work closely together in developing broad understandings of threat indicators. TSA's Threat Analysis Division assesses data collected from a wide array of sources, domestically and abroad, to produce threat analysis products that are disseminated to stakeholders in both the public sector and throughout the rail industry in the United States and Canada. Although the discussion panel included representation from many organizations, the panelists knew one another well. Many panelists stated that they talk with one another on a daily basis.

Strength in Partnerships

Developing and maintaining a holistic threat understanding requires constant coordination among the stakeholders, both internal within government and external with the private sector. Thriving partnerships share certain common goals and understandings that weather the test of time. The 9/11 attacks caused significant economic impact across several levels of the aviation industry as well as disrupting many nation-state economies. For both public and private sectors, a unifying common thread is the shared understanding of economic consequences of terrorist plots that target critical infrastructure.

In the rail sector, the railroad police agencies have a long history of working with local public sector police agencies in investigating cargo thefts and rail asset vandalism. Today there is close interaction among federal, local, and railroad agencies, with the FBI's Rail Security Program and their local field offices taking a proactive role. The FBI frequently supports local law enforcement and railroad police agencies in nonterrorist criminal matters with intelligence and investigative support.

State, local, federal, and railroad partnerships are strengthened through a national network of local-based task forces, such as the FBI-led Joint Terrorism Task Forces (JTTFs). Numbering over 80 JTTFs nationwide, law enforcement representation includes railroad police in many locations.

The American Association of Railroads (AAR) is a nonprofit industry group representing the Class I freight railroads, Amtrak, and some regional railroads. The AAR expressed the strength by which the railroads collaborate with the federal and local government partners. The AAR member railroads have a long history of working with state and local first responders on both safety and security matters. Within the freight railroad industry, AAR leads its members in developing and maintaining unified security plans that are current and inclusive. The AAR unified security plan model focuses on five key areas: (1) train operations, (2) critical infrastructure, (3) hazardous materials, (4) military transport, and (5) cyber and communications. In implementing the plan, the AAR serves as the security information center for the railroad industry and facilitates preparedness exercises jointly, involving railroads and government officials across the United States and Canada. These regular, recurrent, structured exercises are designed to place plans and procedures under stress in realistic terrorism and cyberthreat incident scenarios, develop lessons learned in areas for improvement, and apply those lessons to strengthen future capacities for all participating organizations.

Relationships among federal, state, local, and tribal government agencies are stronger through the establishment of intergovernmental points of contact across jurisdictions. The growth of state and locally operated fusion centers has generated a network of intergovernmental collaboration. Operating under a National Network of Fusion Centers with unifying guidelines, intelligence, advisories, and lessons learned are rapidly and securely communicated. Private sector representatives with proper clearances and bone fide "need to know" are integrated into the National Network of Fusion Centers.

The Rail Sector Coordinating Council, stemming from the National Infrastructure Protection Plan, is the rail industry principal liaison forum of coordination between the railroads, stakeholder organizations, and the government. An important coordination strategy for AAR members is to achieve the goals of the National Infrastructure Protection Plan and sector-specific plans by proactively and collaboratively planning, training, exercising, sharing information, and assessing capacities against risks. The railroad industry supports the threat awareness of fusion centers through sharing of advisories on matters pertaining to terrorism, cyberthreats, and measures to mitigate risk.

U.S. Department of Homeland Security's (DHS) Protective Security Coordination Division fields Protective Security Advisors (PSAs) across the country to engage the 16 critical infrastructure sectors, which include the Freight Rail sub-sector. The PSAs' primary mission is to protect critical infrastructure. The five mission areas are: (1) plan, coordinate, and conduct security surveys and assessments; (2) plan and conduct outreach activities; (3) support National Special Security Events and Special Event Activity Rating Level I and II events; (4) respond to incidents; and (5) coordinate and support improvised explosive device awareness and risk mitigation training. PSAs are security subject matter experts who engage with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the nation's critical infrastructure. PSAs serve as regional DHS critical infrastructure security specialists, providing a local perspective to and supporting the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical infrastructure at the regional, state, and local levels.

In addition, there is a network of railway enthusiasts, called "rail buffs," who make a recreational hobby out of observing and noting railroad activity. Many rail buffs are well known to railway engineers and workers; some even on a first name basis. These rail buffs tend to be very familiar with their railway areas of interest and can easily spot suspicious behavior or activity. The rail buff network is loosely connected through the Railfan Network. Local railroad and law enforcement collaboration with rail buffs is an example of grassroots connectivity.

A collaboration challenge from some organizations is continuity of principal points of contact. For some agencies and organizations, personnel assigned to key collaborative positions change every few years. Relationships are built over time and, when personnel change with

promotions or reassignments, it can be disruptive. At the very least, a degree of institutional knowledge and expertise needs to be re-learned. This matter tends to be more of an issue with some of the federal agencies than local and railroad organizations.

Through the network of government, private, and citizen collaboration around the freight rail industry, terrorists' ability to prepare an attack is made more difficult, takes longer and provides much greater risk of detection and interdiction. Collaborative success is demonstrated in the high volume of thwarted terrorist plots in recent years.

State of Rail Sector Information Sharing

Networks of collaboration are only useful and sustainable if they provide value to the network stakeholders. Meaningful information sharing – distilled from data and intelligence analysis – is critical to keeping ahead of evolving terrorist threats. Within the federal agencies, there are verticals of information sharing between agency headquarters and the agency's field personnel. More important is the information flow that spans across agencies and includes private sector stakeholders.

The federal agencies with responsibilities for freight rail security today are closely integrated in sharing information across common networks and direct collaborative relationships. For example, the FBI information-sharing network goes beyond headquarters to the field, as the FBI oversees 84 JTTFs with representation across numerous federal, state, and local agencies. The FBI's Rail Security Program engages with railroads and other federal agencies at various levels, with multilateral information sharing. The FBI and TSA also collaborate with trusted international partner countries drawing on intelligence, incident analysis, and lessons learned. Collectively, the network of public and private information analysis, intelligence development, and sharing improves stakeholder threat awareness.

Agencies and private sector information sharing takes many forms. The joint government-industry coordinated Rail Intelligence Working Group (RIWG), is an example of public and private sector collaboration in action for information sharing. The group is comprised of representatives from the FBI, TSA, Amtrak, the American Public Transportation Association, and AAR – a partnership that remains unique across critical infrastructure sectors. Recently, the RIWG analyzed the video and the August 2017 *Inspire* edition. These materials urged supporters to target trains, particularly emphasizing so-called "Train Derail Operation" with lengthy instructions on building a "homemade derail device" for this purpose. The RIWG developed and disseminated informational awareness advisories through various rail industry and public sector networks, including the AAR's Railway Alert Network. These materials highlighted both the complexities of the actions advocated and the lack of understanding reflected in the magazine articles of the rail transportation system and its safety and security capacities. This cooperative effort reflects a joint commitment to sharing timely and useful security information across government and industry for security enhancement.

Complementing this work, the AAR publishes the Rail Awareness Daily Analytic Report (RADAR) as well as focused awareness advisories through the Railway Alert Network, keeping railroad and government stakeholders continuously informed on matters of relevance to rail security. Similarly, both TSA and the U.S. Department of Transportation produce and disseminate informational, intelligence, and alert products. Recipients of the governmental and Railway Alert Network products include officials with numerous federal agencies in the United States and Canada, state and regional fusion centers in the United States, and law enforcement and physical and cybersecurity leads for freight and passenger railroads in the United States and Canada.

The FBI's Tripwire Program has proven highly effective as a means for actionable information sharing. Described as "See Something, Say Something with focus," the Tripwire Program educates industry stakeholders on key trends and potential indicators of criminal terrorist preparation. Stakeholders are encouraged to report any suspicious activity with relevant details to local law enforcement or the FBI Field Office. The FBI conducts a structured assessment of Tripwire reports, some of which have led to preliminary investigations with a few resulting in criminal investigations and prosecution before planned attacks materialized.

Effective rail industry-centric information management ensures that priorities are aligned, and timely action is taken, in a concerted effort to create conditions to prevent bad outcomes. AAR pointed out three elements of the railroad industry's security strategy. First, understand that prevention is attainable. Second, worry less about what is not known and learn what can be known as thoroughly as possible. Third, avoid self-inflicted wounds through actions that

ease adversaries' ability to achieve their disruptive, destructive, and event lethal purposes. Gaining continuous situational awareness from reporting by railroad operators while providing these operators with relevant threat intelligence and related security information is advantageous for developing a results-oriented preventive posture.

Through effective information sharing that creates a climate of relevant awareness and response, threats can be either blunted or significantly mitigated in potential effects. AAR also stressed the need to ensure that information-sharing structures avoid inadvertently facilitating the preparation of criminals and terrorists. Rail operations and security information must be shared only with those who have a valid need to know. Government information-sharing networks are only accessible by credentialed personnel who have been vetted and meet agency standards for physical and logical access to systems and information. Similarly, railroads control access to security information received from all sources.

Cyberthreats, vulnerabilities, and attacks are increasing. Threats and attacks are focusing on public facing, business, and operational enterprise systems and devices, including person and nonperson tractions, personal and support staff, and third-party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. These threats have implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems, in addition to known ICS/SCADA weaknesses and vulnerabilities.

Public and private sector leaders are working together to address this threat. Cybersecurity is the fastest growing focus of railroads, government agencies, and DoD. DoD's reliance on commercial rail infrastructure has been long established. Today, DoD TRANSCOM's surface deployment mission is supported in large part by commercial railroads. DoD's rail deployments are closely synchronized with mission commands and the railroad industry, where movement information must be secure. Currently, DoD is working with the Critical Infrastructure Resilience Institute, a DHS Science and Technology center of excellence operated by the University of Illinois at Urbana-Champaign, to develop a refined cyberrisk scoring metric.

Similarly, AAR member railroads have elevated cybersecurity at the top of their priority lists. As freight rail systems become more automated and integrated, railroad investment in securing information technology networks – including those in development for the Positive Train Control system, which includes design to mitigate the risk of exploitation by cyberthreats. Amtrak pointed out that they have invested and continue to invest in securing their cyber systems. Nearly 85% of Amtrak's ticket sales take place on the internet. Amtrak police vigorously investigate growing volume of cyber and financial crimes involving their ticketing system.

A major challenge in top-down information sharing is the security classification of the information. The federal government Code of Federal Regulations (CFR) establishes requirements for managing unclassified but sensitive information. The term "Sensitive Security Information" (Title 49, CFR, Part 1520) is applied to information that falls short of meeting the National Security Classification regulations, but if disseminated it would be detrimental to the transportation security. TSA's sharing of Sensitive Security Information provides an important intermediate level for broader dissemination with regulatory safeguards and information security standards.

Freight Rail Security Regulatory Influence

Both DHS and U.S. Department of Transportation provide federal regulatory oversight of freight rail security matters. Additionally, some states apply regulations that impact freight rail security. The TSA Rail Transportation Security Rule (Title 49, CFR, Parts 1520 and 1580), promulgated in 2006, is among the federal regulations designed to strengthen rail industry security and reduce risk associated with the transport of security-sensitive materials. The Rail Security Rule developed into regulatory requirements practices that most railroads had already implemented. For example, the rule requires secure chain of custody of security-sensitive materials, which most railroads had already performed pursuant to agreed, voluntary security actions with TSA as a prudent business practice. The rule further requires regulated railroads to designate a rail security coordinator and mandates security concern reporting to TSA. The rail security coordinator requirement does enhance consistency in public and private sector coordination with the regulated railroads.

Regulations, at both state and federal levels, have generated linear reporting mandates and prescribed standards. However, regulatory reporting standards tend to be reactive and

cannot replace stakeholder driven initiatives to build strong, functional relationships. As one TSA official stated, "Our success has been built on collaboration, not regulation."

Many on the panel pointed out that regulation alone does little to enhance rail security and may, in some instances, produce the self-inflicted damage that should be avoided. The U.S. Department of Transportation requirement for railroads to report to states detailed information on the routes used, and frequencies of operations on those routes each week, by trains transporting high volumes of crude oil and other flammable liquids has resulted in publication of those schedules. Open-source publication of the operations of hazardous shipments unnecessarily releases security and safety information outside the first responder and community emergency planning agencies – and needlessly exacerbates risk.

Regulatory oversight by government inspectors and reporting regimes strain the railroads' personnel resources. In some situations, rail security coordinators and other railroad personnel are drawn away from performance based rail security matters to address report legibility or formatting. Security regulatory development and implementation should be collaborative between public and private sectors – as the private sector best practices often exceed regulatory standards.

Key Takeaways

The current and future state of freight rail security continues to change. The panel addressed a number of key strengths and some challenges for securing the nation's freight rail infrastructure. Some of the salient points from the Emerging Threats to Freight Rail Infrastructure roundtable discussion include:

- **Threats are dynamic** – There is significant evidence that threat trends involving the freight rail transportation infrastructure are changing. Intelligence assessments and extremists' propaganda and threats reflect a continuing interest of terrorists in targeting rail systems. Cyberthreats are increasing as well, which has implications for business and operations networks of railroads. Generally, the threat to rail systems is low but, as one participants stated, "Low does not mean 'no'."
- **Cyberthreats are increasing** – This includes attacks on public facing, business, and operational enterprise systems, including person and nonperson tractions, personal and support staff, and third - party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. This has implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems.
- **Criminal activities overshadow terrorist threat** – The federal, state, local, and railroad police agencies investigate far more cargo theft, vandalism, and disruptive criminal activity, including trespass and blockades by protesters, than terrorist plots involving the freight rail sector.
- **Stakeholder partnerships are strong** – The coordinated effort among federal, state, local, and private sector agencies and organizations is stronger than ever before. Through rail sector focused task forces, fusion centers, working groups and interagency networks, collaboration for planning, information sharing, training, outreach, response, and recovery are based on common goals of enhancing security.
- **Public and private partnerships are collaborative** – Stakeholder organizations in the public and private sectors have designated points of contact and established functional structures to promote collaboration and coordination around rail system security. Effective practices for elevating prevention and response capacities are widely shared among the railroads and with public sector agencies.
- **Information sharing is multi-lateral and relevant** – Intelligence and security information sharing occurs continuously among freight and passenger railroads, federal government agencies, state and regional fusion centers, and law enforcement agencies through a variety of networks. This extensive effort develops and sustains a current and relevant understanding of threat indicators and informs reporting capacities among stakeholders in industry and government. Enhancing security through constant emphasis on effective information sharing remains a common focus with public and private sector organizations. All involved apply appropriate protections based on need-to-know and access controls.
- **Freight railroad security focus and capacities are strong** – The Class I railroads, as well as most others, maintain strong security capabilities. AAR provides uniform and consistent guidance and support for its railroad members. The railroad industry's unified security plan in use by all Class I railroads and many others is an industry standard. AAR supports security awareness training through products disseminated to freight and passenger railroads via the Railway Alert Network and facilitates preparedness exercises for the

railroad industry, which includes public sector agencies in the United States and Canada. The railroads actively engage with federal, state, and local investigative and intelligence agencies to ensure continued access to relevant information and analysis.

- **Information security challenges remain** – Some information and intelligence obtained by federal agencies is highly classified and has limited distribution in its raw form. Agencies have developed standards for redacting or recasting classified information into unclassified intelligence products while still maintaining security protocols. TSA's Sensitive Security Information is an example of unclassified but sensitive information, which can be shared and managed in accordance with federal regulations. Representatives of state and local agencies as well as designated private sector employees, with bone fide need-to-know, may be sponsored for security clearance to receive classified briefings and intelligence products.
- **There are three key risk mitigation points** – (1) Understand that prevention is attainable; (2) learn as much as possible about what can be known; and (3) avoid self-inflicted wounds. Many potential threats and security risks can be avoided or substantially mitigated by acting on timely and actionable information. Develop thorough practical understanding of security threats at the right levels and align resources and capabilities accordingly. Recognize that resources are finite; partnerships based on common priorities and practical information can be effective in actionably preventing most risks. Avoid inadvertently making the terrorists' or criminals' planning and preparedness easier to put into action. Maintain informational and operational security over sensitive information that could be useful to terrorists and criminals.
- **Railroads are prioritizing cybersecurity** – As the industry moves toward greater reliance on integrated cyber systems, railroads recognize the economic returns for investing in secure system designs. Cybersecurity is a high priority throughout the railroad industry.
- **Railroad regulations have limitations** – Regulations levied on the freight rail industry have increased over the years. Many of the regulatory requirements codify and establish government oversight over best practices that had already been established by freight and passenger railroads. Some regulations between jurisdictions undermine strong security measures. Regulations alone do not create collaboration. Greater alignment between regulatory rule making and the railroads would go a long way to harmonizing best practices and achieving the shared goals between the public and private sector.

Conclusion

Western railroad system infrastructure continues to be an evolving terrorist target of interest. Expressed terrorist organizations' desires to sow economic harm through attacks involving critical infrastructures – for example, passenger *and* freight rail systems – is publicized in their global outreach to affiliated and non-affiliated groups as well as lone actors seeking recognition. Although the proliferation of global, web-based outreach by certain terrorist groups to unaffiliated groups and lone actors may indicate the effectiveness of multinational counterterrorist operations, it also creates new challenges for pre-attack detection and interdiction.

In the United States, the continued strengthening of public and private partnerships in the freight rail sector creates extreme difficulties for terrorists and criminals to succeed in executing attack plots. Intergovernmental cooperation and information sharing continue to improve with actionable lessons learned and pre-attack indicators shared bilaterally between local personnel and national agencies. Similarly, the daily interaction between the rail industry and government officials, at all levels, enhances situational awareness such that terrorist pre-attack and plot indications are more likely detected and proactively thwarted. Joint federal, state, and local interdiction and prosecution of terrorist plotters are indications of the successes stemming from public and private partnerships.

Challenges remain for private sector and government agencies in the freight rail sector. As demonstrated by the security and safety initiatives implemented by railroad companies and standardized by private industry organizations like the AAR, the private sector's economic interests drive innovation that stay ahead of government regulations. Many of the railroad companies' security procedures exceed regulatory minimum requirements, whereas some regulations even divert private sector resource priorities in counterproductive ways. Intergovernmental regulations and policies need greater alignment in developing cohesion between federal, state, and private sector shared objectives for freight rail security and safety. With emerging cyberrisks and

the growing need for information security in the global digital age, all stakeholders in the rail transportation sector need to examine ways to deny terrorist plotters and attackers access to open source information and resources. Creating greater difficulties for terrorists and criminals is a universally shared public and private sector sustainable goal.

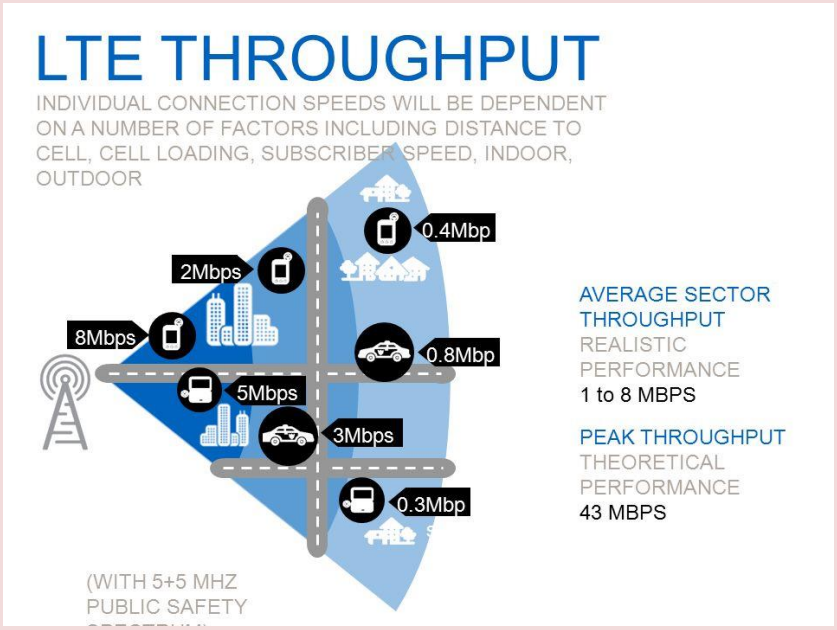
Joseph W. Trindal, *PPS, is a career homeland security professional with over 40 years of experience in both public and private sector. He has been a contributing writer to DomPrep for over 10 years. Having served for two decades with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal, he answered an invitation to contribute in creating the U.S. Department of Homeland Security (DHS) as regional director of the Federal Protective Service for the National Capital Region. During his service as an executive at DHS, he led a select team developing the Chemical Facility Anti-Terrorism Standards regulations, DHS's first legislated regulatory authority. Since his retirement, with over 30 years of government service, he continues executive service, now in the private sector security industries. A past president of the FBI's InfraGard, he led the transformation of the National Capital Region Chapter into a leader in public-private partnership initiatives. Currently, he is president and chief operating officer with the Akal Group of Companies, leading over 2,000 employees serving in 22 countries with a $250M portfolio of U.S. government and private sector contracts. Living in Virginia, and a veteran of the U.S. Marine Corps, he holds degrees in police science and criminal justice.*

Next-Generation Tech for First Responders

Source: https://i-hls.com/archives/80116

Dec 06 – First Responders often lack sufficient means of communications in an emergency, due to the lack of cellular coverage etc., a situation that makes it difficult to get vital information on real-time, make decisions and immediately perform their missions. The LTE cellular network developed by Motorola Solutions offers a solution: a mobile network for immediate deployment designed for critical missions.

According to the company's announcement, the LTE is a fourth-generation closed communication network which enables complete coverage in remote places and in the absence of cellular coverage: natural disasters and fires, terrorist attacks and other situations where cellular networks collapse; remote places such as forests and deserts, etc. The communication network enables conversations, communication with the push of a button (PTT), real-time video streaming and many other applications based on wideband.



The company which specialized in smart communication solutions and advanced technologies for public security agencies has recently widened the scope of its development of analytics and artificial intelligence technologies in Israel. Among its developments in the security field:

- Alexa for the security forces – a digital assistant which uses artificial intelligence, natural language processing engine and IIoT controls. The device enables operable voice commands and the supply of vital information for security forces and critical infrastructure teams, e.g. the remote operation of a police patrol vehicle – sirene turn on, gates opening and closing, traffic lights operation, etc.
- Fire brigade command and control system based on Microsoft's HoloLens headset and wideband communications (LTE) for the security forces. The systems supply the

firefighting commanders real-time imaging of the fire area and critical information from the scene, e.g. the oxygen status and other biometric parameters of the firefighters, as well as intuitive communications with the forces.
- A system combining a smart body camera with artificial intelligence and natural language processing engine enabling detection and identification commands.
- Automatic event calendar for command and control centers, a development enabling the documentation of police and security officers conversations over the communication system and their automatic conversion into text conversations (as in Whatsapp). The technology supplies better event management during an emergency when many events occur simultaneously.

The technologies have been developed in Israel, and in many cases basing on the experience and lessons learned from the response to terrorist attacks, accidents and natural disasters.

How to fight wildfires with science

By Albert Simeoni
Source: http://www.homelandsecuritynewswire.com/dr20171208-how-to-fight-wildfires-with-science

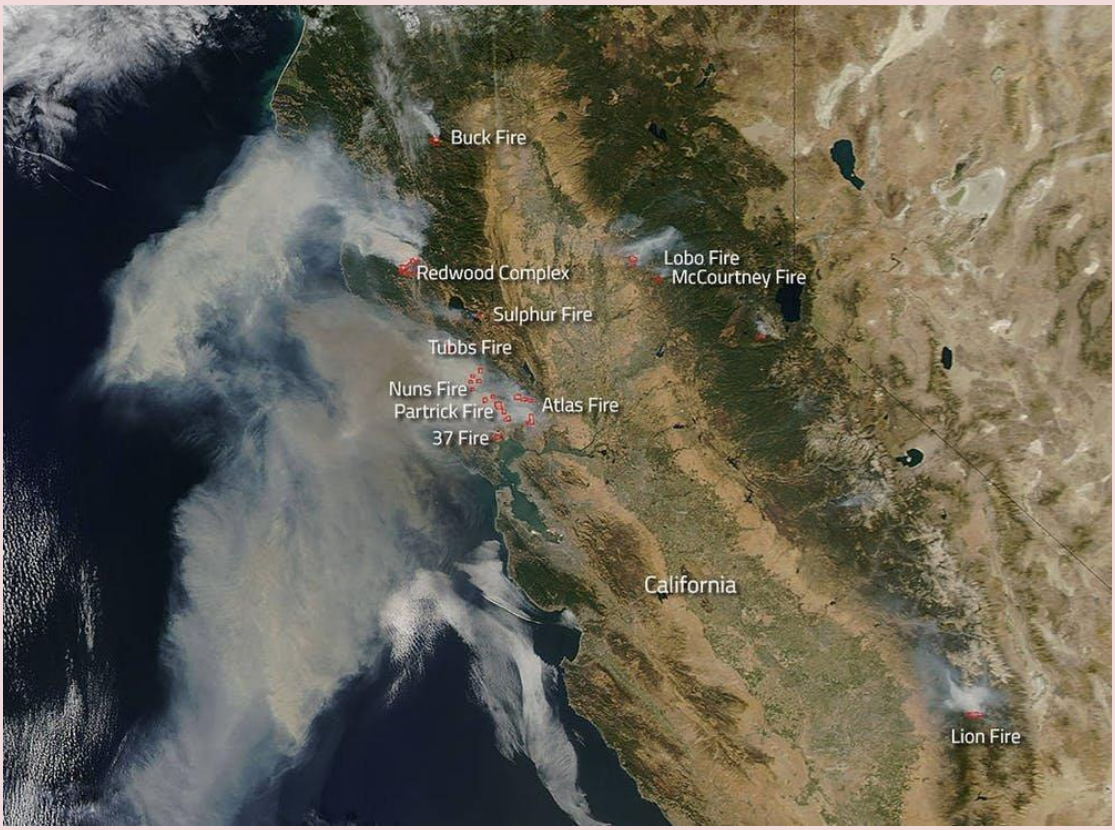
Dec 08 – **In the month of October nearly 250,000 acres, more than 8,000 homes, and over 40 people fell victim to fast-moving wildfires in Northern California, the deadliest and one of the costliest outbreaks in state history.** Now more wind-drive wildfires have scorched over 80,000 acres in Ventura and Los Angeles counties, forcing thousands to evacuate and closing hundreds of schools.
This disastrous fire season raises hard questions. Why have some communities that were deemed safe suffer major damage? Should they be rebuilt in the same way? Are there better ways to fight extreme fires and limit their impact? How can emergency planners prepare better for scenarios where full evacuation is not possible?
This is a global challenge. Brazil, Indonesia, many parts of Africa and Canada typically experience larger wildfires (measured by area burned) than the United States on a yearly average. This year Chile and Portugal have also suffered enormous losses. Australia's Black Saturday fires in 2009 were its worst fire event ever.
Fire is part of ecosystems in much of the world, so societies must learn to live with it. But key issues are still poorly understood. What is the right degree of fire management to decrease the impact of catastrophic fires? What is the most efficient way to protect the wild and-urban interface – the area where houses meet or intermingle with undeveloped wildland vegetation? And what is the best way to evacuate?
In my view and that of other researchers, many countries, including the United States, are underfunding research designed to answer these questions.

Moving into harm's way
Wildfires are increasing and affecting more areas worldwide. One cause is urban sprawl and the dramatic expansion of the wild and-urban interface. In the 1990s this zone increased by almost 11 percent in California, Oregon and Washington, adding over 1 million housing units – mostly in areas of moderate to high fire risk. At the same time, climate change is creating worse and more frequent wildfire conditions.
No one can control the weather, which is likely to become more extreme, but it is critical to do more to understand vulnerabilities that exist at the wildland-urban interface. Research has identified some factors that create these risks, including the ease with which homes ignite and the spread of fire between structures. Developing solutions will require quantifying the risks. It is also important to evaluate how vegetation treatment, structure hardening and better community design can decrease the likelihood of structural ignition and fire spread.

Winds, flames and fuels
U.S. building and fire protection standards and regulations have improved in the last 10 to 15 years, particularly in California, but many communities are still extremely vulnerable. Best practices, such as the National Fire Protection Association's Firewise USA program and California's Fire Safe, are a good start but should be expanded, based on research.

Understanding of vulnerabilities at a structural level is improving but not sufficient yet. Once fire moves from wildlands into developed areas, flames are fueled by engulfed homes and structures, creating conflagrations.

Better community design could help prevent this domino effect, averting massive property losses and evacuations. Communities should contain patchworks of flammable fuels such as vegetation, houses and cars, interspersed with less flammable and nonflammable areas such as parking lots and areas cleaned of vegetation. This strategy can decrease fire intensity, slow down fires and break down large fire fronts into smaller fingers that are easier to fight.



Another priority is the role of flammable building materials. Structural ignition often starts with firebrands – pieces of burning wood that are lofted by winds, and can spread wildfire past barriers and firebreaks – but scientists are still working to quantify their impact.

Many interacting factors influence whether and how wildfires will spread, including fire intensity, wind intensity, the quantity of firebrands that land on structures, the heat that impacts structures, how structures ignite, the distance between structures and vegetation, and the distance between structures. Researchers should aim to design suites of engineering solutions that will be versatile enough to adjust to specific scenarios and quantified exposures.

They should include small-scale steps, such as removing flammable vegetation, pruning trees, using less-flammable construction materials, and dealing with identified vulnerabilities such as fences. And they should extend to larger-scale strategies, such as breaking up wildfire fronts, slowing down fire spread and redesigning communities.

Major costs, modest funding

U.S. fire research is funded by the U.S. Forest Service, the National Institute of Standards and Technology and other federal agencies. Universities receive funding through the Joint Fire Science Program, which is jointly funded by the Interior Department and the Forest Service, and indirectly through other agencies such as the National Science Foundation, the Defense Department's environmental research programs and NASA.

Federal funding for fire research pales compared to the cost of fighting wildfires and the economic damage they cause. For example, in 2017 the Forest Service received about US$27 million for the National Fire Plan Research and Development Program and the Joint

Fire Science Program, while the Interior Department received about $6 million for the Joint Fire Science Program. President Trump's 2018 budget request would terminate Forest Service's participation in the Joint Fire Science Program and reduce the Department of the Interior's funding for the program to $3 million, which would mean no new projects and topics funded. Many members of the research community are concerned about this lack of investment.

For comparison, the Forest Service and Interior together spent nearly $2 billion in 2016 fighting wildfires. The Forest Service alone has spent over $2 billion in this fiscal year on wildland fire suppression. And preliminary damage estimates for the California wildfires range from $1 billion to $6 billion or more.

Similar pressures undercut funding for wildfire prevention in Portugal after its 2011-2014 recession. And the European Union stopped funding basic science related to fire dynamics and wildland-urban interface fires almost a decade ago, focusing instead on applied technological projects and more general research on natural disasters. Funding for firefighting has also declined in Russia, where environmental groups claim that the number of fires is significantly underreported.

Fire conditions are constantly evolving, and basic research coupled with engineering solutions must keep up. Designing more resilient communities and infrastructure and protecting people more effectively are not onetime goals – they are constant. Currently nations are failing to meet the challenge, and impacts on communities are increasing.

Albert Simeoni is Professor of Fire Protection Engineering, Worcester Polytechnic Institute.

Indiana's Emergency Response Guidelines for School Safety

By Robert Quinn

Source: https://www.domesticpreparedness.com/preparedness/indianas-emergency-response-guidelines-for-school-safety/

Dec 13 – The 2016 Legislative Session of the Indiana General Assembly passed Senate Enrolled Act 147 requiring the Indiana Department of Homeland Security (IDHS) to establish minimum standards and approve best practices no later than 1 July 2017 for a school emergency response system. The new guidelines are helping to improve school safety and security across the state and offer a template for other states to consider when reviewing and updating their emergency response systems.

Senate Bill 147 defines the term "emergency response system" and requires the department to establish emergency response system guidelines with input from the Division of School Building Safety within the Indiana Department of Education (IDOE). Emergency response systems were given the following definition:

> *Systems designed to improve technology and infrastructure on school property that may be used to prevent, prepare for, respond to, and recover from a manmade or natural disaster or emergency occurring on school property.*

The legislation was written in such a way that provided IDHS flexibility to develop a product that best addressed the legislative requirement. As mentioned in the definition above, it was important that the product addressed an all-hazards approach to school safety, which would more effectively address a well-rounded emergency response system. The legislation required IDHS to simply develop guidelines, rather than requirements for schools to follow. This has allowed Indiana schools to be flexible with their implementation of the guidelines.

Collaborative Effort

It was essential for state government to include external stakeholders in both the public and private sectors to ensure that the developed guidelines included the most appropriate information and was developed with input from around the state. The product working group involved nine Indiana professional associations related to public safety and education, federal professional associations, and state government agencies that brought important perspectives into the decision-making process (all partners are listed on page 1 of the document).

This group brought together approximately 20 individuals who met four times throughout 2016 and the first half of 2017 to implement a strategy, discuss and debate product content, and ensure that a well-rounded safety and security document was developed.

The Product

The final product, titled *Indiana School Safety Guidelines for Emergency Response Systems*, identified 17 school emergency response components as decided by the project working group. The components address the necessary pieces of an emergency response system that are encouraged to be included in every school. The guidelines focus on the following recommendations:

- Access Control & Visitor Management
- Training & Exercise Opportunities
- Planning, Procedure, and Policy
- Facility Safety Leadership and Direction
- Importance of Building Relationships with and Involving Local First Responders

These five topics are expanded upon within each of the 17 components.

One of the consistent themes of the product is "people over products." The group acknowledges the importance of physical tools for safety and security (e.g., doors, locks, windows), but without training these tools are less effective. Putting the focus on the people involved in school safety emphasizes building relationships with first responders, preparing uncommon stakeholders (e.g., facilities staff, parents, bus staff) for emergency situations, and identifying methods of utilizing the large student population as a trained safety and security mitigation tool.

On 1 July 2017, the project working group successfully developed a product that has been disseminated around Indiana. To share this information, professional associations, local emergency management agencies, and IDOE were utilized, and a copy was posted for the public on the IDHS website.

Moving Forward

The legislation not only required IDHS to develop guidelines, but also maintain them. No specific maintenance schedule was provided, but IDHS determined that an annual review of the product was appropriate and would disseminate an updated product on 1 July 2018.

With the 2017 product released, it is important that IDHS request feedback from individuals who work in and around schools on a daily basis. To do that, the IDHS needed to get into the communities and talk with its partners. This socialization initiative is helping to gain statewide agreement and support for the included content, to guide content, and to direct the future of this product.

IDHS identified County School Safety Committee Meetings, held in each Indiana County, as the best method for receiving product feedback. Meetings occur at the discretion of the committee, some on a monthly basis, whereas others occur once per year. County

commission meetings bring together representatives from the schools, first responders, local government, state government, and relevant private industry.
Through the end of 2017 and into early 2018, IDHS intends to attend county commission meetings around the state to elicit input. Through December 2017, IDHS has already attended 10 county meetings in various parts of the state. The important feedback received has seen information added to the National Incident Management Systems trainings that is specific to school employees and addresses the importance of providing safety training to part-time or contract staff.
The project working group will continue to play a critical role in the development and revision of this document. The working group will review any information included in this document to maintain transparency and collaborative input.

Robert Quinn *currently serves as the Indiana State continuity director for the Indiana Department of Homeland Security. In this position, he leads the IDHS school safety projects. Working with school safety specialists from around the state, he has been able to facilitate the coordinated efforts to create school safety guidelines assigned by the Indiana Senate Bill 147 (2016). He has been involved in addressing school safety topics such as architectural design and renovation of schools within Indiana, providing additional hazmat and radiological awareness information, improving both higher education and K-12 event management preparation, and assisting in the development and implementation of a statewide higher education/emergency management consortium.*

"It's your mother. She wants to know if you were wearing clean underwear."


IOI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
ASYMMETRIC
THREATS

Rethinking the value of water

Source: http://www.homelandsecuritynewswire.com/dr20171127-rethinking-the-value-of-water

Nov 27 – The value of water for people, the environment, industry, agriculture, and cultures has been long-recognized, not least because achieving safely-managed drinking water is essential for human life. The scale of the investment for universal and safely-managed drinking water and sanitation is vast, with estimates around $114 billion per year, for capital costs alone.

But there is an increasing need to re-think the value of water for two key reasons:

- *Water is not just about sustaining life, it plays a vital role in sustainable development*. Water's value is evident in all of the 17 UN Sustainable Development Goals, from poverty alleviation and ending hunger, where the connection is long recognized - to sustainable cities and peace and justice, where the complex impacts of water are only now being fully appreciated.
- *Water security is a growing global concern.* The negative impacts of water shortages, flooding and pollution have placed water related risks among the top 5 global threats by the World Economic Forum for several years running. In 2015, Oxford-led research on water security quantified expected losses from water shortages, inadequate water supply and sanitation and flooding at approximately $500B USD annually. Last month the World Bank demonstrated the consequences of water scarcity and shocks: the cost of a drought in cities is four times greater than a flood, and a single drought in rural Africa can ignite a chain of deprivation and poverty across generations.

Oxford says that recognizing these trends, there is an urgent and global opportunity to re-think the value of water, with the UN/World Bank High Level Panel on Water launching a new initiative on Valuing Water earlier this year. The growing consensus is that valuing water goes beyond monetary value or price. In order to better direct future policies and investment we need to see valuing water as a governance challenge.

Published in Science, the study was conducted by an international team (led by Oxford University) and charts a new framework to value water for the Sustainable Development Goals. Putting a monetary value on water and capturing the cultural benefits of water are only one step towards this objective. They suggest that valuing and managing water requires parallel and coordinated action across four priorities: measurement, valuation, trade-offs and capable institutions for allocating and financing water.

Lead author Dustin Garrick, University of Oxford, Smith School of Enterprise and the Environment, explains: 'Our paper responds to a global call to action: the cascading negative impacts of scarcity, shocks and inadequate water services underscore the need to value water better. There may not be any silver bullets, but there are clear steps to take. We argue that valuing water is fundamentally about navigating trade-offs. The objective of our research is to show why we need to rethink the value of water, and how to go about it, by leveraging technology, science and incentives to punch through stubborn governance barriers. Valuing water requires that we value institutions.'

Co-author Richard Damania, Global Lead Economist, World Bank Water Practice said: "We show that water underpins development, and that we must manage it sustainably. Multiple policies will be needed for multiple goals. Current water management policies are outdated and unsuited to addressing the water related challenges of the twenty-first century. Without policies to allocate finite supplies of water more efficiently, control the burgeoning demand for water and reduce wastage, water stress will intensify where water is already scarce and spread to regions of the world - with impacts on economic growth and the development of water-stressed nations."

In conclusion, co-author Erin O' Donnell, University of Melbourne adds: "2017 is a watershed moment for the status of rivers. **Four rivers have been granted the rights and powers of legal persons**, in a series of groundbreaking legal rulings that resonated across the world. This unprecedented recognition of the cultural and environmental value of rivers in law compels us to re-examine the role of rivers in society and sustainable development, and rethink our paradigms for valuing water."

— Read more in Dustin E. Garrick et al., "Valuing water for sustainable development," Science 358, no. 6366 (24 November 2017): 1003-05.


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

10 Questions for Selecting Business Continuity Software

By Erin Valentine

Source: https://www.domesticpreparedness.com/resilience/10-questions-for-selecting-business-continuity-software/

Dec 13 – Being resilient when faced with an emergency or catastrophic event requires preplanning to ensure that operations can continue with minimal interruption throughout the event or restart soon after the event. Business continuity software can help bridge the continuity gap during these times. Answering these 10 questions before purchasing will help ensure a good match between the software and the user. Choosing a business continuity software tool can be like choosing a new car. There is an overwhelming abundance of possibilities available in every model, size, and price range. The buyer narrows down the selection by asking themselves questions about functionality, capacity, affordability, and maintenance costs. An organization in the market for a business continuity software package should begin by asking themselves the same type of questions.

Question 1: Does This Organization Really Need Business Continuity Software?

Before shopping for a car, for example, buyers should consider whether they actually need a car at all. Maybe they could get by with a bicycle. Business continuity software is essentially the same at the core: a database capable of aggregating data and producing reports. User must then determine other criteria, for example: whether they need the system to do more than simply store information; and whether they have few enough plans that they can update and maintain the documents manually. If so, a database management system merged with a word processor may suffice.

Business continuity management can present a huge administrative burden. However, business continuity software allows the operator to input data once and have it cascade across multiple plans and reports. One alternative to expensive software is the Department of Homeland Security's (DHS) Ready.gov website, which offers a free Business Continuity Planning Suite with a training module, automated plan generators, and a self-directed exercise for testing the completed plans.

Question 2: What Does the Organization Need the Software to Do?

In the car scenario, the buyer considers the intended uses – for example, just to go back and forth to work every day, or to haul a trailer. If the user needs business continuity software to perform more complex functions, it helps to identify those needs before purchasing a product. Some features and functions to consider include, but are not limited to: Business Impact Analysis (BIA) tools; risk assessments; incident management capabilities; emergency notifications; tests and exercises; and mobile device applications. Some systems allow users to choose these options individually. The most important factor is that the user interface is simple and easy to use.

An integrated BIA tool can be particularly valuable in determining critical business functions and recovery times, as well as identifying assets and dependencies. The findings can then be integrated into business continuity plans. Many programs offer an incident management tool that can turn response and recovery plans into systematic actionable tasks with timed reminders and an event log. However, be sure the program can accept and store supporting files such as PDFs or Word documents.

Question 3: How Much Can the Organization Afford?

Pricing for business continuity software varies greatly depending on factors such as integrated capabilities, number of users, level of technical support, and hosting options. At some point, car buyers have to determine whether they can afford an initial deposit and monthly payments. Similarly, an organization considering business continuity software should prepare for an up-front implementation fee and annual licensing fees, in addition to potential charges for user training and technological support. Many programs base costs on the number of users. As the organization grows, the software needs to grow with it, which often requires additional user licenses.

Question 4: Who Hosts the Software and How Safe Is the Data?

The car shopper may consider vehicle security: street or garage parking at night; garage locks and security; and car alarm systems. Most business continuity software offered today is hosted in a cloud-based environment, but there are a few self-hosted solutions. For those interested in Software as a Service (SaaS), make sure to look into the security of the hosting data center. Federal government organizations require offsite data centers be certified by the Federal Risk and Authorization Management Program (FedRAMP). If the organization collects

personally identifiable information as part of the business continuity cycle, that data should not only be encrypted, but also backed up regularly and quickly recoverable.

For a car, this may include determining whether a bike rack from the old car will fit onto the new one. For business continuity, whether the existing technology works with the new technology may be a concern. Some business continuity software is designed to integrate with third-party applications, such as human resources databases. This type of functionality saves a great deal of time, especially when personal contact information has to be updated across multiple databases and plans.

Other business continuity software is designed to integrate with emergency notification services like Everbridge. The user can activate the notification feature using personnel contact information inside the business continuity software. Other useful features include integration with existing Geographic Information Systems (GIS) and Active Directory services.

Question 6: How Easily Can the Software Be Implemented?

How the organization has been managing its business continuity to date, how is has been storing its data, and how it has structured its plans help answer this question. The organization should make sure that existing data could easily be imported. Most business continuity software allows for the upload of spreadsheets. When it comes to formatting plans, however, most software is less flexible. If the organization currently creates plans in a word processing program, the new software may not be able to recreate that format exactly. In car terminology, the person buying a new car should not expect the gas tank to be on the same side of the car as the old one.

Other issues may arise for organizations whose business continuity programs are less mature. In the past, the business continuity coordinator may have been doing all the heavy lifting. Once a software program is implemented, individual plan owners may be asked to complete an online BIA or input plan data themselves. If the organization's business continuity program is not fully mature, it may be difficult for employees to understand and adapt to the demands of the software.

Question 7: How Should the Software's Output Look?

Car buyers have an idea of what they want the new car to look like – for example, sleek and shiny, or tough and functional. Similarly, business continuity applications produce output differently. Some software create plans as Word documents, but most produce PDF documents, making them more difficult for plan owners to add comments or changes. Many software packages offer custom reports, although some are easier to create than others. Some reports are as easy as drag-and-drop; others require the user to master programs like Crystal Reports. Some software does not allow the user to create custom reports at all; instead, the user must ask the software provider to create the reports for them.

Warning: if the organization depends on call trees for employee notification, make sure the new software will support them – many vendors consider call trees outdated and no longer offer this feature.

Question 8: What Training Will Users Need?

Moving a business continuity program from a word processing document and a spreadsheet to a fully integrated software program can be like going from an automatic to a manual transmission: all of the sudden, there are multiple moving parts and the driver needs to learn coordination to avoid stalling. New software can present a steep learning curve. Not only is there the challenge of learning to operate the programs, there is also the challenge of teaching plan owners to assess and prioritize their business functions. If individual plan owners are responsible for conducting their own BIAs, a significant amount of training may be required. Software owners can either conduct the training themselves, or pay the vendors to do so.

Question 9: How Much Technological Support Will Be Required?

While a car buyer determines the value in purchasing a roadside assistance plan, the business continuity professional determines how much technological support users of the business continuity software will require, as well as when and how the support will be provided. Business continuity software varies in terms of technological support, so several needs must be assessed: time (24/7 support or only during business hours); availability (business's hours compared to vendor's hours); accessibility (live support or online portal); and cost.

Question 10: Where Is the Best Place to Start?

Just like car dealerships, there are a multitude of software vendors. The findings of an independent research organization, such as the Gartner Magic Quadrant for Business Continuity Management Program Solutions are a good place to start. Recommendations

from peers and professional organizations are also valuable. Vendors will gladly demonstrate their software via webinar; and some even offer a free trial period.
As with any purchase, thorough research and comparison are key. Keep in mind, though, that the organization may be using this software for years to come. It is important to choose a package that is best for the business right now as well as flexible enough to grow along with it.

Erin Valentine, *CBCP, MBCI, is the business continuity/disaster recovery coordinator at General Dynamics Information Technology (GDIT). She spent the first decade of her career as an exercise and training administrator at the Maryland Emergency Management Agency (MEMA). Prior to GDIT, she supported the Social Security Administration's Office of Security and Emergency Preparedness as a disaster preparedness specialist. She holds a bachelor's degree from Towson University and is certified by FEMA as a Master Exercise Practitioner and Professional Continuity Practitioner. She is a Certified Business Continuity Professional (CBCP) and a Member of the Business Continuity Institute (MBCI). She currently serves as the program director of the Central Maryland Chapter of the Association of Continuity Professionals.*