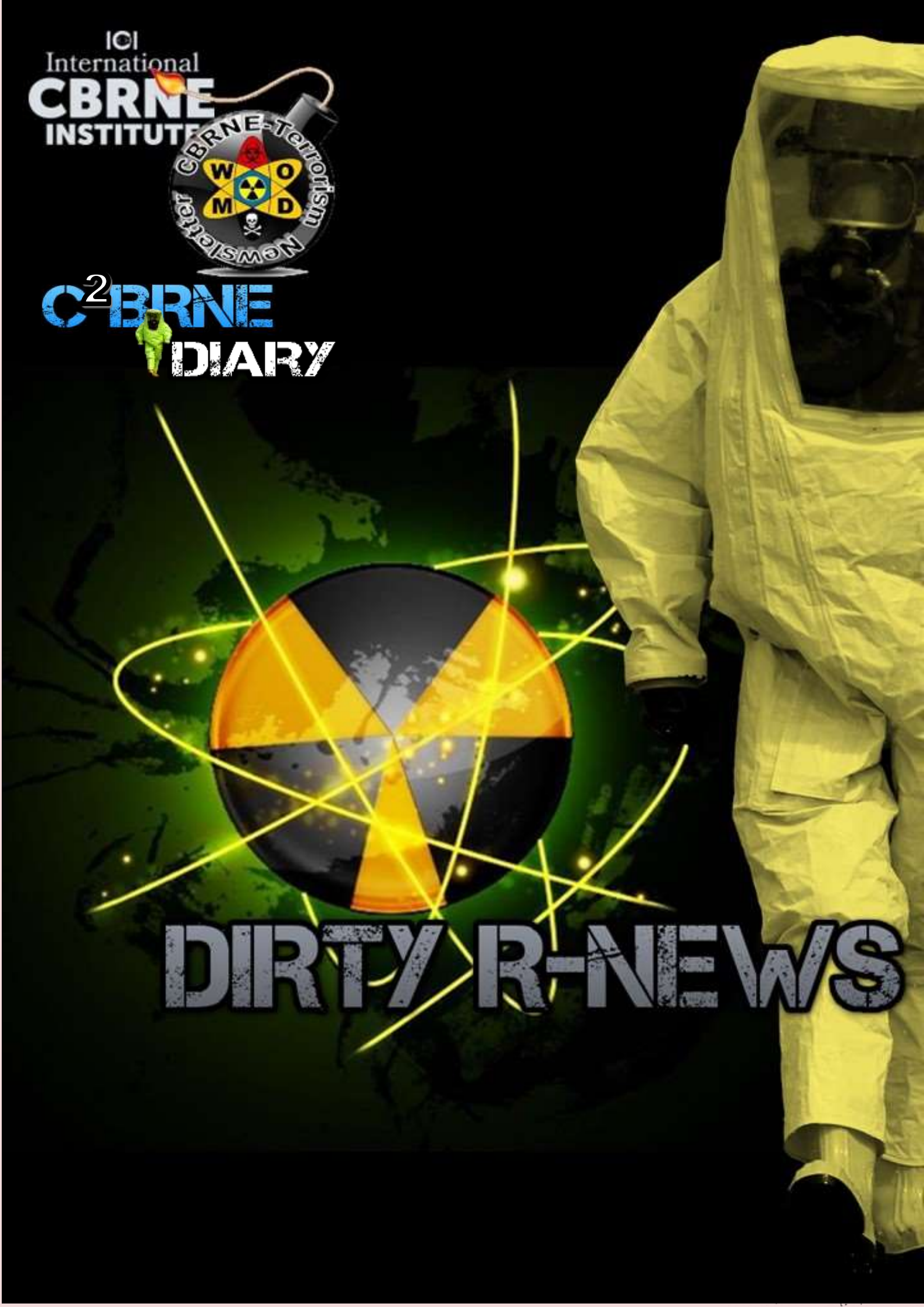
2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

December 2018

www.cbrne-terrorism-newsletter.com


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
DIRTY R-NEWS

Saudi Progress in Nuclear Research

Source: http://www.inss.org.il/publication/saudi-progress-nuclear-research/

Nov 29 – In November 2018, Saudi Crown Prince Mohammad bin Salman laid the foundation stone for seven scientific/technological projects in the kingdom, including a nuclear research reactor. Saudi Arabia's interest in nuclear matters is nothing new, nor is the concern that in certain conditions, the kingdom is liable to move toward nuclear weapons. Indeed, even though it does not yet have any capabilities to speak of, anxiety about a Saudi nuclear project was validated last March when for the first time bin Salman said publicly and explicitly that if Iran acquires a military nuclear option, the kingdom will acquire the same capability without delay.

While construction of a nuclear research reactor is not a prerequisite for construction of large scale nuclear plants, as has been demonstrated by the United Arab Emirates, from a certain perspective, it is a wise step for a country lacking human and technological infrastructure. Such a measure is liable to prove alarming, however, if it becomes clear that its goal is not merely to train staff for the nuclear reactors, but also to prepare the infrastructure for possible production of plutonium from the irradiated nuclear fuel in the research reactor. This is certainly possible: The Iraqi reactor was originally presented as a nuclear research reactor, and other reactors can, under certain conditions, be used for this plutonium production. The US is likely to demand that the reactor is powered with fuel enriched up to 20 percent, which will prevent the fuel from being used to separate plutonium and make it difficult (although not impossible) to irradiate natural uranium in order to produce plutonium. The P-5+1 countries are unlikely to knowingly supply Riyadh with a reactor fueled by natural uranium from which it is easier to produce plutonium for military purposes. According to one source, the reactor's power will be very low – approximately 100 kilowatts – a level that will allow study and research, but not production of a significant quantity of plutonium.

Negotiations between the United States and Saudi Arabia on nuclear cooperation were renewed over the past year. These talks had reached an impasse under the Obama administration, due to the kingdom's refusal to forego its "right" to enrich uranium that could be used as nuclear fuel in the nuclear reactors. Uranium enrichment can certainly be used for the legitimate purpose of providing fuel for nuclear power plants, but can also be used as a source of fissile material for nuclear weapons, as in Pakistan and Iran. The Trump administration is considering a new approach from that of the Obama administration: to allow limited enrichment in Saudi Arabia. US Secretary of Energy Rick Perry is to a large extent the main proponent of the new approach, but it has encountered some resistance from both Republican and Democratic legislators, who have expressed concern about Saudi Arabia's nuclear intentions. In addition, several legislators are now seeking suspension of the secret negotiations with Saudi Arabia following the murder of Jamal Khashoggi and the Saudi intervention in Yemen. Congressional pressure on the administration is expected to increase, given that many legislators are urging a reappraisal of relations with Saudi Arabia, which will further complicate the nuclear negotiations.

Saudi Arabia does not want to be left behind Iran. Several years ago, it announced an ambitious - some say overambitious - nuclear program involving construction of 16 nuclear reactors. The completion date for the reactors has been consistently postponed, and is now 2040. For construction of the first two reactors, Saudi Arabia has received bids from companies in the US, China, Russia, France, and South Korea, and announced that it will soon select the companies for construction of the reactors, which are scheduled to become active toward the end of the coming decade. The reactors will probably be located on the Gulf coast close to the border with the United Arab Emirates. South Korean Electric Power Corporation (KEPCO), which is admired by Riyadh for its success in building reactors in the UAE, likely has the best chances of winning the tender to build the Saudi reactors.

Saudi Arabia has serious reasons to seek civilian nuclear energy in order to meet its growing energy requirements, reduce its dependence on oil, and release more oil for export, but it is fairly clear that the main motive now for its nuclear development is security interests. As Riyadh sees it, the nuclear agreement with Iran increased Tehran's aggression and did not halt its long term nuclear ambitions. Another motive is prestige. Just as Saudi Arabia does not want to trail behind Iran, it is not happy about the UAE's relatively rapid progress in this area. Competition for prestige has always been an important feature of relations between the Arab Gulf states, and has motivated much of the infrastructure activity in these countries, including in military

procurement. It is thus possible that the implicit threat in starting the project was designed to push the US and the international community into stepping up their pressure on Iran in order to prevent it from producing nuclear weapons. The declaration about construction of the reactor at the present time, however, also has an internal aspect related to bin Salman's status and his desire to bolster it, especially in view of the Khashoggi affair aftermath.

The UAE, which completed construction of the first civilian nuclear reactor on its territory in April, reached an agreement with the United States in 2009 to refrain from enriching uranium in exchange for essential international nuclear aid. This barrier has been labeled a "gold standard" for future nuclear agreements, but Saudi Arabia is unwilling to accept it; from Saudi Arabia's perspective, it should be allowed to do whatever is permissible for Iran. As a rule, Saudi Arabia wants to position itself so that it has as many (nuclear) options as possible. More than any other regional actor, Saudi Arabia has a strategic motive and the economic capabilities to accomplish this. A sustainable nuclear program will help Saudi Arabia keep step not only with Iran, but also with the UAE, Turkey, and Egypt, which are only at the beginning but have made more nuclear progress than Saudi Arabia. As for inspection of the Saudi nuclear program, Riyadh has signed the Nuclear Non-Proliferation Treaty and since 2009, an inspection agreement with the International Atomic Energy Agency (IAEA), but this is a minimal agreement only. Saudi Arabia has not signed the Additional Protocol that greatly expands the authority of IAEA inspectors. The current agreement (Small Quantities Protocol) obligates Saudi Arabia to very little, and in any case requires a revision when construction of the nuclear research reactor begins.

Development of the Saudi civilian nuclear program is a long term goal, given the lack of sufficient technological knowledge and appropriate facilities in the kingdom. The JCPOA, if it remains in effect, gives Saudi Arabia more or less a decade in which to develop a "civilian" nuclear effort without withdrawing from the NPT. In the short term, under the scenario of an Iranian breakout to nuclear weapons Saudi Arabia may already have some kind of response available from Pakistan. Despite some tension in recent years, Pakistan still constitutes strategic depth for Saudi Arabia, and is liable to provide it with assistance in developing nuclear weapons.

Israel faces a dilemma. On the one hand, acceptance of enrichment capability in Saudi Arabia in the framework of negotiations between Riyadh and the US is liable to cause a regional avalanche if countries like Jordan, Egypt, and Turkey also demand this "right." As it has already hinted, the UAE is likewise liable to regard itself as not obligated by the agreement with it. In any case, if Saudi Arabia decides to seek military nuclear capability in the future, the planned civilian nuclear program is liable to provide it with a short cut to military nuclear capability. On the other hand, Israel has an interest in the United States, which is more committed than many other countries to non-proliferation standards, winning access to the Saudi nuclear market.

It is therefore likely that the US will exert pressure on Saudi Arabia to grant the license to South Korea for building Westinghouse-made nuclear power plants. Washington will thereby be more aware of what occurs in this area, and will gain additional leverage over Riyadh. In this way, Saudi Arabia's ability and motivation to covertly develop nuclear capabilities can also be reduced. The question arises regarding the manufacturer of the research reactor to be built in Riyadh. There are many possible sources for this, including the US and many other countries, such as France, Russia, China, Argentina, and possibly also Pakistan. To a considerable extent, the supplier of the reactor will determine its purpose, because it is fairly clear that the supplier will have extensive influence on both the future purpose and the supply of the nuclear reactors.

As Riyadh will not be able to complete a sustainable nuclear project without massive outside assistance, the US and Saudi Arabia will have to reach a compromise. One possibility is a partnership (financial, not technical) in an American facility that will enrich uranium from Saudi raw materials (the Shah of Iran was a partner in a French enrichment plant). A less likely possibility is that the US will build and operate an enrichment facility on Saudi territory. President Trump wants to preserve his relations with Riyadh, and is concerned about the interests of the American nuclear industry, which is experiencing difficulties. Although it has major common interests with Riyadh and, according to reports, benefits from cooperation with it, Israel should take action in Washington to prevent Saudi Arabia from attaining unlimited enrichment capability, and to try to make sure that the nuclear transaction with it, should one materialize, will be as close as possible to the nuclear "gold standard."

Ephraim Asculai *worked at the Israel Atomic Energy Commission (IAEC) for over 40 years, mainly on issues of nuclear and environmental safety. In 1986, he went to work at the IAEA in Vienna on issues of radiation protection of the public. During 1990-1991 he was the Scientific Secretary of the International Chernobyl Project. In 1992, Dr. Asculai returned to Israel and became heavily involved in the deliberations leading to the conclusion of the Comprehensive Test-Ban Treaty (CTBT). In his final period at the IAEC he served as the Director of External Relations. During his sabbatical at the Institute for Science and International Security (ISIS) in Washington, D.C. he authored Verification Revisited: The Nuclear Case, published by the ISIS Press. Dr. Asculai retired from the civil service in 2001. In 2002 he joined the Jaffee Center for Strategic Studies (now incorporated into the INSS). He has since published several papers dealing with WMD non-proliferation in general, and Middle East issues in particular, including the monograph Rethinking the Nuclear Non-Proliferation Regime in 2004. He received his Ph.D. in Atmospheric Sciences from the Hebrew University in Jerusalem.*

Dr. Yoel Guzansky *is a Senior Researcher at the Institute for National Security Studies, Tel Aviv University. Dr. Guzansky is a visiting Fellow at Stanford University's Hoover Institution, Israel Institute Postdoctoral Fellow, and a Fulbright Scholar. Before he joined INSS, he served at the National Security Council in the Prime Minister's Office, coordinating the work on Iran, under four National Security Advisers and three Prime Ministers. He is the author of The Arab Gulf States and Reform in the Middle East (2015); Between Resilience and Revolution: The Stability of the Gulf Monarchies (INSS: Hebrew, 2016) and co-author (with Kobi Michael) of The Arab World on the Road to State Failure (INSS: Hebrew, 2016).*

EDITOR'S COMMENT: I was always wonder why some countries are entitled to have nuclear weapons and others not. Who makes the decision that country A is a good country to have nuclear power while country B is a bad country? Who decides that country C is politically correct to have nuclear capabilities while this is not an issue for country D? What if one day KSA announces that they have 10 nuclear weapons or 50 of them? Pakistan did that. Israel did that. And the nuclear private group did nothing. Turkey announced the construction of 3 nuclear plants even when its seismic activity is well known. Did anybody did anything or even protest against it? Of course not! It would be better to use nuvlear power for peaceful purposes and not as a political card and a threat. Hypocricy is equally dangerous to nuclear weapons.

Cevidra® Calixarene 50ml

Source: http://www.cevidranuclear.com/en/produit

Cevidra® Calixarene cleansing & decontaminating cream in 50 mL tube.
Commercialised under license from the IRSN Patent FR0858703

Composition
Ingredient: **Calixarène carboxylique** (0,75 %)
Excipients: Paraffin oil, Water, Emulsifiers, Surfactants et Preservatives

Indications and limits on use
Cevidra® Calixarene is a **medical device** intended to treat external contamination with radionuclides (uranium, plutonium, americium, thorium, Cobalt, Caesium and Strontium). Its use on wet skin and/or hair under medical supervision is part of a decontamination protocol and must be followed by copious rinsing.

To be used on healthy skin.
The studies carried out have confirmed the performance of **Cevidra® Calixarene** on undamaged and excoriated skin. In studies on Frantz diffusion cells carried out by the IRSN, no diffusion of carboxylic calixarene has been observed across excoriated skin.
There is no data available on the performance of **Cevidra® Calixarene** in case of injury. The characteristics of the injury (extent and depth) could influence the diffusion of the calixarene: it is recommended to avoid use on injured skin.

Avoid direct contact with eyes.

To be used with care on people with a known allergy to one of the components.

For external use, do not swallow.

Instructions for use
A tube of **Cevidra® Calixarene** is intended for a single use to decontaminate the hair, scalp and body or to decontaminate a contaminated area of the body (hands, face, an arm, etc.) during the emergency decontamination procedure put in place on the site.
The areas to be decontaminated are carefully washed by gentle friction using decontaminating cream.
The cream acts immediately by its specific chelating effect for actinides and by its cleansing effect for all radionuclides that may be present in a more or less soluble form.
So as to optimise the contact between the **Cevidra® Calixarene** cream and the body area to be contaminated, it is preferable to wet the skin and/or the hair in advance.
After using the decontaminating cream, the treated area must be rinsed with water starting from the top of the treated area and finishing with the lowest part.
It is not necessary to leave the product in prolonged contact with the skin and/or the hair to increase the efficacy of decontamination. For increased decontamination of a heavily exposed area, it is recommended to repeat the wash/rinse cycle several times over the same area.
If one dose is not sufficient to wash the whole body surface to be decontaminated, several doses may be used.

Management of serious incidents, undesirable effects and quality problems
Any anomaly noted before, during or after the use of **Cevidra® Calixarene** must be notified to the manufacturer of the medical device. Cevidra will investigate this anomaly as part of its materiovigilance procedure.

Laboratoire CEVIDRA
45, boulevard Marcel Pagnol – 06130 Grasse
Tel. : +33 (0)4 93 70 58 31 ; Fax : +33 (0)4 93 77 24 62 ; contact@cevidra.com

Any serious incident linked to the use of the medical device must be notified to the manufacturer or to the competent authority in the member state.

Dissuading Adversaries and Their RN Pathways: Integrating Deterrence Theory and Analytics in the GNDA

Source:https://start.umd.edu/pubs/START_DissuadingAdversariesRNPathways_ResearchBrief_Nov2018.pdf

The Dissuading Adversaries and their RN Pathways (DARNP) project expands upon several extant analytical and computational models and data collections of potential radiological or nuclear (RN) adversary behaviors that UWT-START researchers have previously developed, many for Department of Homeland Security Domestic Nuclear Detection Office (DNDO). The project uses cutting-edge non-state actor deterrence theory and game-theoretical approaches to combine these previous models, which themselves integrate deep qualitative and contextual empirical data on violent non-state actors with theoretical insights drawn from terrorism studies, organizational psychology, political science, criminology, sociology, and engineering.

Applications

UWT-START has used the DARNP model to estimate possible adversary responses to RN detection countermeasures. One funder, the Defense Advanced Research Projects Agency (DARPA), sought to mobilize a network of portable radiation detectors (PRD) as a deterrent and preventative measure against radiological or nuclear attacks perpetrated by non-state actors against major U.S. cities. In furtherance of

Policy Scenario	Expected Casualties (Log)	Expected Costs	Cost Avoidance/Policy Cost Factor
Highway Detectors	**0.553210922**	$8,411,498,584	336
Maritime Interdiction Enhancement	0.632241054	$9,613,141,239	**1489**
Leadership Removal	1.164802875	$12,505,763,774	472
Tier 1 Cities PRD Network	1.023664706	**$3,547,342,799**	120
Universal PRDs	1.183380061	$16,800,528,791	157

*Note: **Bolded text** indicates the best outcome in each column.*

that effort, the START-UWT team assessed several configurations of PRD networks and urban coverage to estimate preferable deployment strategies. Moreover, the model has been used to analyze a range of other potential defensive strategies: increased border security, increased maritime security, targeted strikes against organization leadership, highway-located fixed radiation detectors, and outfitting highway patrol officers with PRDs.

▶▶ Read the rest of this article at source's URL.

Responders provide technical expertise in case of nuclear weapons accidents

Source: http://www.homelandsecuritynewswire.com/dr20181130-responders-provide-technical-expertise-in-case-of-nuclear-weapons-accidents

Nov 30 – Decades ago, technical experts from the national labs responded in an ad hoc manner to accidents involving nuclear weapons, called "broken arrows."

Thirty-two such accidents have occurred since the 1950s, so the Accident Response Group was created about five decades ago to provide technical expertise in assessing and safely resolving nuclear weapons accidents.

"With the resources the Department of Energy can bring in the form of ARG, rest assured there will be a safe weapon recovery," said Harry Cincotta, ARG project lead at Sandia National Laboratories. "If ARG does have to respond, we are ready, and we're bringing the best scientific minds in nuclear weapons on the planet with us."

Although U.S. nuclear weapons are managed with great care in maintenance and transportation, ARG's manager Bill Beenau said ARG is prepared to respond in the event of any extraordinary circumstance.

ARG leadership recently celebrated the realignment of the ARG program into the Military Liaison Department. The realignment will build off of the existing relationships the Military Liaison Department has with the Department of Defense, and enhance ARG's existing technical relationships with DOD maintenance and explosive ordnance disposal groups. Ultimately, this will improve awareness of the technical expertise ARG brings to the table, should an accident happen.

"Our weapons are the safest in the world," said Dan Summers, a longtime ARG volunteer who has focused on nuclear weapons surety for decades. "They have tremendous safety features, and we consider a variety of accident conditions when designing and testing them,

including fire, crushing damage, even weather events."

ARG safely assesses, recovers nuclear weapons damaged in accidents

Sandia Lab says that ARG brings together diverse experts in nuclear weapons and health and safety from Sandia, Lawrence Livermore and Los Alamos national laboratories as well as the Remote Sensing Laboratory and Pantex Plant. Each facility has its own area of expertise. The physics labs — Los Alamos and Lawrence Livermore — focus on the nuclear package. As the nuclear engineering lab, Sandia focuses on the whole weapon, Beenau said.

ARG is a group of volunteer emergency responders, like a volunteer fire department made up of experts at the top of their field. Volunteers are on call on a rotating basis for the initial phase of response. If necessary for a safe recovery, ARG can expand to a team of about 50 experts for round-the-clock field operations.

ARG is one of many National Nuclear Security Administration nuclear and radiological emergency response groups. Sandia is also heavily involved in the Radiological Assistance Program, which shares a lot of experts and expertise with ARG.

Experts from across the nuclear enterprise need to be nominated by current members of ARG or weapons systems program leadership before they can volunteer. "We want the folks who handle the routine technical challenges of the nuclear weapon systems to be a part of ARG," said Cincotta.

Ryan Kristensen was nominated for ARG about four years ago. A systems engineer, he started working with some ARG volunteers on a specific project. Through them he learned about ARG's critical mission. Beenau said, "Ryan Kristensen is a great example of what ARG is becoming. He is a highly skilled engineer and is bringing a new, fresh perspective to ARG."

For Kristensen, the most fulfilling part of volunteering for ARG is working as a team in the field during exercises. "It's great when you can come together and achieve a difficult task. It's not often you can work with a team like that and know you've made a difference," he said.

Emergency responders provide technical expertise to Explosive Ordnance Disposal

ARG regularly participates in emergency exercises designed to test everything from equipment and deployment times to collaboration with other agencies, such as the DOD and FBI. These exercises involve very realistic models but no actual nuclear weapons. "During an exercise or real-world event, we're not Sandia, Los Alamos or Lawrence Livermore; we're ARG," said Kristensen. The boundaries between DOD and DOE responders relax as well, Kristensen said. "Explosive Ordnance Disposal are the hands-on guys, and we ensure what they do is safe for them and the weapon."

These exercises test the ARG responders' limits too. During an exercise in 2005, Summers had to splice a damaged fiber optic cable in winds over 75 mph, while wearing a full protective suit, in order to restore ARG's secure communications system. "If you don't practice for real, you're never going to be ready," said Summers.

Kristensen thinks the post-exercise debrief and celebration is also an important part of building bonds between responders from across the nuclear enterprise and agencies for the next exercise or real-world event.

"Home Team" provides expert knowledge and support for field responders

In addition to the field responders, ARG also provides technical support in the form of the Home Team, a collaborative network with nodes across the nuclear enterprise and at NNSA headquarters. They serve as a conduit to the enterprise's technical experts, which can be tailored to the exact weapon system and the precise damage caused by the accident.

"The ARG responders in the field have secure, reliable, dedicated, high-speed communications with the Home Team and the precise experts needed," said Brenda Townsend, a member of Sandia's Home Team for fifteen years. This communication allows ARG to deploy far fewer people to the site of an accident, which is cost effective.

In addition to the weapons systems experts, the Home Team includes a team responsible for double-checking the weapon recovery plans, a team to ensure the communication networks work effectively and a team that handles the logistics of getting the ARG responders to the site of the accident and making sure they have everything they need when they arrive, such as hotel rooms.

Townsend primarily serves as a communications specialist, but she's also responsible for staffing the communications and logistics

positions. She said, "I really believe in ARG's mission. It gives me satisfaction to provide the substructure to allow ARG to do its job efficiently and effectively."

Sandia's Home Team is the lead Home Team and can coordinate requests for information from the field or headquarters to the other Home Teams with the right expertise. The Home Team uses secure phone lines, video conferencing and even instant messaging to interface with each other, responders in the field and the DOD. This secure communication is aided by a portable integrated video system, or PIVS. This secure fiber optic-based communications system can carry video and audio from the accident area to the Home Teams. The volunteers responsible for setting up the system and hauling the 85-pound reels of fiber optic cables are colorfully called PIVS mules. Cincotta was a PIVS mule during his first exercise, almost 25 years ago.

"Once I got out to the exercise, the importance of it got ahold of me. The important mission either resonates with you as a scientist or engineer or it doesn't. And it certainly resonated with me," said Cincotta. "Every accident situation is unique so every response is somewhat unique, so it's intellectually stimulating too."

Military warns EMP attack could wipe out America, 'democracy, world order'

By Paul Bedard

Source: https://www.washingtonexaminer.com/washington-secrets/military-warns-emp-attack-could-wipe-out-america-democracy-world-order

Nov 30 – In an extraordinary and sobering report meant to educate the nation on a growing threat, a new military study warns that an electromagnetic pulse weapon attack such as those developed by North Korea, Russia, and Iran could essentially challenge the United States and displace millions.

"Based on the totality of available data," said the report from the Air Force's Air University and provided to Secrets, "an electromagnetic spectrum attack may be a threat to the United States, democracy, and the world order."

The report, titled, "Electromagnetic Defense Task Force," and the product of a mostly classified summit of officials from 40 agencies just outside of Washington earlier this year, is a forceful call for a new focus on preparing for either an enemy EMP attack or a natural hit such as a solar storm.

While it is focused on the devastating impact an EMP hit would have on the military, it appears to support a congressional warning that up to 90 percent of the population on the East Coast would die in a year of an attack that would dismantle or interfere with electricity, transportation, food processing, and healthcare.

Consider just some of the warnings in the report from the United States Air Force Air University and the Curtis E. LeMay Center for Doctrine Development and Education. Citing figures from the Union of Concerned Scientists, the report:

- 99 nuclear reactors would likely melt down without electricity to cool them.
- 4.1 million would be displaced from areas around the nuclear plants as the radioactive cloud spread.

The report highlighted electronic systems on an Airbus A-380. (Screenshot/LeMay Center for Doctrine)

- Military and commercial jets, such as those built by Airbus, could be degraded. "Alarmingly, aircraft designed to carry large numbers of people and sizable cargo are allowed to operate without certainty about their level of resilience."
- Bases would be cut off, making defense and counter-attacks impossible.
- Civil unrest would start in "hours."
- Power and GPS could go dark. "An EMP would cause instantaneous and simultaneous loss of many technologies reliant on electrical power and computer circuit boards, such as cell phones and GPS devices."
- "Failures may include long-term loss of electrical power (due to loss of emergency generators), sewage, fresh water, banking, landlines, cellular service, vehicles."
- 18 months or more are required to replace key elements of the electric grid that would be damaged or knocked out.

Figuring out just which country launched an attack would be difficult since certain weapons could be delivered in a satellite.

Figure 1.7. Airbus A-380 electronic systems. (Source: FAA.)

It also noted the development of the 5G mobile network and how it will run communications and why it must be protected, especially since China is the biggest investor in its development.

"Because control of 5G is roughly equivalent to control of the Internet, open 5G is critical to freedom and free-market economics. Meanwhile, access to the 5G-millimeter wave bandwidth will be critical to operations in all war-fighting domains, in particular, space command & control," said the white paper.

Lt. Gen. Steven Kwast, the commander of Air Education and Training Command, said, "As electromagnetic technologies fuse in new and often dangerous ways, it's critical that the military and industry make honest evaluations of present and future conflict states to ensure we're proactive rather than reactive."

He also advised for predicting how U.S. foes will try to outsmart any fixes to the electric grid and other targets of an EMP attack.

"French actions before WWII demonstrate that even bold action, such as building the Maginot Line, can be rapidly overcome through imagination. The imagination that defeated the Maginot Line was the German Blitzkrieg which unexpectedly exploited the only gap in the wall. Groundbreaking research like this can help the wider defense community understand not only how take bold action, but how to take the right bold action to prevent catastrophic outcomes," said the general.

The report said that the government should focus on the issue and declare it a critical issue. What's more, it called for a central effort to push for EMP prevention and reaction should an attack come.

The report, written by experts Air Force Maj. David Stuckenberg, former CIA Director James Woolsey, and Col. Douglas DeMaio, also called for a national and congressional publicity campaign to alert the nation and governmental leaders to the threat.

"The potenti
al for an adversary to inflict damage on states through EMS attack has grown significantly," said the 69-page report, which warned, "An EMP attack affects all devices with solid-state electronics and could render inoperative the main grid and backup power systems, such as on-site generators."

It highlighted the lack of a reaction plan or major focus on an EMP attack, even if just from a solar flare. "In some areas, there is a complete absence of strategy," said the report. It added, "EMP is a tragedy of the commons as 'no one's job jar.'"

Iran planned to build five 10-Kt bombs by 2003: Nuclear experts

Source: http://www.homelandsecuritynewswire.com/iran-planned-build-five-10-kt-bombs-2003-nuclear-experts

Nov 23 – The Institute for Science and International Security published a paper Tuesday containing new details about Iran's nuclear weapons program and demanding that the International Atomic Energy Agency ensure that Iran's nuclear weapons program is "ended in an irretrievable permanent manner."

The latest report — authored by David Albright, a former weapons inspector and president of the institute; Olli Heinonen, former deputy director general of the IAEA; and Andrea Stricker, a senior policy analyst at the institute — follows up on previous reports based on information contained in the Iranian nuclear archive recovered by Israel earlier this year.

According to the latest report, Iranian documents show that Iran had specific plans to build five 10-kiloton nuclear devices by 2003. The plans from the archive show that Iran's planning for these weapons was very detailed, including expected costs and a timetable.

However, Iran did not develop the weapons by 2003 and reoriented its program. Iran "had put in place the infrastructure for a comprehensive nuclear weapons program capable of one day building far more, if required," the paper reported.

Contrary to the assertions of the IAEA in late 2015, prior to the implementation of the nuclear deal, Albright, Heinonen, and Stricker write that Iran "had achieved much more than feasibility and scientific studies relating to nuclear weapons." In fact, they continued, "Iran preserved an extensive amount of this nuclear weapons-related equipment, material, software, and other information in an archive and warehouse, the former the contents of which were partially seized by Israel, and the latter which Israel later identified."

Though Israel had provided the files it recovered from the archive to the IAEA, the agency has not acted on the new information. In fact, the paper pointed out that Israel publicly revealed its discovery of the Iranian nuclear archive and warehouse only "after briefing the IAEA and it failed to act."

"It is not only the Secretariat, but the IAEA Board of Governors, which has not lived up to its task," Albright, Heinonen, and Stricker write in their conclusion. "They have created a double nonproliferation standard which, unless remedied, will decrease the chance of ensuring Iran does not build nuclear weapons and will serve as a playbook for future proliferators."

In an op-ed published last month in *The Hill*, Josh Block, the President and CEO of The Israel Project, pointed out that it was becoming clearer that the IAEA did not have a full grasp of Iran's nuclear weapons program and implications of those limits.

"The gaps in the IAEA's knowledge — of Iran's past nuclear work, of its military sites, of items mentioned in Section T of the nuclear deal, and of the nuclear sites discovered by Israeli intelligence — raise questions about the full extent of Iran's nuclear program," Block argued.

Weapons experts: Satellite images confirm Netanyahu's claims about Iran's nuclear warehouse

Source: http://www.homelandsecuritynewswire.com/dr20181204-weapons-experts-satellite-images-confirm-netanyahu-s-claims-about-iran-s-nuclear-warehouse

Dec 04 – Satellite images obtained over the summer confirm charges made by Israeli Prime Minister Benjamin Netanyahu in September that Iran had a secret nuclear warehouse in Tehran, a team of weapons inspectors wrote in a paper published Thursday.

The paper — authored by David Albright, Olli Heinonen, Frank Pabian, and Andrea Stricker — asserted that the satellite pictures show the "steady progression of containers disappearing from the site from July into September," likely removing "equipment and nuclear material" from the warehouse. Albright is founder and president of the Institute for Science and International Security as well as a former United Nations weapons inspector; Heinonen is a senior advisor

to the Foundation for Defense of Democracies and a former Deputy Director General of the International Atomic Energy Agency; Pabian is a former inspector for the IAEA, and Stricker is a senior policy analyst at the Institute.

In his 27 September speech to the United Nations General Assembly, Netanyahu charged that in addition to a nuclear archive — that he had revealed in April — Iran maintained a warehouse of equipment used for its nuclear weapons program.

The paper described images showing some 15 shipping containers by the nuclear warehouse from December 2017 until the middle of this year following the revelation of the nuclear archive.

Despite Iranian denials and claims that the facility identified by Netanyahu was really a carpet cleaner, "photographs and photographic analysis by Israel show that the carpet cleaning site is directly across the street from the actual atomic warehouse," the paper concluded.

Though Netanyahu had shared the intelligence with the IAEA about the containers leaving the area of the warehouse, the paper noted that "the IAEA did not act on this." By failing to follow up, "the IAEA may have lost a remarkable opportunity to have asked to go to the site while shipping containers remained there, and irretrievably lost its capability to find the equipment and confirm its true purpose."

The authors assert that by failing to act, the IAEA lost a chance to ensure implementation of Section T of the nuclear with Iran, which is to ensure that Iran is not pursuing any research that could help it develop nuclear weapons. "The United States has a responsibility," they wrote, "as a member state of the IAEA, to ensure that such inaction does not continue."

They also pointed out that the IAEA's lack of action undermines assurances that "the JCPOA would make it easier to mount inspections when concrete evidence would arise." Instead, it "validates" concerns of the JCPOA's critics, who questioned whether it would enhance enforcement of Iran's obligations.

Getting hands-on with nuclear emergency response training

By Steven Pike

Source: https://www.argonelectronics.com/blog/getting-hands-on-with-nuclear-emergency-response-training

Dec 05 – Large-scale releases of ionizing radiation are thankfully a rare occurrence. But with just over sixty commercially run nuclear power plants currently in service in the US, and fifteen operational nuclear reactors located across seven plants in the UK, the risk of an accidental release, however minor, is one that must be meticulously trained for.

The monitoring equipment used in the management of radiation incidents is relatively simple to use. But what is crucial is to be able to create realistic nuclear emergency response training scenarios that truly test the capability of every trainee.

In this blog post we revisit a day-long USAF radiological survey exercise that incorporated the use of PlumeSIM, along with a variety of Argon's radiation hazard simulators, to create a realistic and engaging training experience.

Exercise objectives
A core goal for USAF the exercise controllers was to be able to enhance the overall quality of the training scenario and in particular to improve upon the use of the standard inject training methods.
In previous exercises this might have comprised something as simple as a student being shown a piece of card to replicate a reading - or in a slightly more high-tech version of the same exercise, an electronic notepad might have been provided with a set of hypothetical instrument readings.
The use of a simulation control system using Argon's PlumeSIM software however, was to add a whole new level of realism to these traditional training approaches.

Briefing the team
The exercise commenced with the response team being briefed on an incident of unknown severity taking place at a fictitious nuclear power station approximately twelve miles away and just upwind of the team's present location.
The team's challenge? To decide what action would be required, to determine what equipment they would need in order to assess the potential risk, and to brief the local authority with appropriate recommendations.

The exercise requirements
The requirement of the exercise simulation requirement was as follows:

- The replication of a single plume comprising the radionuclides 137C, 131I and 90SR
- That the plume reach the training area exactly forty-minutes after initiation of the exercise
- That deposition be across the entire training area

Equipment and instrumentation
The following simulation instruments were required in order to accurately assess the scene:

- A radiation survey simulator
- An EPD-Mk2 Dosimeter simulator
- A SAM 940 spectrometer simulator
- An Alpha simulation for RADECO air sample
- Filter contamination simulation

The simulation control system comprised a lap-top with the Argon Rad PlumeSIM software and live field base station, which provided effective real-time exercise control throughout the exercise area.
A local map was downloaded and calibrated using a feature within PlumeSIM to create a .jpg image of the local terrain. This map would prove invaluable both in assisting in planning the simulated exercise and also in tracking the students throughout the scenario.
Members of each survey team were equipped with a survey meter, personal dosimeters, and a spectrometer. The remainder of the students were provided with hand-held portable radios for the purposes of communications, logistics, data collation and generation of the hazard prediction plots.
The trainee's first decision was to deploy a Radeco air sampling station. While the assembly of the sampler proved to be relatively easy, there was more than one view as to what airflow setting should be used during the warm-up period, and also the importance of keeping the exhaust of the generator used to power the Radeco a reasonable distance from the air sample intake. There was also some debate between students as to what the ideal airflow rate should be after the initial warm-up phase.
The exercise coordinator then announced that a radioactive release had been confirmed and that the estimated time of arrival of the release to the current location was forty-minutes. At this point the simulated plume release was initiated, with the system configured to provide plume cover at the desired time over the exercise area.

Adaptability
A feature of PlumeSIM is the ability to fast forward or pause the exercise as needed. This enabled the exercise controller to manage the staging of the exercise to suit the specific progress and status of the participants.
Each survey team member wore a portable player device. The exercise control system was then automatically transferred to the player unit which broadcast the simulated radionuclide activity based upon the student's geographic location.

The students' movements throughout the exercise were monitored in real time and recorded for after-action review later back in the classroom.
A simulation source had also been installed on the inside of the filter paper holder, which meant that when the simulation Alpha probe was offered up to the filter paper a reading noticeable above background could be obtained. The reading was reported to the control cell, together with the flow rate and the duration of the sample period, which enabled the airborne activity level to be determined.
A survey of the local area was then requested. A survey team of four comprised two team members each carrying generic survey simulators, a third team member with a SAM940 spectrometer simulator, and the fourth team member with a radio communications device. Two of the team were also wearing simulation dosimeters based upon the EPD-Mk2.
The areas in which the survey team would receive simulated radiation readings, and the level of these readings, had been pre-determined by the exercise controller so that initial readings would be obtained typically 150 meters away from the command station.
The survey team spread with a distance of ten meters between each of the three instrument-carrying members, with the communications operative following a little behind the line.
As the survey team approached the "hot zone", the readings started to climb above background level.

Lessons learned
From an observer point of view, this was the point where the exercise started to get really interesting. It was a very sunny day and the combination of the team members' bulky PPE and the bright sunlight meant that the smaller displays were a lot harder to read.
The respirators also weren't fitted with voice modules, which meant that even simple verbal communication was a challenge, and even more so when a message was being relayed across a hand-held portable radio.
Another interesting observation was confusion over units of measurement. As it happened, some instruments had been set to indicate in Rem, while others were set to indicate in Sv/hr.
While it is fair to say that there would most likely be consistency within particular groups as to the units of measurement used, serious incidents can often require multinational involvement with the inevitable preference for varying units of measurement among different groups. What was clear was that those expected to use instruments of any type must be well practiced in being able to read and correctly interpret a variety of displays.
A number of visiting teams were also put through the same exercise scenario, some of which comprised members who had not worked together before. This in itself highlighted some interesting problems, with differing levels of proficiency within the teams, depending on if (and how often) they had trained and worked together. The value of training regularly as a team was evident. But equally too there was much to be gained from being required to work with a unfamiliar team, under challenging physical and environmental conditions.
The PlumeSIM simulation system enabled a sophisticated radiation training scenario, involving multiple radionuclides, to be implemented with ease and to be readily repeated.
From an instructor's viewpoint the simulation exercise also offers some clear advantages, for example not having to calculate the dose alarms and simulated dosimeter readings for the inject cards.
There was also great value in being able to generate relatively high instrument readings which most operators had never had the opportunity to experience before.

Case Study: A White Supremacist Dirty Bomb?

By Dr. Andrew Karam
Source: http://nct-magazine.com/december-2018/case-study-a-white-supremacist-dirty-bomb/

In the summer of 2010, when I was working for the New York City Department of Health and Mental Hygiene (DOHMH) I received a call from a colleague in the Fire Department of New York (FDNY). He told me that an elderly gentleman had recently died and, when his apartment was being cleared out, workers found some alarming items – a box full of Nazi paraphernalia, a number of what appeared to be hand grenades and mortar and artillery shells, and a sealed box marked

"radioactive" and labeled with radiation stickers. This raised some concerns, especially given the heightened profile of various hate groups around the world.
The person discovering these materials called the city's emergency phone number, and the person taking the call, following procedure, notified the Fire and Police departments. The possible presence of radioactive materials led to the call to DOHMH; specifically, to the Bureau of Environmental Emergency Preparedness and Response, in which I headed the Radiation Unit. So I grabbed some of our instruments and one of my staff and headed on over to the scene.
When we arrived, two FDNY trucks had blocked off both ends of the street and an NYPD helicopter was hovering overhead. In addition to FDNY, representatives from the NYC Department of Environmental Protection (DEP) were also present. Cops from the Emergency Services Unit (ESU) Hazardous Materials (HazMat) Unit were in charge of the scene; the HazMat Unit's senior lieutenant was someone I knew well so I found him and let him know we were on the scene.

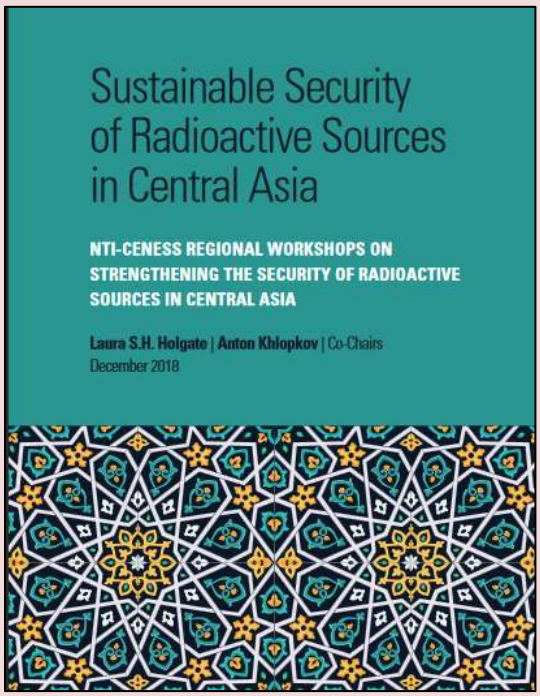
▶▶ Read the rest of this article at source's URL.

Andrew Karam *is a radiation safety expert with 35 years of experience, beginning with 8 years in the US Navy's Nuclear Power Program that included 4 years on an attack submarine. He has published over two dozen scientific and technical papers and is the author of 16 books and several hundred articles for general audiences. He has worked on issues related to radiological and nuclear terrorism for over 10 years.*

Preventing Dirty Bomb Terrorism: New NTI-CENESS Report Highlights Central Asian Republics' Commitment to Preventing Radiological Risks

Source: https://www.nti.org/newsroom/news/preventing-dirty-bomb-terrorism-new-nti-ceness-report-highlights-central-asian-republics-commitment-preventing-radiological-risks/

Dec 03 – Sustained regional dialogue between all relevant stakeholders—including regulatory, customs, border security, and energy authorities, as well as international partners—is needed to effectively address the challenge of radioactive source security in Central Asia, according to a new report by the Nuclear Threat Initiative (NTI) and the Moscow-based Center for Energy and Security Studies (CENESS).



Sustainable Security of Radioactive Sources in Central Asia, released at the International Atomic Energy Agency's (IAEA) International Conference on the Security of Radioactive Material, is the culmination of a two-year joint effort by NTI and CENESS to improve regional coordination on the security of radioactive sources and to prevent illicit trafficking of these sources in Central Asia.
As in other regions, **Central Asia is home to thousands of radioactive sources, most of which are used for medical, industrial, and research applications.** Often, the sources are located in busy, open settings, such as hospitals in city centers, or remote areas with little or no physical protection. If these sources escape regulatory control, they could be used to build radioactive dispersion devices, more commonly known as "dirty bombs."
"Largely as a result of poor chain-of-custody procedures and insufficient regulatory controls, thousands of radioactive sources have gone missing around the globe," the report says. "Even in countries with effective regulatory controls in place, high disposal costs and a lack of repositories have led end users to abandon radioactive sources at the end of their life cycle. These are challenges that affect every region of the world, including Central Asia."

Over the last two years, NTI and CENESS sponsored regional workshops, with support from the Government of Canada and in cooperation with the IAEA and the Governments of Kazakhstan and Kyrgyzstan, bringing together more than 70 experts to discuss opportunities to strengthen radioactive source security in Central Asia. Participants included experts from Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, the Russian Federation, the United States, Canada, the Eurasian Economic Commission, and the IAEA.

"These challenges are transnational in nature, requiring effective coordination and information exchange among all stakeholders," said Laura Holgate, NTI Vice President for Materials Risk Management, a co-chair of the regional workshops. "The NTI-CENESS workshops served as an excellent model of the kind of dialogue we would like to see happen more regularly in this region."

Anton Khlopkov, CENESS director and workshop co-chair, said, "The example of joint efforts by CENESS and NTI demonstrates the great potential of Russian-US cooperation in strengthening radiation security, including cooperation facilitated by the IAEA."

▶▶ **The report is available in English and Russian.**

What should we do with nuclear waste?

Source: http://www.homelandsecuritynewswire.com/dr20181212-what-should-we-do-with-nuclear-waste

Dec 12 – Some 80,000 metric tons of spent nuclear fuel have accumulated at more than 75 sites in 35 states – and the inventory is growing.

Failure to develop a strategy for permanent storage and disposal of this fuel costs Americans billions of dollars a year and jeopardizes the future of nuclear power as a carbon-free source of energy, according to Rodney C. Ewing, the Frank Stanton Professor in Nuclear Security and a Senior Fellow at the Freeman Spogli Institute for International Studies and at the Precourt Institute for Energy and the co-director of Stanford's Center for International Security and Cooperation.

A new report offers new recommendations for solving the U.S. nuclear waste problem, after discussing why conventional risk assessments don't go far enough and what makes this challenge more difficult than putting a man on the moon.

The three-year study spearheaded by Ewing with input from some seventy-five technical experts, government officials, leaders of nongovernmental organizations and affected citizens proposes a different path than the one so far taken. "We have to really change what we're doing if we want to succeed," Ewing said.

Ewing, in a discussion with Josie Garthwaite of Stanford's School of Earth, Energy & Environmental Sciences, talks about the report's core recommendations, why conventional risk assessments don't go far enough and what makes this challenge bigger than putting a man on the moon.

Josie Garthwaite: What would you like to see replacing the status quo of nuclear waste management in the U.S.?

Rod Ewing: We recommend a new not-for-profit independent corporation that's owned and supported by the utilities that operate nuclear power plants. This independent, private corporation would receive over a period of decades the more than $40 billion in the Nuclear Waste Fund, which has accumulated fees from ratepayers who use electricity generated by nuclear power plants. The Nuclear Waste Fund was established to pay for the disposal of commercially generated spent fuel.

The new organization would deal only with spent fuel from commercial reactors. Defense waste is an entirely different issue and should, at this time, remain the responsibility of the federal government.

The report's recommendation in effect would create two approaches for nuclear waste management and disposal: commercial spent fuel would be the responsibility of a utility-owned corporation and defense waste would remain the responsibility of the federal government. If both succeed, great. If one succeeds, that may open the door to the success of the other. As an example, the high-level waste from defense programs might finally be accepted for disposal at the commercial repository for a fee.

Garthwaite: What are some of the implications of transferring responsibility from the government to the utilities?

Ewing: According to the Nuclear Waste Policy Act of 1982, the federal government was to take ownership of the used nuclear fuel from the utilities in 1998. In the absence of a geologic repository, the government was not able to take ownership of the fuel, which now accumulates at reactor sites across the country. The utilities have sued the government and have won a settlement to cover the cost of their continued storage of the fuel at reactor sites. This settlement costs the taxpayer some $500 million a year with the total costs over time reaching some tens of billions of dollars.

The utilities package and store the fuel in ways that are economical from their perspective, but the result may well be packages that are unsuitable for transportation and disposal. In other words, there is a huge disconnect in the backend of the nuclear fuel cycle in the U.S. Our proposal to put the utilities in charge of the handling, transportation and disposal of the fuel removes many of these disconnects.

Garthwaite: One of your group's recommendations is for communities to volunteer to host a nuclear waste repository, or at least accept it. What are some of the reasons that a community would volunteer for this?

Ewing: We have communities that are very interested in the opportunity for economic development. The downside is you don't want communities volunteering just because they need the economic stimulus. The goal is to identify a technically defensible site near a community that understands why the site is suitable and safe. In Sweden and Finland, the repositories are located near communities that also have nuclear reactors and a good understanding of nuclear safety.

Garthwaite: Can communities ever really get a complete picture of what it will mean to host one of these repositories, given uncertainty about how these materials and sites will behave in the distant future? What are some of the technical and scientific challenges that must be overcome if this waste is going to be stored permanently?

Ewing: One of the points we make in the report is that the present regulatory framework extends over evolutionary timescales – out to one million years. In the U.S. there's a heavy emphasis on a quantitative, probabilistic risk assessment, which calculates risk out to a million years in order to determine whether a site complies with regulations. But in the report, we strongly endorse a different approach, the safety case, which has been used in other countries.

The safety case goes beyond calculations and includes qualitative assessments of safety, particularly over long time periods. With such an approach, the determination of safety does not rest on the calculations, but rather on a compelling argument for safety. As an example, locating a repository in an area with very old rocks, hundreds of millions of years old, can be one of the arguments for the long-term stability and safety of the site over one million years.

Garthwaite: In a best-case scenario where this does move forward and goes through all steps that you would hope for, how long will this endeavor take?

Ewing: Beginning from scratch, the identification and characterization of a site, the design and construction of the repository and the licensing process can take as much as 40 to 50 years. Once the repository begins to receive waste, it will continue operation for up to 100 years, given the amount of waste the U.S. can expect to accumulate. At that point, we would expect the repository to be sealed permanently.

Sometimes colleagues have said, "We put a man on the moon, the Manhattan Project created the first nuclear weapons – why can't we site and build a geologic repository?" My answer is that this is a very different type of activity – one that requires creative and rigorous science and engineering and careful attention to the social aspects of the process. In this field one has to be prepared to deal with a changing political environment and a skeptical public. This is why trust is such an essential characteristic of any organization dealing with nuclear waste.

New Technology to Detect Radiation in Millions of Containers

Source: https://i-hls.com/archives/87443

Dec 14 – Detecting small amounts of dangerous nuclear material in one container out of millions is a challenge to security professionals worldwide, as solutions are needed that are capable of efficiently scanning up to 100% of cargo transiting a port. This high level of screening enforcement can only be achieved with systems that produce very low false alarms during primary screening and rapid alarm resolution capabilities, including secondary screening.

L3 Security & Detection Systems (L3 SDS) has been awarded a contract by the U.S. Department of Homeland Security. The company's solutions focus on port and border security screening and airport checkpoint, checked baggage and air cargo screening, as well as secure government and commercial facilities and events.

The company will provide radiation monitoring portals at ports of entry operated by the U.S. Customs and Border Protection agency. The contract is part of a federal programme to enhance the detection of radiation in cargo containers and prevent unauthorized nuclear materials from entering the country.

The **CR-Portal gamma/neutron detection solution** is designed for 24/7 monitoring. The safe portals use passive radiation detectors and are specifically designed for a variety of uses. The CR-Portals are integrated portal configurations with optional sensor capability using the company's CV 2 software, according to their website.

The **CV 2 software solution** integrates data from a variety of scanning systems onto a single, centralized display. The software is a user-friendly, visually-based solution that allows analysts to quickly assess cargo contents locally or remotely for contraband and other illegal materials.

According to porttechnology.org, the CR-Portals are the "continued evolution" of L3's advanced radiation monitoring portals, which have been used in the Netherlands since 2014. The technology has been tested, according to L3, under the most rigorous and comprehensive testing regimen for radiation portal monitors.

Pak Chin, President of L3 SDS, said: "L3's advanced detection radiation monitoring portals will enhance Customs and Border Protection's ability to perform screening with significantly improved accuracy and effectiveness." "The portals detect dangerous radioisotopes masked by other materials while allowing for normally occurring radioactive materials – thereby improving cargo throughput."

A Mobile Complex System for Fast Internal Contamination Monitoring in Nuclear and Radiological Terrorism Scenarios

By Ignazio Vilardi, Giuseppe Antonacci, Paolo Battisti et al

Enhancing CBRNE Safety & Security: Proceedings of the SICC 2017 Conference pp. 21-30
Source: https://link.springer.com/chapter/10.1007/978-3-319-91791-7_4

Abstract
In order to properly respond to an emergency of nuclear and radiological terrorism, we realized a mobile complex system (MCS) for conducting on field a large-scale individual monitoring of internal contamination by gamma emitters. The proposed MCS consists of a collective protection apparatus and a HPGe portable spectrometer for whole-body and thyroid measurements. The MCS performance was evaluated and showed, assuming, for instance, an acute inhalation of ^{137}Cs and ^{131}I occurred 5 days before measurement, detection limit values resulting in a committed effective dose equal to 0.07 mSv, and a maximum committed equivalent dose to thyroid equal to 1.3 mSv, respectively. Considering the annual limit of effective dose for public exposure and the lowest reference level to plan stable iodine prophylaxis, the proposed MCS has a significant sensitivity to be used for fast internal monitoring in nuclear and radiological emergencies from malicious acts. This MCS allows to operate in contaminated environment and to monitor daily a large number of individuals.

Pharmacology of radiological protection. An operative proposal

By Ciccotti M.[1,2], Carbone D.[4]., Ciccotti M.E.[5], Peluso I.[6], Buccolieri C.[2], Scimonelli L.[7], Munzi D.[2], Di Muzio M.[5], Sciarra T.[2] and Palmery M.[1] and Lista F.[3]
1. Department of Physiology and Pharmacology "V. Erspamer"
2. Joint Veteran Center, Scientific Department, Army Medical C enter, Rome, Italy
3. Scientific Department, Army Medical Center, Rome, Italy.
4. Department of Oral and Maxillofacial Science, "Sapienza" University of Rome
5. UO Clinical Pharmacy, INRCA-IRCCS Ancona 60121.
6. Research Centre for Food and Nutrition, Council for Ag ricultural Research and Economics (CREA-AN), Rome, Italy.
7. Higher Institute of Health, seconded to the Ministry of Health

Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

After the Chernobyl accident in 1984, the risk of exposure of the population to ionising radiation as a result of nuclear disasters came back to the fore with the Fukushima accident. The accepted therapeutic approach is to administer potassium iodide tablets in order to reduce the incidence of thyroid cancer. This study aims to analyze pharmacologically active molecules with high shielding power against ionizing radiation currently used in clinical practice as **amifostin**, capable of acting on several mechanisms such as: reduction of oxygen consumption, blocking the production of free radicals, increasing the DNA repairing ability, while maintaining the integrity of the **p53 gene**. As well as **l-carnitine** which acts as an excellent cell scavenger rather than using of molecules with high antioxidant power such as **resveratrol**, with the aim of hypothesizing a special self-rescue kit to be used in case of nuclear accident. This pharmacological approach will strengthen the mechanisms of response and cellular repair, reducing and mitigating relapses following a radiological accident.

Counter method against I2(g) radionuclides in CBRN scenario

By Quiñones J.[1], Pascual L.[1], Fernández M. D.[1], Jose A.[1], Amigo L.[1], Cobo J. M.[1] and Mazanec K.[2]
1. Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT), Avenida Complutense nº

40, 28040, Madrid. Kingdom of Spain.
2. Military Research Institute, Veslařská 230 637 00 Brno, Czech Republic.
Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

Iodine radionuclides are ones of the most hazardous nuclides from nuclear power plant accidents due to their easy dispersion, solubility and impact on human health. Moreover, iodine radionuclides are extensively used in biomedical applications facilitating its availability and accessibility, and consequently the possibility of theft or clandestine sale for use for terrorist or criminal purposes, i.e., CBRN attack. These risks justify the interest in the development of reliable processes for the efficient capture of iodine airborne released to the environment which is the objective of this work. The proposed procedure combines the use of solid sorbents and wet scrubbing. The capacity of microstructured metal oxides to retain iodine has been tested at laboratory scale and the effectiveness of process, in a facility that simulates a real scenario. In these tests, iodine was dispersed as I2(g), and subsequently, metal oxides micro particles were scattered for its sorption. Finally, the oxide particles with the retained iodine were precipitated by means of a system of nebulized water developed under the European project Counterfog. The coupled system of microparticles plus nebulized dissolution is postulated as an emergency counter for first response to a CBRN scenario regardless of the origin, i.e., accident and/or malicious act.

Development of a radiation-detection simulator with smartphones and beacons for first responders against radiological threat

By Tsuchiya K.[1], Moritake T.[2], Ishigaki Y.[3], Kosukegawa N.[4]
1. National Research Institute of Police Science, Japan
2. University of Occupational and Environmental Health, Japan
3. The University of Electro-Communications, Japan
4. Yaguchi Electric Corp, Japan
Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

We have developed a radiation-detection simulator (emulator) using smartphones and Wi-Fi or BLE (Bluetooth Low Energy) beacons. A **Wi-Fi beacon** transmits a data with SSID (Service Set Identifier) from the wireless access point. A BLE beacon is used as indoor positioning system. Smartphone's software (mobile app) can detect RSSI (Received Signal Strength Indication) from their transmission. Signal strength increases as first responder with a smartphone moves closer to the beacon. We developed a mobile app for calculating pseudo gamma-ray dose rate from RSSI and displaying it on smartphone. We evaluated our developed emulator, **USOTOPE** (Utilizing Safety-radiation source Object + radioisoTOPE). The relation between indicated dose rate and distance from a beacon was measured in a building and in open space. We confirmed USOTOPE approximately followed the inverse-square law (1/r2). It was found that this was available within at least 20m from the source position, in which the equivalent dynamic range was 0.1 to 10 uSv/h. This radiation-detection emulator helps the training for searching suspicious radiological sources.

Food safety after nuclear accidents: looking back to Chernobyl experience to propose new approaches for risk mitigation

By Moramarco S.[1,2] , Puleio A.[2,] Carestia M.[1,3]
1. Department of Biomedicine and Prevention, University of Rome Tor Vergata
2. International Master Courses in " Protection against CBRNe events" - University of Rome Tor Vergata, Italy
3. Department of Industrial Engineering, University of Rome Tor Vergata
Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

Food contamination is particularly relevant in case of nuclear accidents. The risk on food supplies and distribution systems is a real threat for health, ecology, economy and political stability. Food contamination in a country can also have a significant effect in other parts of the world, so that timely sharing of information between countries in case of those events is paramount. A relevant negative example come from the Chernobyl accident (former Soviet Union 1986), where countermeasures were flawed and a lack in timely advice, especially for private farmers, were registered. In the first week, management of animal fodder and milk production (including the prohibition of fresh milk consumption) would have helped significantly to reduce the toxic effects. In many European countries, levels of radionuclide (Iodine I-131 and Caesium Cs-134/137) in fresh, dairy products, vegetables, meat, berries, mushroom and fish were found increased immediately after the catastrophe. At the same time, measurable amounts of Chernobyl contaminants were found also in food products like pasta, cheese, juices, tea, imported from all central east side countries, Turkey to Norway. Considering the long decay time of radionuclides and their impact on foodstuff, it is key to predict and monitor the long term effects on food safety and human health after the Chernobyl accident.

3D Numerical simulation of a stealth radiological attempt to a military base

By Marturano F.[1,3], Ciparisse J. F.[2,3]

1. Italian Air Force 9th Air Brigade ISTAR-EW 2

2. University of Rome Tor Vergata- Department of Industrial Engineering, Italy

3. International Master Courses in " Protection against CBRNe events" - University of Rome Tor Vergata, Italy

Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

Radiological attempts are becoming a greater concern in military and civilian milieus, as they are insidious, very harmful and can easily be realized with a limited quantity of materials. The effects of such strikes are severe consequences both for the people coming into contact with the radioactive substance and for the denial of the contaminated area for a long time. Dirty bombs are the most feared devices, but a silent release of a radiological material may be much more effective, as it doesn't raise any alarm. This work is intended to show how dangerous a release of 60Co, carried out by a drone over a military installation, could be for both the personnel and the overall performance of the unit based there. For this purpose, a numerical study of this scenario has been carried out in two steps. First, a CF D simulation of the unsteady multiphase flow over the target has been performed to calculate, with a high level of accuracy, the local and instantaneous concentration of radioactive particles. Then, a clinical model has been applied during the post-processing phase of the results to estimate the local expected mortality on the basis of the inhaled quantity of radioactive material.

Biomarkers for early detection of the levels of ionizing radiation exposures: preliminary results of a SPS-NATO funded project

By Giovanetti A.[1], Bartoleschi C.[1], Pardini M. C.[1], Marconi R.[2], Pinnarò P.[3], Sanguineti G.[3], Canfora M.[4], Awad N.[5], Strigari L.[2]

1. Laboratory of Biosafety and Risk Assessment, Division of Health Technologies, Department of Sustainable

Territorial and Production Systems, ENEA (Rome, Italy);

2. Laboratory of Medical Physics and Expert Systems, IRCCS Regina Elena National Cancer Institute (Rome,

Italy);

3. Radiotherapy Department, IRCCS Regina Elena National Cancer Institute (Rome, Italy);

4. Scientific Direction, IRCCS Regina Elena National Cancer Institute (Rome, Italy)

5. High Institute of Public Health, University of Alexandria (Alexandria, Egypt);

Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

A radiological/nuclear (R/N) emergency may cause a casualties' toll high enough to overwhelm the medical facilities in charge. It is therefore highly needed a tool to sort the unaffected subjects from those individuals requiring immediate medical evaluation and intervention. The early assessment of absorbed dose may also aid in predicting the severity of later health outcomes and to put in place early and effective medical countermeasures. The reference biomarkers are dicentrics or micronuclei count in lymphocytes providing results starting from 50h and 74h.
Here we present the preliminary results of the Italy-Egypt project "A PANEL OF BIOMARKERS AS NOVEL TOOL FOR EARLY DETECTION OF RADIATION EXPOSURE" funded by NATO SPS, aiming at validating a fast, accurate and handy tool for detecting absorbed dose soon after exposure.
The selected early biomarkers included blood counts, DNA breaks and radio-inducible proteins tested on blood from patients submitted to one fraction of radiotherapy with doses/fraction of about: 200; 350; or >500 cGy in Italy and in Egypt.
Based on univariate and multivariate correlation our results indicated that early biomarkers may be used for the assessment of the dosage to the target and/or to the whole body after partial irradiation.

Super-rich prepare for doomsday in Dh180m American bunkers

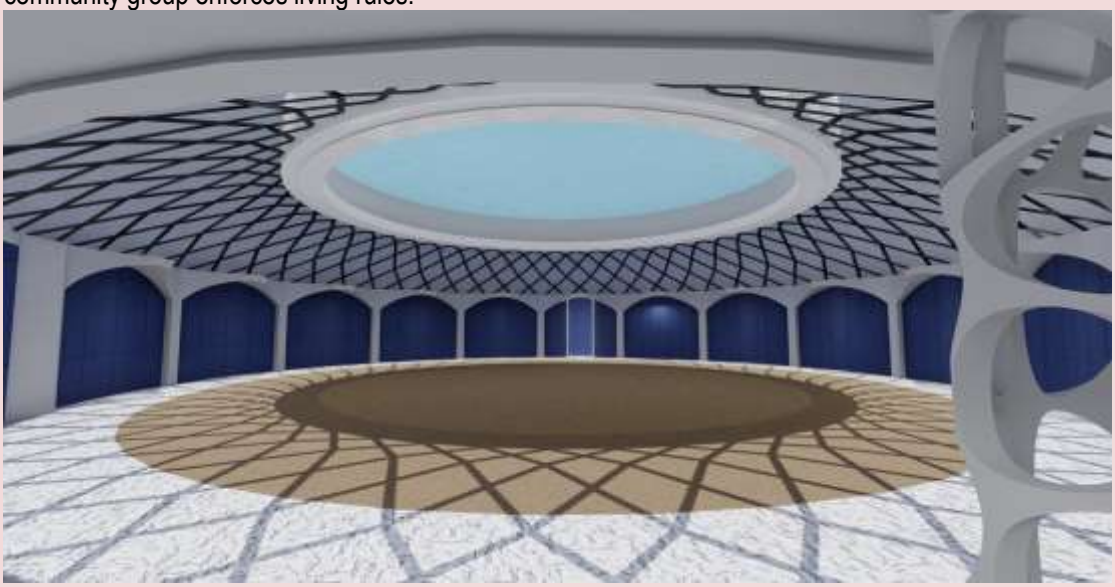
Source: https://www.thenational.ae/uae/super-rich-prepare-for-doomsday-in-dh180m-american-bunkers-1.804263

The dome of one of the underground bunkers. Courtesy: Survival Condo Project

The super-rich are looking at luxury doomsday bunkers in America that can withstand a nuclear attack or catastrophic natural disaster.
These units are known as "survival condos" and are many metres underground in a former Cold War-era missile silo in Kansas. People can try to ride out the worst there for at least five years.
Prices start at $1.5 million (Dh5.5m) for a basic 85 square metre unit, while a cool $50 million (Dh183 million) can get you the entire 15-storey silo, which can accommodate 120 people.
No firm purchases have been made and the identity of those interested is not clear as they are represented by third parties who sign non-disclosure agreements. But developer and owner Larry Hall believes the interest is serious and has even been asked to produce designs for a mosque and helicopter pad by one client.
Mr Hall told *The National* he knows of several interested buyers in the UAE who want to inspect the doomsday bunkers.

A design rendering of how a helipad would look close to the underground complex. Courtesy: Survival Condo Project

"We were recently asked to show both the completed silo and the new one that is under construction to a group from the UAE," Mr Hall said.
"We are hoping that this visit happens in January. The new facility has a narrow window in the schedule to support these types of changes but that window will be closing fairly soon."
These people are believed to be rich and influential figures who want to buy the whole silo rather than individual units.
"I would say this is unique to the Middle East as their interest is the entire facility – which is much more interesting."
Residents would have access to a swimming pool, dog-walking park, rock climbing, a classroom, theatre and a shop. An aquaponic farm produces food. Special lighting and plans to rotate communal jobs to fight boredom are part of efforts to meet the psychological challenges posed by long-term life underground. A community group enforces living rules.



A design plan of the mosque that could be incorporated into the underground bunker. Courtesy: Survival Condo Project

Renewable energy comes from wind turbines supplemented by diesel generators, while water comes from an aquifer. Buyers also must pay monthly service charges, excluding tax. There is 24-hour security.

Mr Hall has completed one silo, while the second is expected to be finished within 16 months. The existing bunker has 12 units, while the newer one will be bigger and could accommodate 24 units.
The original silo is sold out and those who purchased units are largely self-made millionaires who bought them for their families.
Mr Hall owns one of the units himself and said he believes interest from the UAE and the Gulf region to be even greater than he is aware of because non-disclosure agreements stop agents from revealing buyers' identities. Those interested also tend to be secretive.
The developer said one agent, who claimed to represent clients in the UAE, Saudi Arabia and China, told him that in all three cases the buyer wanted a "safe space" for their citizens.
"He [the agent] used the examples of students going to American universities, diplomats and even engineers and their families living or working in the US," Mr Hall said.

The entrance to the existing luxury bunker, with its wind turbine on the left. Courtesy: Survival Condo Project

"The concern was also the same – if some catastrophe, either man-made or a natural disaster were to happen, these citizens would have a safe place to go on short notice to find safety."

Residents have access to many facilities, including a swimming pool. Courtesy: Survival Condo Project

The silo's upper section has 2.7-metre thick walls that can withstand a nuclear blast producing winds of more than 3,200kph. There are also advanced communications systems and residents would also be given secure transport to the silo in the event of a disaster.

Known as Altas F, the silos were named after a type of intercontinental ballistic missile, and only 72 were built by US army engineers in the 1960s. Most of them were decommissioned by the 1970s and sat idle for years until Mr Hall bought one for $300,000.
He previously worked as a government contractor and saw a gap in the market after 9/11 when emergency planning re-emerged as a government priority. He sank millions of his own money into the project.
The rising interest in these units is linked to the "prepper", or survivalist, movement, whose members stockpile food, water and medicine in readiness for a worst-case scenario.
“The interesting fact about Kansas is that it is in the middle of nowhere,” said Mr Hall.
“But it is halfway to everywhere.”

North Korea 'may have used foreign scientists to further its nuclear ambitions'

Source: https://www.telegraph.co.uk/news/2018/12/20/north-korea-may-have-used-foreign-scientists-nuclear-ambitions/

The launch of the Hwasong-12, an intermediate range ballistic missile in 2017 Credit: HOGP/AP

Dec 20 – North Korea may have been exploiting collaboration with foreign scientists to bypass tough international sanctions and further its nuclear weapons programme, according to a new investigation.
An analysis released by the James Martin Centre for Nonproliferation Studies in Monterey, California, flags at least 100 journals published jointly by North Korean and foreign scientists that have “identifiable significance for dual-use technology, weapons of mass destruction (WMD), or other military purposes.”
The findings, based on scientific journals spanning more than six decades, shed some light on how North Korea could have advanced so rapidly in building its nuclear and missiles technology despite long-running and harsh international penalties to prevent it from doing so.
The large majority of the 1,304 research papers dating from 1956 to April 2018 involve natural sciences, engineering or mathematics, but among the identified “areas of concern or potential concern” are Romanian assistance with uranium purification and GPS-related work with Germany and China.
Most of the research that warrants a closer look involves collaboration with Chinese scientists.
In an interview with The Telegraph, Joshua Pollack, one of the lead authors on the report, highlighted work on the “isolation of high voltage cables” and on automotive technology as apparently “clear-cut” examples of potential breaches of the ban on the transfer of dual-use equipment.
Dual-use in this sense would be any legitimate technology that could also be appropriated to assist the creation of WMD or nuclear reactors.

Joint Chinese and North Korean papers on automotive technology had set off alarm bells as they included a computer system that could make the axels on a truck operate independently, said Mr Pollack.
"That is something that is not associated with an ordinary truck. There are civilian applications for that but in North Korea the obvious use for that is a missile launching vehicle," he revealed.
Such an extensive analysis of the risks of scientific collaboration with North Korea is rare, but it is not the first time the issue has been raised.
Last year, Ken Kato, director of the Tokyo-based Human Rights in Asia, wrote to the ambassadors of the five permanent members of the United Nations Security Council, urging them to close a legal loophole that allegedly allowed pro-North Korean scientists to remain in sensitive research positions.

Students wear virtual reality goggles during a science class at Pyongyang Teachers' University
Credit: Dita Alangkara/AP

"There are six Korean scientists who have been able to remain in sensitive research positions after claiming to have switched their political allegiances to South Korea," Mr Kato claimed on Thursday. He has not yet received a UN response to his earlier enquiry.
Mr Pollack and his team conclude that "UN member states must decide what research activities by their nationals or within their territory lie within the scope of sanctions, and which activities are better avoided in order to uphold the integrity of the sanctions regime."
He added: "We do not want to hand Kim Jong-un a shortcut to advancing his military, advancing his weapons of mass destruction."
But the complicated nature of scientific research also creates a dilemma about where to draw the line.
Mr Pollack stressed that concerns over the misuse of some research should not lead to a "blanket ban" on scientific collaboration with the secretive regime, which prizes scientists so highly that it awards them with the best housing in the capital, Pyongyang.
"You would have to have very strong reasons to shut the North Koreans out, bearing in mind that science contributes to human welfare and progress. It's not all about weapons," he said.
Many Western researchers are heavily vetted by their governments before they can proceed.
British cooperation with Pyongyang over the years has included "frontiers on mathematics", engineering principles and, more recently, studies of Mount Paektu, a volcano on North Korea's border with China.
James Hammond, a geophysicist at the Birkbeck University of London, who has been working on the project alongside American, Chinese and North Korean colleagues, told NPR that it took almost two years to get US and UK government approval to carry in sensitive seismic equipment.
Research on the volcano could prove vital to saving many lives if there was a future eruption, Mr Pollack pointed out.

"I think it may be the case that we don't do enough when there are humanitarian issues. In particular, epidemiology comes to mind. In both China and North Korea there is a lot of drug-resistant tuberculosis, for example… And disease doesn't care that much about borders," he said.
Finally, he argued, scientific collaboration made sense from a strategic point of view. Towards the end of the Cold War, cooperation between Soviet and American scientific establishments helped to build bridges between the two enemies.
"Having these bridges between scientists is not a bad thing from a perspective of enlightened self-interest," he said.

Weapons experts: Iranian nuclear archive shows that Iran lied about uranium mine

Source: http://www.homelandsecuritynewswire.com/dr20181221-weapons-experts-iranian-nuclear-archive-shows-that-iran-lied-about-uranium-mine

Dec 21 – **Nuclear weapons experts, who have reviewed the Iranian nuclear archive that Israel recovered from a Tehran warehouse, concluded that Iran lied that a uranium mine was under control of its civilian atomic energy agency.**
Nuclear weapons experts, who have reviewed the Iranian nuclear archive that Israel recovered from a Tehran warehouse, concluded that Iran lied that a uranium mine was under control of its civilian atomic energy agency in a paper published jointly by the Foundation for Defense of Democracies and the Institute for Science and International Security on Wednesday.
The paper — written by David Albright, a former weapons inspector and president of the institute; Olli Heinonen, former deputy director general of the International Atomic Energy Agency (IAEA); Frank Pabian, a former inspector for the IAEA; and Andrea Stricker, a senior policy analyst at the institute — asserts that Iran falsely told the IAEA that its uranium mine at Gchine was under civilian control, when it, in fact, remained under the auspices of its military nuclear weapons program.
"The site was originally part of the AMAD plan to produce nuclear weapons. It was military-owned and created to produce uranium for Iran's covert nuclear fuel cycle and five initially-planned nuclear weapons," the paper charged in its conclusion. "Gchine is but another egregious example of Iran's deceptions to the IAEA and the international community."
In reviewing the files recovered from Iran's nuclear archive, the team has previously learned not only that Iran's nuclear weapons program had progressed further than previously thought, but that Iran possessed "advanced capabilities" to develop nuclear weapons. What the experts concluded, was that "that Washington and the IAEA were constantly underestimating how close Tehran was to a bomb" prior to negotiating the deal that was finalized in 2015.
In a previous paper published by the institute, Albright, Heinonen, and Pabian argued that the new information contained in the archive "necessitates calling for more action by the IAEA and the Joint Commission, which administers the Joint Comprehensive Plan of Action (JCPOA)."
In an op-ed published in October in The Hill, Josh Block, the President and CEO of The Israel Project, noted that the IAEA had failed to follow through on the Israeli revelations and the implications of those failures on the agency's overall knowledge of Iran's nuclear weapons work.
"The gaps in the IAEA's knowledge — of Iran's past nuclear work, of its military sites, of items mentioned in Section T of the nuclear deal, and of the nuclear sites discovered by Israeli intelligence — raise questions about the full extent of Iran's nuclear program," Block argued.
The documents and files that Israel smuggled out of Tehran in January, and which Israeli Prime Minister Benjamin Netanyahu publicized at the end of April, consists of some 100,000 pages and covers Iran's nuclear weapons program during the years of 1999 to 2003.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

EXPLOSIVE NEWS

200 years to go before Laos is cleared of unexploded US bombs from Vietnam war era

By Padraic Convery By Padraic Convery
Source: https://www.scmp.com/magazines/post-magazine/long-reads/article/2173220/200-years-go-laos-cleared-unexploded-us-bombs

Nov 19 – Thanksgiving is an American tradition that is unknown in most of the world. Fifty years ago, however, it landed in Laos, the small, impoverished Southeast Asian nation that was to become perhaps the longest-suffering casualty of the United States' war in Vietnam.

Thanksgiving is held on the fourth Thursday in November. In 1968, that fell on November 28, and on that day, at the height of the war and on the orders of president Lyndon B. Johnson, turkey dinners were helicoptered in to American soldiers who were on a mission to sever the Ho Chi Minh Trail – the network of paths and tracks that constituted North Vietnam's military supply lines to the south of the country – that ran through eastern Laos.

LBJ's festive dinners were flown in at the same time as the US began dropping millions of bombs on the trail, which it had already been targeting for four years. Half a century later, Laos is still dealing with the deadly legacy of that bombing campaign, which left an estimated 100 million pieces of unexploded ordnance on the ground.

On a dusty dirt road near the sleepy southeastern Laotian town of Xépôn, just 20km from Route 909, which follows one of the Ho Chi Minh Trail's main arteries, and 46km (29 miles) from the border with Vietnam, the day begins with a warning.

"Minh, remember, no metal," says Calum Gibbs, a burly young Scotsman and an operations officer with the Scotland-based Halo Trust, one of several NGOs helping to clear up unexploded munitions left by the nine-year US campaign of aerial attacks on Laos, which ended in 1973. "There's metal in your tape measure."

Minh is a lean Laotian man, his skin like leather, trained by Halo as an unexploded ordnance (UXO) disposal expert. He sheepishly hands his tape measure to colleague Gah, then disappears into the forest to re-examine a bomb found by villagers. A Halo team has already tried, unsuccessfully, to destroy the weapon.

Gah explains that taking metal close to the still-active fuses on some munitions could cause them to detonate. "The most dangerous ones are very sensitive – sensitive to temperature or with a fuse activated by magnetism," he says.

As we mill around beside our four-wheel drive, Minh is somewhere among the trees, checking how much explosive is left in the weapon after the first attempt to render it harmless. Ten minutes later, he returns. "From the fuse, there's 45cm of high explosive," Minh says. "The parts that are left are quite thick metal, so we cannot burn a fire to detonate it. This bomb is quite big – 500lb."

"So … Plan?" Gibbs asks. "Destroy it?"

Minh will calculate the area that will have to be taped off before the bomb can be detonated. For the disposal of a 500lb bomb, Halo advises that no people or livestock should be within a 1.5km radius. That distance can be reduced by using earthworks, sandbags and walls, but the road we are standing on is well within the blast zone. It will have to be closed off.

Gibbs gestures towards a pile of sandbags at the top of the riverbank that he says was part of a protective bunker. "This was our firing point when we blew the item initially," he says. "A 1.5km firing cable is not very practical, so you have a bunker that you build inside the blast zone, with a certain number of sandbags over the top, nice and secure from frag."

Bunkers, road closures, dozens of Halo staff to seal off the blast zone, kilograms of C4 explosive, hundreds of metres of firing cable and the constant risk that something might go fatally wrong – all to get rid of a single large bomb. And the US dropped close to 300 million on Laos!

As troops' turkey dinners were being choppered in that November, the bombing campaign was being massively ramped up, from about 4,700 sorties in October 1968 to some 12,800 the following month. In total, the US launched about 580,000 bombing missions over Laos – equivalent to a planeload of bombs every eight minutes, 24 hours a day, for those nine years – making it the most heavily bombed country per capita in history. It has been estimated that possibly one-third of the devices failed to detonate, and as many as 80 million remain unexploded. They litter villages, tracks, farmland and forest across much of the country. At the current rate of progress, making Laos completely safe again will take 200 years.

Nevertheless, progress has been made. When I visited Xépôn 20 years ago, it was a ramshackle collection of small houses and huts with no electricity. Route 909 was hardly a road at all. Deadly explosives lined the dusty, cratered track and many more unexploded munitions – mainly cluster bomblets – lay in wait in fields for unlucky farmers and other villagers.

Today, the Route 909 section of the Ho Chi Minh Trail near Xépôn is a smooth, two-lane blacktop along which American-made trucks thunder. Power lines that did not exist two decades ago follow the road. There is a tidily maintained war museum, and fishermen's canoes in the Xépôn River have been fashioned from the discarded long-range fuel tanks of B52 bombers.

Further north, in the province of Xiangkhouang, where British bomb-clearance NGO Mines Advisory Group (MAG) has been working for 24 years, the story is similar. In the provincial capital, a small town named Phonsavan (where, two decades ago, it seemed that every house incorporated bomb casings and panels from aircraft), main roads are paved and tidy, shops and other businesses have sprung up, and there are street lights where once there was no electricity after 10pm.

Canoes made from B52 fuel tanks on the Xépôn River. Picture: Padraic Convery

Upgrading major roads and providing electricity has been a priority across the country, and UXO clearance resources – of both government and private contractors – have been committed accordingly. The discovery of precious metals and minerals in the Xépôn area has attracted foreign companies, which has led to the stepping up of bomb-clearance efforts around those projects.

When it comes to land that local people have to live and work on, however, clearance has, in the main, been left to NGOs such as Halo, MAG, Norwegian People's Aid and Japan Mine Action Service.

"We prioritise our clearance based on impact and beneficiaries, so we can clear an area that's going to be used for [crop] cultivation or a school," says Gibbs. "In one of the villages we drove through earlier, we cleared an area and they built a school on it. That's exactly what we want."

Gibbs emphasises the importance of education in keeping people safe. "We send out risk-education teams to educate kids," he says. "They have a UXO song and the kids sing it so they remember that UXO are dangerous."

Victims of the explosives scattered across Laos are, in fact, disproportionately young. "On my second day in the country, there was a fatality, an eight-year-old," Gibbs says. "They looked like they'd been throwing it around. They'd found it in the forest." He remembers the offending explosive as being a BLU 24 cluster bomblet, which is the size and shape of a tennis ball. "One kid died, one was severely wounded, and three young girls suffered blast fragmentation injuries.

They've lived with it for so long – their parents, their grandparents – it's a feature of life. It's almost like they've just become normalised to it, which is really sad

Calum Gibbs, operations officer, Halo Trust

"I remember what I was like as a kid," says Gibbs. "If I grew up here, I'd be playing with this stuff. You see an iron-looking ball and it's something to throw at your mates.

"We get out and … show pictures of these things to kids, but I remember what I was like at school, and when someone comes in to teach you about whatever, you're playing with your mates and talking about football. They've lived with it for so long – their parents, their grandparents – it's a feature of life. It's almost like they've just become normalised to it, which is really sad."

Thanks to NGOs' education efforts and continuing clearance, casualty rates are declining, down from about 200 deaths annually two decades ago to 50 or so in recent years. "The figures I've seen show 50,000 casualties since the war ended in terms of UXO accidents," Gibbs says. "Because now most of the urban areas have been cleared, they're getting less and less, but as the population expands and more areas are cut for upland [rice] paddy and that sort of thing, people are going to be interacting with UXO more and more."

Minh says that Halo's survey teams receive about 60 call outs every month for UXO discovered by villagers, and that its disposal experts destroy 70 to 80 explosive devices a month. As unused land is earmarked for development, however, Halo is in a race against time. The work is hard, dangerous – and excruciatingly slow.

All of which is demonstrated when we accompany a clearance team, sweating under body armour and ballistic goggles, up a steep hillside and through thick undergrowth on a banana plantation. About 200 metres (650 feet) in, we come across a marker of blue spray paint surrounding a BLU 26 cluster bomblet, which is on a list of items to be destroyed in a controlled blast later in the day. Such bomblets are the most prolific killers among the UXO in Laos.

A BLU 26 cluster bomblet in Xépôn. Picture: Padraic Convery

Our next stop, after a bone-shattering drive up a rutted track, is on a hillside where an area perhaps the size of a football field has been stripped of vegetation to allow clearance workers to use metal detectors. It has taken eight of them a week to defoliate and survey the area, during which eight live cluster bomblets and a larger bomb have been discovered. More are suspected of being buried under the surface.

Detectors wail with alarming frequency as we slog up the slope. Each time, a hole is dug in a fixed radius around the locus of the signal, and whatever lies beneath the soil is identified. Usually, it turns out to be shrapnel, but every signal must be investigated. Fragments are removed from the area – nothing that can set off a metal detector should be left behind.

Fortunately, there have been no casualties among Halo's survey and clearance teams. What's more, jobs at the NGO are highly sought after by locals, and Halo is now preparing to boost its headcount in Laos from about 330 to 550.

"We're only just starting interviews, and we might have 2,000 people turn up," Gibbs says. "Everyone wants to work for Halo because it's international NGO money, and it's job security and stuff like that, even though it might well be that it's just for a year."

That's always a difficulty – the funding is at the whim of politicians. They might decide this year that their priorities are going to be different to appeal to voters. Few politicians see beyond their term in office
Calum Gibbs

In a country where most people get by on less than US$2 (HK$15.50) a day, an NGO job represents a lucky break, even if employment can be cut short by the stroke of a pen in Whitehall or Washington.

The vast majority of Halo's funding in Laos comes from the British and American governments, and the NGO received a significant shot in the arm for its operations there when US president Barack Obama, in his final months in office, in late 2016, pledged to double his country's US$45 million contribution to UXO clearance in the country. That was a three-year commitment.

"Some governments get really involved in the mine-action sector, and it waxes and wanes depending on who's in charge," Gibbs says. "That's always a difficulty – the funding is at the whim of politicians. They might decide this year that their priorities are going to be different to appeal to voters. Few politicians see beyond their term in office."

The precariousness of funding is a frequent topic of conversation in the UXO clearance community in Laos, and unrealistic clearance targets expected by international donors can be a source of frustration.

"Because the targets are almost unattainable, there's every chance that the government department involved will turn around and say, 'Well, you failed to meet your targets, so we're not going to give you the money again,'" one foreign NGO worker says, adding, "It won't be me that suffers, it'll be the local staff."

While employment by a foreign NGO lasts, locals benefit from not just attractive pay, but also professional training. And although they are digging on their hands and knees in the stifling heat, and do face genuine risks, as Gah explains, "they feel they're doing something good – something good for their country".

The population of Laos has grown rapidly, from 3 million in 1975, when the ruinous Vietnam war finally ended, to close to 7 million todays. With a median age of about 21 years, Laos has the youngest population of Asia, it is believed, so the overall fertility rate is high and numbers are predicted to continue rising. With ever more mouths to feed, the need for more land to grow crops on also rises, placing more people in danger.

"During rice-growing season," says Gibbs, "everyone's out and they'll find more items, so we'll get more calls."

Harvest season in Laos (which at the time of writing was well under way) also brings increased UXO-related risks. As Americans tuck into their Thanksgiving turkey dinners on November 22, just like the US troops in Southeast Asia half a century ago, Laotian people, especially those in the rural areas that were devastated by the US bombing, will be giving their own thanks – so long as the rice crop comes in without any more casualties inflicted by a long-ago war.

What happens when an explosive is detonated?

By David S. Moore

Source: https://www.abqjournal.com/1251949/what-happens-when-an-explosive-is-detonated-ex-scientists-at-lanl-are-working-make-explosives-safer-and-easier-to-handle.html

Nov 30 — When an explosion goes off, we often think of the damage it does. We seldom think of explosions as constructive, but explosives have always been a critical component of industries such as mining, construction, transportation and even metal bonding.

Despite great advances in explosives since Alfred Nobel invented dynamite, the concept of detonation still baffles scientists. Although linked with the term "explosion," detonation is quite a different matter. An explosion is defined as a sudden event that results in a loud noise and the fast, typically spectacular burst that breaks apart and sends pieces flying outward. One example of an explosion is a water heater whose pressure-relief vent for some reason plugs up. The

pressure then builds in the water heater to the point that it finally bursts with so much force that the water heater rockets from the basement up into your house. Derived from the Latin word detonare, which means to thunder down, a detonation is what scientists call a supersonic burn-front. Picture someone lighting the fuse on a stick of dynamite. The point at which the material is burning is known as the burn-front – it is the location of the burn as it travels through the fuse material. If the velocity of this burn-front moves slower than the speed of sound (subsonic) along the material, the result is simple burning, also known as deflagration. If the velocity is faster than the speed of sound in a material, it is a supersonic burn-front. It builds a powerful shock wave, one whose incredible pressures can propel metal, break rocks and move earth. It is this type of supersonic burn-front that is known as detonation.

A detonation typically takes place in less than a millionth of a second. Moreover, the density of the materials during detonation is incredibly high and temperatures reach a few thousand degrees. Such a hostile and fast environment makes it extremely difficult to study detonation with the naked eye.

The mystery of detonation centers on the chemical reactions that take place right after the supersonic shock wave hits the material, a process that lasts only a billionth of a second. To unravel this mystery, scientists at Los Alamos National Laboratory combine computer simulations and innovative experiments that verify what the computers come up with, particularly the simulations of the short-lived chemical bonds formed during detonation.

One-way Los Alamos scientists actually observe and study detonation is to significantly shrink the size of an explosion. The tiny scale enables scientists to drive shock waves into materials so thin it is possible to see through them. Using a laser, researchers send a pulse of light at exactly the moment the shock wave strikes the super-thin material. That lets them observe and record the impact and the resultant chemical reactions.

Such experiments began in 1998. Since then, recording technology advanced enough to enhance the detail of these reactions, enabling scientists to make significant gains in understanding the chemical reactions associated with detonation.

By better understanding how detonation works chemically, scientists will better understand what makes explosives so sensitive. An explosive's sensitivity is related to those first chemical reactions associated with detonation. By unraveling which chemical reactions are the most sensitive, it may be possible to redesign molecules so that they retain the same performance, but are much less sensitive, and thus make the explosive safer and easier to handle.

The Holy Grail of this work is to predict the behavior of explosives. Although there are many other phenomena that are active during the initiation of real explosive materials, identifying the initial chemical reactions is key to predicting their properties and behavior.

With nearly 75 years of work in unraveling detonation, Los Alamos scientists are inching closer to this Holy Grail. Today, the United States alone uses 3.4 billion kilograms of explosives every year – that's 24 pounds per person annually for military and industrial applications. Imagine the variety of new applications once it is possible to produce truly powerful, but easy to handle, controlled and safe explosives.

David S. Moore *is a Los Alamos National Laboratory Fellow and a Fellow of the American Chemical Society studying the behavior of molecules under shock compression in the Los Alamos Shock and Detonation Physics group.*

Some Explosives' Facts

By Berto Jongman
Source: http://nct-magazine.com/december-2018/ibc-threat-assessment/

- Thanks to the efforts of the International Campaign to Ban Landmines (ICBL) the total stockpile of antipersonnel mines worldwide has been reduced from 160 million to about 50 million. It is hoped that the remaining stockpile can be eradicated before 2025.
- In 2017, casualties of landmines/ERW were recorded in 49 countries and resulted in 2,793 dead and 4,431 injured; 87percent of the casualties were civilians and of the civilians, 47 percent were children.
- In 2017, non-state armed groups (NSAGs) produce dimprovised landmines in Afghanistan, Iraq, Myanmar, Nigeria, Pakistan, Syria and Yemen.

Berto Jongman *began his academic career at the Stockholm International Peace Research Institute (SIPRI) in Sweden. From 1982 to 1987 he worked as a researcher at the Polemological Institute of the University of Groningen where he participated in a project on early warning of armed conflict and political violence. In 1987 he moved to the University of Leiden where he acted as data-manager of the Project on Interdisciplinary Research on the Root Causes of Gross Human Rights Violations (PIOOM). In 2002 he moved from academia to government. From early 2002 to late 2012 he worked as a senior terrorism analyst for the Dutch Ministry of Defence. During this period he participated in a number of Advanced Research Working Groups of NATO, e.g. on radicalization, cyber crime/terrorism and the use of Internet by terrorist organizations. A large part of his work at the Ministry involved terrorist threat assessments, including the quarterly assessment of the terrorist threat to the Netherlands for the NCTV. He left the Ministry of Defense in late 2012 and is currently active as a consultant in the area of CBRNe.*

Mauritania 31st country to declare itself mine-free

Source: https://www.apminebanconvention.org/newsroom/press-releases/detail/article/1543500277-mauritania-31st-country-to-declare-itself-mine-free/

Nov 11 – Areas of Mauritania that were under the threat of anti-personnel mines for forty years are now deemed safe.
"I am extremely honoured to declare that after four decades since these weapons were laid and nearly two decades of clearance, Mauritania is free of all known mined zones.
This makes us the 31st State Party to the Anti-Personnel Mine Ban Convention to declare such feat," said Mr. Alioune Ould Menane, Coordinator of Mauritania's humanitarian mine clearance programme for development (pndhd).
The statement came during the Seventeenth Meeting of the States Parties gathered in Geneva until 30 November where the Conference takes stock of challenges remaining to meet the ambition of a world free of anti-personnel mines by 2025.
"Contamination is the residue of the 1976-1978 conflict in Western Sahara which was characterized by erratic laying of anti-personnel mines and a disproportionate number of these weapons used," added Mr. Menane.

"Mauritania became a State Party in 2000 and began the enormous task of clearing hazardous areas soon after. Due to difficulties encountered, Mauritania had to request additional time for clearance and our new deadline was set for 1 January 2021. We are glad we were able to finish our work before that date."

Anti-personnel mines laid threatened, mutilated and killed civilians, were an impediment to development in the north and blocked basic socioeconomic activities such as grazing, fishing, tourism and commerce.

"Landmine contamination and that from other explosive remnants of war were found in three regions of Mauritania in an area of approximately 68 square kilometres which were cleared and returned to the population and administrative authorities.

The Mauritanian Government provided 68% of the overall cost of demining while the international community including France, Germany, Italy, Japan, Luxembourg, Norway, Spain, Sweden, Switzerland, the United States and various United Nations organisations including UNMAS, UNICEF and UNDP supported our efforts by contributing the remaining 38%."

Convention President H.E. Suraya Dalil Ambassador of Afghanistan to Switzerland and UN in Geneva, congratulated Mauritania for achieving this important objective.

"Mauritania should be proud for not giving up on its enterprise to become mine-free. Our ambition of a world free of these weapons by 2025 can only be achieved with increased and cooperative efforts like in Mauritania."

The Convention is the prime humanitarian and disarmament treaty aimed at ending the suffering caused by landmines by prohibiting their use, stockpiling, production and transfer, ensuring their destruction and assisting the victims of these weapons. It was adopted on 18 September 1997 and entered into force on 1 March 1999. Together, the **164 States Parties have destroyed more than 51 million landmines** and 158 States Parties have fulfilled their stockpile destruction obligation.

Inside ISIS' weapons factory where terror fanatics' built suicide belts and car bombs on an industrial scale

Source: https://www.thesun.co.uk/news/7925865/inside-isis-weapons-factory-where-terror-fanatics-built-suicide-belts-and-car-bombs-on-an-industrial-scale/

HEMRL develops device to detect 25 types of explosives

Source: http://idrw.org/hemrl-develops-device-to-detect-25-types-of-explosives/

Dec 15 – A group of scientists from High Energy Materials Research Laboratory (HEMRL) of Defence Research and Development Organisation (DRDO) has developed a device called '**OPX Revilator**', which can detect more than 25 pure explosives as well as trace of explosives mixtures in mud, sand, sugar, salt and diesel oil. "An explosive detection kit,

known as EDK, was earlier developed by HEMRL. Based on the principal of colorimetry, it is capable of detecting eight explosives. Concerted efforts were made to develop a new portable device using optics

and image processing technologies, which resulted in evolving a new device which is OPX Revilator. This device has capability to detect more than 25 explosives," KPS Murthy, HEMRL director, told TOI on Friday. The device is a portable, miniaturised, electronic detector, capable of detecting almost all the explosives used by antisocial elements and in improvised explosive devices (IEDs). **The OPX Revilator is capable of detecting and identifying explosives in solid and liquid phases reliably. It can be operated in laboratory and field conditions.** It is vitally useful for detection and identification of suspect, unknown samples. It can be used under all weather conditions and is sensitive up to the PPM level," Murthy informed. This device is highly useful for homeland security and civil security operations at airports, railway stations, shopping malls, multiplexes, schools, colleges, universities and all strategic locations. "This device can play a crucial role in post-blast analysis. Besides, the armed forces and para military forces can use it for their operational purposes," Murthy said. PK Mehta, director general of armament combat engineering (ACE), said, "The mass production of the product will be done through transfer of technology (ToT)."

Bomb explosion rips through Athens TV station

Source: https://www.euronews.com/2018/12/17/bomb-explosion-rips-through-athens-tv-station

Dec 17 – A bomb explosion ripped through the offices of Greek television station Skai TV in Athens in the early hours of Monday morning.

No injuries were reported, however, the force of the blast caused "extensive damage" to the station, Skai TV reported.

Two other broadcast stations, Zougla.gr and ANT1, said they received anonymous phone calls at 1.45 a.m. local time, warning that a bomb would explode at the Skai TV office in a further 45 minutes.
"The stranger gave a 45-minute margin and said three times that 'it's not a hoax,'" Zougla.gr said.
Police were then rushed to the scene to evacuate the area before the explosion occurred.
Video footage posted to YouTube by Zougla.gr shows the moment of the explosion.
No group took claimed responsibility in the immediate aftermath of the blast, however, police are reportedly looking for several persons who were spotted planting an explosive-filled bag close to the Skai TV building.
Greek anti-terrorism police are investigating the incident.
Olga Gerovasilis, the Greek minister of citizen protection, visited the site of the explosion on Monday morning, making a statement of warning to the perpetrators.
"We are here from the very beginning with the chief of the Greek police for an incident that damages democracy," she said. "But democracy is shielded even more, and, of course, it is not threatened."
Greek MEP Girgos Kurtsos called the explosion a "bomb against democracy."
"The bomb against Skai is a bomb against information and democracy," he wrote on Twitter. "At the beginning of a crucial election period, some people want to shake everything up."
"Our answer is democratic unity. We are all Skai!"

EDITOR'S COMMENTS: Some remarks derived from the recent bomb attack: (1) Complete abence of outer perimeter defense; (2) the combination of the warning given and the time of detonation indicate that it was a meant to kill attack; (3) the Claymont mine similarity indicates advanced knowledge of explosives' dynamics; (4) people responsible for the defense of this target did not think as terrorists when preparing their plans. All these have been said so many times that is really annoying to repeat them addressing deaf people in high places. What if next time there is no warning? What if next time the IED is placed in a spot able to cause destructive direct effects on the skeleton of the building? What if next time is during the day – a rainy or snowey day for example? Who will notice an abandoned bag? It reminds me the main excuse following the deadly wildfire in Athens this summer: "Until now the 4 lanes of the highway always stopped the fire's progress!" Well, this time it was a crown fire that jumped the asphaltos and burned a whole suburb killing 100 people, injured tens of residents and destroyed hundrends of properties. Because the unexpected always happens!

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Iranian Hackers Held US Hospitals, Police Depts for Ransom

Source: https://clarionproject.org/iranian-hackers-hold-us-hospitals-police-depts-for-ransom/

Nov 29 – Iranian hackers have been charged by the U.S. in a cyberattack scheme that shut down the computer systems of U.S. hospital, schools, universities, police departments and utility companies and forced them to pay million to regain control of their servers.

Hackers used ransomware called SamSam to lock files and computer systems, the BBC reported. The systems were only unlocked when the ransom fee was paid.

Two Iranians, Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, hit 230 victims who paid more than a combined $30 million to have their files unlocked. One victim, a hospital in Hollywood, was forced to turn away patients because of the attack.

A number of different government facilities fell victim to the attack in Atlanta, including the police department. A utility company in Atlana was also infected.

The ransomware was also used against facilities in the UK and Canada.

"To execute the SamSam ransomware attack, cyber actors exploit computer network vulnerabilities to gain access and copy the SamSam ransomware into the network," the FBI explained.

"Once in the network, these cyber actors use the SamSam ransomware to gain administrator rights that allow them to take control of a victim's servers and files, without the victim's authorization.

"The cyber actors then demand a ransom be paid in Bitcoin in order for a victim to regain access and control of its own network."

Analysts said the ransomware was not particularly sophisticated. Rather it was effective because the computer systems it was able to infect were poorly maintained and out-of-date.

The ransom money was paid by Bitcoin, a digital currency, to two separate "wallets" (accounts).

The U.S. Treasury imposed sanctions on two other Iranians — Ali Khorashadizadeh and Mohammad Ghorbaniyan – and their Bitcoin accounts for helping the attackers convert the ransom money from Bitcoin into Iranian currency.

The case marks the first time digital currency accounts were put under sanctions. As for the hackers themselves, the FBI stated:
"Although the alleged criminal actors are in Iran and currently out of the reach of US law enforcement, they can be apprehended if they travel, and the United States is exploring other avenues of recourse."

A New Approach to Tackling Cybersecurity

By Sherri Ramsay
Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/a-new-approach-to-tackling-cybersecurity/

Nov 28 – Every day our computers and networks are being attacked. Sometimes it takes the attackers only minutes to selectively target a vulnerability and compromise our systems. Then they are able to quickly exfiltrate our data, while avoiding our defenses. There is an extensive set of attackers – nation-states, criminals, hacktivists, terrorists, and even "lone wolves." Corporate entities and governments no longer have the luxury of only worrying about powerful nation-states. They must be prepared to defend against any of these attackers. The harsh reality is that these attackers collaborate across the spectrum while we continue to operate mostly in independent stovepipes, defending ourselves as if we are each on an island. The cyber threat is asymmetric; the playing field has been leveled.
Every cybersecurity headline serves as a warning that no organization is immune from attacks. So what can we do? Breaking the current cycle will require a fundamental shift in thinking. It will require leadership. Consider the following three-part strategy.
First we need to make our networks defensible; that is, we need to harden our networks. The best place to start is the comprehensive approach offered by the Center of Internet Security's Top 20 Critical Security Controls. The controls are a prioritized set of best practices created to stop the most pervasive and dangerous threats of today. The controls provide organizations with a highly focused set of actions that are implementable, useable, scalable and compliant with global industry and government security requirements. The controls also serve as the foundation for many regulations and compliance networks, including NIST 800-53, ISO 27002, PCI DSS 31, CSA and HIPAA.
Secondly, once our networks are hardened, we must actively defend them. This is a mindset change. We can no longer have system administrators who only "administer" the networks and IT departments who only maintain the networks. We need to change the culture to one of network defense, where everyone who has access to the network has a role to play. The defenders must continuously assess both the network and the behavior of the network, monitoring the network itself and the network traffic for anomalies. And they must be prepared to take immediate actions.
The third part of the strategy is collaboration among and between industry and government, taking a page out of the attackers' playbook. We, the "good guys," must share our relevant information, pool our expertise and connect our responses in a timely manner. We must collaborate both on threat intelligence and mitigations/solutions. In effect, we are crowd-sourcing our cyber defense. By crowd-sourcing in a timely manner, we are more likely to have actionable intelligence giving us the ability to address vulnerabilities and to take responsive actions that will keep attackers from stealing our data.
The oil and natural gas industries have implemented this approach, collaborating to combat the vast cyber threats facing the energy sector. The American Petroleum Institute (API) just released a report that was co-sponsored by the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and the Natural Gas Council, along with all member organizations, demonstrating the industry-wide approach to cybersecurity, and not allowing politics to influence response and actions. The collaboration across energy industries is crucial given the globally critical importance of oil and natural gas. Any cyber attack on the oil and natural gas industry would not only affect the US, but would have an immediate international ripple effect.
The bad guys will continue to exploit our networks as long as we let them. We must (1) harden our networks, making them defensible, (2) actively defend them, and (3) crowd-source both threat information and response actions. It is time for us, the good guys, to change our model and successfully gain the higher ground. Let's use a winning strategy!

Sherri Ramsay *is the former Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC) and a former member of the*

Armed Forces Communications Electronic Administration (AFCEA) Board of Directors. She currently works as a cyber security consultant.

Predicting the impact of hackers, earthquakes – and squirrels – on the power grid

Source: http://www.homelandsecuritynewswire.com/dr20181123-predicting-the-impact-of-hackers-earthquakes-and-squirrels-on-the-power-grid

Nov 23 – What would it take for an entire American city to lose power? What circumstances and failures in the electrical grid's infrastructure would lead to a dramatic, long-term blackout? And what weak points could utility companies invest in to help prevent a catastrophic shutdown?

A three-year project at Lawrence Livermore National Laboratory (LLNL) is attempting to answer those questions using a new algorithm called "Squirrel" to model power outages and enable government agencies and utilities to automatically identify weaknesses in the power grid. Squirrel is part of a three-year Laboratory Directed Research & Development (LDRD) project aimed at determining the risk to the grid from a cyberattack, called the Quantitative Intelligent Adversary Risk Assessment (QIARA). But because Squirrel is "cause agnostic," according to project manager Jovana Helms, it can be used with any kind of threat or hazard, including a malicious hack, earthquake or even squirrels (which often chew into electrical wires and cause outages).

"Squirrel is part of a methodology to assess the risk by identifying critical failures," Helms said. "It solves the inverse problem: for a given consequence of interest it enumerates critical failures that can lead to that consequence. It tells you where to pay attention and how to prioritize your resources. Once you enumerate critical failures you can determine which hazards can cause it and develop mitigations that are hazard agnostic or tailored to a specific hazard."

LLNL notes that Researchers say one of the major challenges in determining risks to the grid is the cascade effect. If one substation fails it could impact the entire grid infrastructure. Using Squirrel, in conjunction with GridDyn, an open source power grid simulator developed at LLNL that models transmission power flow, researchers analyzed what series of actions would have to happen to cause a 500-megawatt load loss on a small grid model. Surprisingly, Helms said, the simulation found 730 critical failures of consequence, including the most susceptible relays and grid components. In about half of all critical failures, one particular relay was consistently part of the enumerated failures. Such insight could be particularly crucial when resources for bolstering grid resiliency are limited, researchers said.

"Let's say our concern is that a bad actor will take one gigawatt of power offline. We're looking at what are the ways that could happen," said principal investigator Meghan McGarry. "Squirrel helps us identify what critical failures would lead to that outcome. What we want to know is what input conditions are required for the load loss of our output. What changes do I have to make to the input to lose that one gigawatt?"

Squirrel, the researchers said, could allow government agencies and public utilities to narrow the list of possible scenarios that could lead to catastrophic failures and determine where to prioritize protection, which would be virtually impossible with manual methods. Using the Lab's high-performance computing capabilities, the algorithms are able to work off the GridDyn model, change various parameters and look at potential solutions that could stave off a massive outage.

"We can start with what we care about and work backward," Helms said. "It eliminates inconsequential scenarios and identifies how a consequence of interest can happen. When we start with the consequence, the first step is to identify critical failures that can cause it. That's where Squirrel comes in. It finds critical failure points in an automated way."

Because the modern grid is much more automated and exposed to the internet, Helms said, it is smarter, but also much more vulnerable to adversaries and malicious hackers. In light of incidents such as the malware-induced grid outage in the Ukraine in 2015 and 2016, the threat of a hack resulting in a blackout is very real, Helms said.

Despite the risk, cybersecurity is costly and time-consuming for utility companies, and currently it isn't humanly possible to dream up all the scenarios that would lead to an undesirable outcome. With natural disasters, researchers can use probability models to get a solid estimate of whether a failure will happen, but intelligent adversaries or hackers wouldn't be probabilistic in nature, they said. But by knowing what to protect, scientists could narrow the list of attack scenarios that would result in a major outage.
A little more than a year into the project, there's still more work to be done before Squirrel can be applied to large-scale systems. LLNL researchers will further develop the modeling capabilities in the coming years and push for more complex, coupled models that can consider combined consequences like communication and power flow, gas and electricity, as well as more complicated transmission and distribution models. Follow-on work could involve collaborating directly with utility companies to identify vulnerabilities and perform risk assessment using actual grid systems from the utilities to create more accurate models. Squirrel has garnered interest from utility partners. If successful, researchers said, Squirrel could help utilities and government agencies increase the resilience of the grid against any type of impactful situation and could later be applied to oil and gas pipelines and transportation.
"Right now, we have a simple model that might have 46 transmission lines that can be switched on or off," McGarry said. "Even in a simplified grid, you're already in a problem space that's 2^{46} possible configurations, which is too big to search with brute force. The main aspect now is developing algorithms for a more intelligent analysis of the space. Our goal is to is to model a 10,000-line system, that would be a useful scale. But even at the level we are now, you can look at it and determine components that are critical to the system."

Biohacker: Meet the people 'hacking' their bodies

Source: https://www.bbc.com/news/technology-46442519

Dec 05 – Biohackers want to make their bodies and brains function better by "hacking" their biology. The BBC's Victoria Derbyshire programme meets the people who are inserting technology under their skin, adopting extreme diets and trying to change their DNA.

Liviu Babitz wants to create new human senses. Touch his chest and you feel his first effort, a vibration every time he faces north. If some animals can already sense direction, why shouldn't we?
He can feel north because of an electronic implant on his chest called the "North Sense". It includes a compass chip, Bluetooth connection and is attached to the skin with two titanium bars like a piercing.
Liviu, 38, is the chief executive of his own company, Cyborgnest, which designed the implant. He sees this as the first step in an entirely in-built navigation system and hopes to end what he calls "generation screen".
"You walk on the street staring at your phone. You want to get somewhere but you have no idea what's happened in the world around you because all you did was stare at the screen on the way," he says.
"Imagine if you didn't need it, you could navigate the world exactly like a bird and you would know exactly where you were all the time - blind people could navigate."

'Biologically fluid'
His invention is highly unusual but actually seems tame in comparison with **Rich Lee**, a 40-year-old cabinet-maker from St George, in the US state of Utah.
Rich is a grinder - a biohacker that does extreme body modification. In his

fingers, he has magnets and two near-field communication (NFC) chips that can be programmed to link to websites or open car doors, among other tasks.
He has a biotherm chip in his forearm, which can constantly monitor body temperature (but are usually used in pets), and headphone implants right in his ears.
He has also attempted "Crispr" - probably the most extreme and controversial kind of biohacking, a technique used by scientists to target and edit your genes.
While scientists are still working out the limits and dangers, Rich is experimenting at home and admits if he gets it wrong, he could kill himself.
"We've got all this genetic engineering knowledge and what I'm backing is the concept of being able to change your genes or get genetic modification like you would get a tattoo," he says.
"I want to see a biologically fluid society where people can just augment these things."
This home biohacking can of course go very badly wrong - Rich pulls up his trouser legs to reveal a selection of scars from implanted shin guards that got so swollen they had to be removed, which he did with pliers and no painkillers.

Concussion
Luke Robert Mason, director of the Virtual Futures organisation, says there is a great deal of excitement around biohacking but "we are a long way from radically altering the human body in the sorts of ways they evangelise".
"What we see today are the first steps by a brave group of pioneers. Today's reality is a lot more experimental (and painful) than is often communicated to the public.
"There is a lot that can be learned from the outcome of their self-experimentation. Some have even argued that biohackers might increasingly be responsible in helping the advancement of wearables and wellness technologies."
There are biohackers working with far less extreme - though still very experimental - methods.
Corina **Ingram-Noehr,** 33, an American events organiser living in Berlin, has a daily ritual involving technology, diet and more than 20 different vitamin supplements to try to keep in peak physical condition.

Next to a cupboard that resembles a chemist's shop, she also has a Power Plate, which vibrates from 30 to 50 times a second to make her exercise more effective. And while vibrating, she uses an infrared light in an attempt to build collagen in her skin.
Corina can also be found walking the freezing cold streets of Berlin with bare legs. She calls this her cheap biohack version of cryotherapy - or cold therapy - and admits the "cops on her street" think it is hilarious.
She discovered biohacking when recovering from a serious concussion that left struggling to speak. Her boss recommended trying medium chain triglycerides (MCT) oil, which helped her "head turn on" and acted as something of a gateway drug for biohacking.
"It opened the floodgates and I was like, 'If this works, this one little thing works so well - like, what else can I do?'
"Biohacking for me is taking control of your own biology. It's taking shortcuts to get to a place that you want to be - so shortcutting your health. That's kind of how I think of it at least."

▶▶ **Read also:** Biohacker Aaron Traywick found dead in a spa

Secure Sensors, Secure Sensors Networks and Best practices against cyber-CBRN attacks

By Barcio F.[1], Volpetti V.[1], Palmerio V.[1].
1. Tekne srl, Contrada Alboreto snc, Ortona (CH);
Presented at the "Workshop on Countering Radiological and Nuclear threats" – 8th November 2018, Rome, Italy

Critical infrastructure, such as airports, seaports, borders, hospitals, or areas with high density of population are sometimes protected with security systems equipped with also CBRN sensors or simple radiation-monitoring devices. This equipment is used to warn, detect and prevents threats related to the detection and usage of unauthorized agents or to the presence of contaminated substances released after incidents. Available on the market, there are modern CBRN sensors with high performance in terms of detection that, in order to maximize their versatility and interconnection capabilities to existing security systems and networks, trade off several weaknesses to cyber-attacks.

As some experts have warned, cyber-attacks on vulnerable sensors and networks could be used to disrupt CBRN facilities, such as chemical plants or nuclear power plants or to spoof the measures coming from monitored areas. Since such facilities are run by computers connected to a larger network, hacking those devices would allow sabotaging the control mechanisms. A terrorist or a saboteur would be able to regulate the flows and the equipment so that it would operate at unsafe levels, turning – in a worst-case scenario – the facility itself into a weapon of mass destruction, or "simply" creating panic situation generating a false emergency situation. Against cyber-CBRN attacks not only large and complex IT infrastructures should be protected but especially sensors and detectors with limited network capabilities. The presentation will address some solutions of secure sensor architectures.

GAO Report on Emerging Threats Highlighted by Dual-Use Technologies

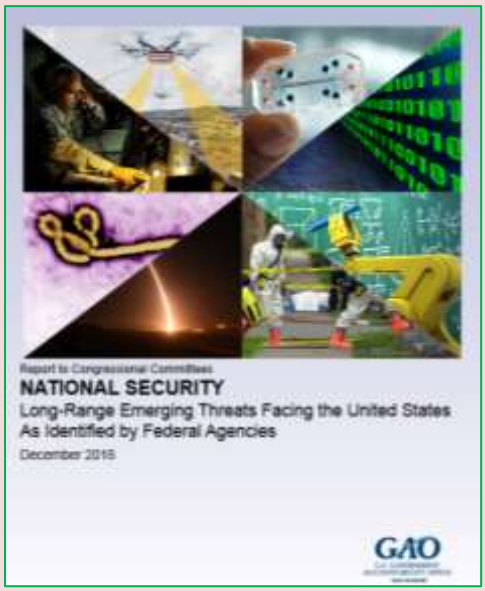
Source: https://www.meritalk.com/articles/gao-report-on-list-of-long-range-emerging-threats-highlighted-by-dual-use-technologies/

Dec 17 – Federal agencies identified 26 long-range emerging threats to U.S. national security, including emerging technologies and foreign cybersecurity threats, a new report by the Government Accountability Office (GAO) found.

To identify the threats, the GAO administered 45 questionnaires across the Department of Defense (DoD), Department of State (State), Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI). The threats identified were those that might occur in approximately five or more years, or during an unknown timeframe. The analysis from the departments broke down the long-term threats into four categories which were: Adversaries' Political and Military Advancements, Dual-Use Technologies, Weapons, and Events and Demographic Changes.

Dual-Use Technologies refers to tech that may be developed by governments or the private sector for innocuous reasons, but in adversarial hands, can pose a risk to national security. The threats identified by the report are artificial intelligence (AI), quantum information science, the Internet of Things (IoT), autonomous and unmanned systems, and biotechnology, and other emerging technologies, such as 3D printing.

Agency officials identified that adversaries may gain increased access to AI, which could then be applied to weapons, as well as quantum communications, which would allow adversaries to develop secure communications that the U.S. could not intercept or decrypt. Quantum computing could also allow adversaries to decrypt information that would allow them to target U.S. personnel and military operations.



The study refers to difficulties that the U.S. could encounter when it comes to cybersecurity as IoT grows, including allowing adversaries to attack commercial and military tech devices. A growing threat of technological advancements in adversarial hands also includes "developing autonomous capabilities that could recognize faces, understand gestures and match voices of U.S. personnel," which could have a negative effect on military operations. Per the report, China, Russia and North Korea are developing Intelligence, Surveillance, Reconnaissance Platforms (ISR) which could allow people or equipment to be tracked globally in near-real time.

The report also identified 3D printing and sophisticated encryption technologies that would allow adversaries to manufacture weapons and impede U.S. efforts to monitor terrorist and criminal activities. The DoD concurred with the findings, while the DHS and ODNI provided additional comments.

Dual-Use Technologies

Artificial Intelligence (AI)» Adversaries could gain increased access to AI through affordable designs used in the commercial industry, and could apply AI to areas such as weapons and technology.

Quantum Information Science» Quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt. Quantum computing may allow adversaries to decrypt information, which could enable them to target U.S. personnel and military operations.

Internet of Things (IoT)» The United States may face difficulties protecting networks and data as IoT grows and traditional approaches for security (e.g., encryption) may no longer effectively protect information. Adversaries could also disrupt IoT-enabled critical infrastructure and devices.

Autonomous and Unmanned Systems» Adversaries are developing autonomous capabilities that could recognize faces, understand gestures, and match voices of U.S. personnel, which could compromise U.S. operations. Unmanned ground, underwater, air, and space vehicles may be used for combat and surveillance.

Biotechnology» Actors—which may include state or non-state entities such as violent extremist organizations and transnational criminal organizations—could alter genes or create DNA to modify plants, animals, and humans. Such biotechnologies could be used to enhance the performance of military personnel. The proliferation of synthetic biology—used to create genetic code that does not exist in nature—may increase the number of actors that can create chemical and biological weapons.

Other Emerging Technologies» Actors may gain access to new technologies previously limited to militaries, such as affordable and sophisticated encryption technologies, which would hinder U.S. efforts to monitor terrorist and criminal activities. Other emerging technologies—such as additive manufacturing (i.e., 3D printing)—may be vulnerable to cyber attacks or be used to manufacture restricted materials, such as weapons.

▶▶ **Read the report at:** https://www.gao.gov/assets/700/695981.pdf

Hackers Launching 480 New Malware Attacks Per Minute, Surge in IoT Device Targeting

By James Cullum

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-launching-480-new-malware-attacks-per-minute-surge-in-iot-device-targeting/

Dec 19 – **An average of 480 new malware attacks occurred per minute between July and September and there was a sharp increase in the number of attacks against Internet of Things devices,** according to a quarterly report by cybersecurity company McAfee.

Ransomware attacks remain popular, with a 45 percent increase over the past four quarters, and new IoT device malware attacks increased 73 percent in the third quarter and 203 percent in the past four quarters. While the number of disclosed incidents targeting the U.S. fell 18 percent, that figure will likely change in the fourth-quarter report in the wake of last week's widespread bomb threats emailed across the country.

"Cybercriminals are very opportunistic in nature," said John Fokker, head of cybercriminal investigations at McAfee. "The cyber threats we face today once began as conversations on hidden forums and grew into products and services available on underground markets. Additionally, the strong brands we see emerging offer a lot to cybercriminals: higher infection rates, and both operational and financial security."

What Hackers Are Talking About

In the third quarter, McAfee researchers found conversations on hacker forums around the following topics:

- User credentials from hacked email accounts
- Skimming credit card details in e-commerce site malware
- Vulnerabilities in RIG, Grandsoft and Fallout, and on GandCrab ransomware
- Global companies that offer logins to computer systems provide "one stop or cybercriminals looking to commit fraud, selling RDP access as well as Social Security numbers, bank details, and online account access."

By the Numbers

According to the report, "cybercriminals have taken notice of the growing volume and lax security of many IoT devices and have begun to focus on them, harnessing thousands of devices to create a mining super-computer. **New malware targeting IoT devices grew 72 percent, with total malware growing 203 percent in the last four quarters. New coin mining malware grew nearly 55 percent, with total malware growing 4,467 percent in the last four quarters."**

McAfee tabulated 215 publicly disclosed security incidents, down 12 percent from the second quarter. While new mobile malware decreased by 24 percent, there was the appearance of the new Fortnite "cheat" and a fake dating app, the latter of which targeted members of the Israel Defense Forces and allowed hackers access to phone calls and a device's location, contacts and photos.

McAfee predicted in a Threat Predictions Report last month that attacks in 2019 will be more advanced than ever before.

*Multimedia journalist **James Cullum** is Managing Editor of Homeland Security Today's Federal Pages. He has reported for over a decade to newspapers, magazines and websites in the D.C. metro area. He excels at finding order in chaotic environments, from slave liberations in South Sudan to the halls of the power in Washington, D.C.*

The Pentagon Thinks Cyber Ops Could Be the Next WMDs

Source: https://www.govexec.com/defense/2018/12/pentagon-thinks-cyber-ops-could-be-next-wmds/153689/

Dec 19 – For years, the phrase "weapons of mass destruction," or WMDs, referred to physical threats: Nuclear bombs, chemical attacks, and biological warfare.

Department of Defense officials, however, are expanding the definition to include offensive cyber operations. They think the threat is so big, that they're seeking ideas from academics, research institutions, and non-profit organizations on how to counter a possible cyber-armageddon. Earlier this week, the Pentagon's Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction, or PASCC, issued a solicitation requesting white papers to help the US prepare for such attacks.

"A new perspective is needed to address this problem," it wrote in the document. "It should include independent organizations not anchored to traditional WMD definitional and doctrinal concepts."

In other words, the Pentagon is looking for out-of-the-box thinkers.

A growing threat

In recent years, Russia, China, North Korea, and a number of violent extremist organizations have launched offensive cyberspace operations against the U.S. PASCC says the cyber attacks are becoming more sophisticated—and a more integral part of US adversaries' military strategy.

PASCC points out that a powerful enough cyberstrike could destroy critical infrastructure, take the financial system offline, or compromise the accuracy of essential military systems. It also noted the potential threat of social media, which it says could be used to spread "false rumors and innuendo designed to strain alliances, divide polities, and undercut public confidence in institutional integrity and social cohesion."

Cyber-nuclear links

The main research question the Pentagon is trying to answer through its solicitation is related to the links between cyber warfare and WMDs. It wants to know how the U.S. adversaries might use cyber operations to make their weapons more lethal, or to erode the U.S.'s WMD defenses.

Cyber attacks can't destroy a city, but they could potentially manipulate a nuclear weapon by hacking into its controls, says Jeffrey Lewis, a WMD expert at the James Martin Center for Nonproliferation Studies in Monterey, California.

"With nuclear weapons, every single piece hinges on the command-and-control system," he says. "Would you try to blow up every single nuclear weapon in Russia, or would you try to shut down the command-and-control system so the orders never got there?"

Is the U.S. ready?

The Pentagon's second question is whether the U.S.'s plans take into account those connections between cyber and nuclear warfare.

The U.S. already incorporated cyber operations into its Nuclear Posture Review, which reflects the Pentagon's official nuclear policy. Earlier this year, the Trump administration created a new category of attack to which US forces could respond with a nuclear strike: "significant non-nuclear strategic attacks." The term is "a euphemism for a cyber attack on our nuclear command-and-control systems," says Lewis.

He believes retaliating against a cyberattack with a nuclear weapon is excessive and dangerous, a point he plans to make in his own submission to the Pentagon's call for papers.

EDITOR'S COMMENT: It seems that the new title of our journal (*C²BRNE Diary*) could proved to be prophetic of the new acronym to include cyber threats.

Cybercrime is on the rise, and Norway is worried

Source: http://www.homelandsecuritynewswire.com/dr20181221-cybercrime-is-on-the-rise-and-norway-is-worried

Dec 21 – As society becomes ever more technology-driven and digitized, electronic crime is rising along with it. **In Norway, cybercrime results in an annual loss of 0.64 percent of Norway's GDP** — this amounts to NOK 19 billion ($2.2 billion) a year, money that does not benefit society.

When investigative reporters from the Norwegian newspaper *Dagens Næringsliv* (DN) scrutinized playback patterns in Tidal's music streaming service, they brought in researchers from the Norwegian University of Science and Technology (NTNU) to work on the case. It's become increasingly common for the university to work with police to solve the growing problem of digital crime.

As society becomes ever more technology-driven and digitized, electronic crime is rising along with it. The Center for Cyber and Information Security (CCIS) works with digital investigations. The center has the largest Nordic professional group in the field and also plays an important role in the European context.

Expertise in digital investigation was exactly what *Dagens Næringsliv* (DN) was looking for when they were examining playback log files of the Norwegian-developed music streaming service Tidal. DN suspected the streaming service of manipulating the playback numbers for the Beyoncé and Kanye West albums "Lemonade" and "The Life of Pablo."

"DN analyzed 1000 users. When NTNU was asked to examine the playback patterns, we felt that this was too small a sample size to draw any conclusions one way or the other," says Ph.D. candidate Jan William Johnsen.

"We had to check if there was any legitimate reason for the playbacks. It might be that DN had by chance selected users who had unusual playback behaviour," he said.
Johnsen was the NTNU Digital Forensics Group member who worked with the analyses of the playback logs.
The NTNU Digital Forensics Group is a specialized academic research group at CCIS.
Gemini, which publishes research news from Norway, notes that Tidal rejects and denies the claims by *Dagens Næringsliv*.

Fraud revealed
The researchers began to analyse the raw data that contained the playback patterns of all Tidal users for a limited period of time. Among other things, the analyses showed that some users had listened to the same song up to 122 times at exactly the same time, if the numbers were accurate. The completed review revealed more than 320 million fake playbacks of the two albums, distributed among 1.7 million user accounts. "We used mostly advanced statistical analysis methods to review the playback patterns of all Tidal users. The analysis work began at the end of January and beginning of February. It was a big job and the final report was delivered to DN in April," says Johnsen. DN published the article on Tidal's suspected fraud in May 2018.
The alleged economic gain in the Tidal case was that the artists Beyoncé and Kanye West had been paid too much money – at the expense of other artists who had music in the streaming service. But even though a lot of money was involved for the artists, it amounts to relatively modest sums in the big picture of cybercrime.

▶▶ **You can read the report here:** Digital Forensics Report for Today's Business

Huge sums
The financial crimes associated with the Internet as a whole involve huge sums.
Studies carried out by other sources, and compiled by the NTNU Digital Forensics Group, show that Norwegian cybercrime results in an annual loss of 0.64 percent of Norway's GDP. **This amounts to NOK 19 billion ($2.2 billion) a year – money that does not benefit society.** "Nineteen billion is a lot of money. These are the only the numbers we're aware of. But in all likelihood the numbers are much bigger," says Professor Katrin Franke, who coordinates the NTNU Digital Forensics Group.

Gearing up against electronic crime
Franke and her colleagues have as their main motivation to see more money benefit the community from their cybercrime work. At the same time, they want to reduce the risk of damage from the failure or misuse of digitization. In order to succeed, this special group is working closely with Norwegian law enforcement and other institutions internationally.

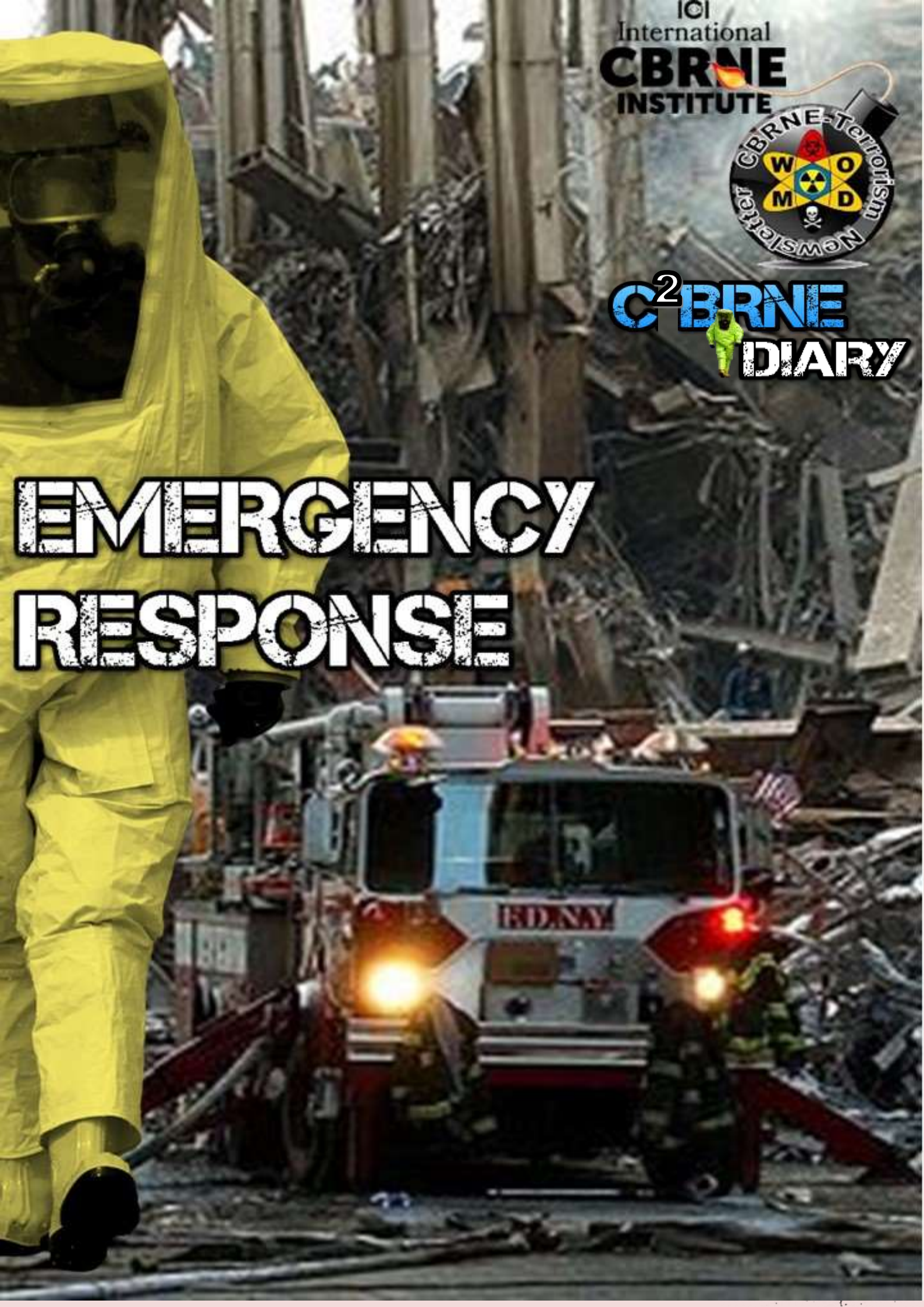
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

NEW CHAPTER AS OF JANUARY 2019


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE

Israeli device that extracts water from the air helps California firefighters quench thirst

By Abigail Klein Leichman

Source: http://www.homelandsecuritynewswire.com/dr20181130-israeli-device-that-extracts-water-from-the-air-helps-california-firefighters-quench-thirst

Nov 30 – An emergency response vehicle (ERV) carrying an innovative Israeli machine that pulls drinking water out of ambient air is on its way to California to provide hydration to police and firefighters dealing with the aftermath of two massive wildfires that have taken at least eighty-seven lives.

The vehicle and the GEN-350 atmospheric water generator were sent by Watergen USA, the American subsidiary of the Israeli company that invented the system.

"The chairman of our company in Israel believes very strongly in humanitarian efforts to assist those who have lost everything in California," said Yehuda Kaploun, president of Watergen USA.

Specifications

- Generates up to 156 gallons (600L) of clean fresh drinking water daily
- Water spouts on both sides of the truck
- Dispenses cold and ambient water
- Storage for emergency medical supplies and provisions
- Installed DC Outlets with battery charging capacity for communication devices
- Dimensions: 8' x 24' x 8.75' (2.4m x 7.3m x 2.7m)

Available Add-Ons:

- 260-390 gallon (1000-1500L) water reservoir
- 130 gallon (500L) fuel tank for week long operation
- Emergency Lighting
- Custom logo or paint
- WIFI

Watergen USA CEO Ed Russo said aid workers can serve for longer periods of time if they have adequate drinking water, and the GEN-350 reduces the number of plastic bottles needed on scene.

The 800-kilogram (1,763-pound) Watergen GEN-350 can produce up to 156 gallons (600 liters) of water per day from the ambient air. The unit has an internal water-treatment system and needs no infrastructure to operate except electricity, which is supplied from a generator and charging stations on the ERV.

The U.S. Department of Health and Human Services has declared a public health emergency in the state of California.

Watergen USA has launched a Go Fund Me campaign to bring an additional ERV and a GEN-350 to California.

Watergen USA's ERV previously brought a GEN-350 unit to Florida following Hurricane Michael in October. The company partnered with World Central Kitchen, an organization of chefs working to fight hunger and poverty, to prepare food for hurricane victims.

"Watergen USA was pleased to partner with some world-class chefs to assist in the rescue efforts to provide people with gourmet meals using the world's best chefs and using the world's best water," said Kaploun.

***Abigail Klein Leichman** is a writer and associate editor at ISRAEL21c.*

Worst-Case Scenarios: Sudden & Total Isolation

By Joseph Cahill

Source: https://www.domesticpreparedness.com/healthcare/worst-case-scenarios-sudden-total-isolation/

Sept 04 – Cornwall, New York, is a mid-sized town in the Hudson River Valley, served by a volunteer ambulance corps and two volunteer fire departments. During Hurricane Irene in 2011, a critically important bridge washed out and most major roads in the area were flooded, leaving the town separated from the vital resources and services essential to any community. The Cornwall situation played out over and over again throughout the entire northeastern United States, in areas ranging in size from single homes to crowded neighborhoods, and from small towns to medium-sized and larger cities.

Key Goal: Maintaining Access to Emergency Services

From the perspective of EMS (Emergency Medical Services) teams and individual volunteers, this sudden isolation meant not only that local residents were unable to reach aid stations, shopping malls, and other community centers, but also that hurricane victims, and others requiring urgent medical care, could not be quickly and safely transported to hospitals or other medical facilities.

In some situations when the local transportation infrastructure is impacted, *no* medical facility is accessible. In other situations, though, medical facilities may be accessible and functioning but are not equipped to provide full-scale responses. Although many community hospitals have on hand the medical resources needed to cope with a flood or other natural disaster, other facilities – particularly those in remote or sparsely populated areas – are more susceptible to "isolation" risks than the more fully equipped facilities in larger and less remote communities.

Under those circumstances, outpatient clinics, urgent care centers, and other non-emergency facilities must do the best they can; but there are certain risks involved. These facilities have the ability to treat and stabilize patients, for example, but they usually do not have the same quantity or variety of medical resources that community hospitals possess. This means that critically ill or injured patients must be transported – by a medevac helicopter, for example – to other facilities for the more complicated/advanced care they might need. Use of that option shortens the transport time, but also entails other risks, particularly in difficult weather conditions.

Flooding is not the only hazard that may isolate a community immediately after a natural or manmade incident. Any factor that disrupts the efficient functioning of one or more of a community's "lifeline" sectors – energy, water, communications, transportation, or emergency services – could create what for all practical purposes would be a virtual island. For that reason alone, it is important to: (a) fully evaluate each facility in a given jurisdiction during the planning process; and (b) use the findings to determine how the loss of services from each lifeline sector might adversely affect the response and recovery phases of an incident.

Plan for the Worst, Hope for the Best

Even in towns or other communities that do not have the geography or topography conducive to being almost literally cut off from the outside world, emergency response agencies must have a useful planning tool for identifying all potential risks and developing the contingency plans needed to cope with various incident scenarios. In larger jurisdictions, this "thought exercise" could be applied when considering smaller areas within the jurisdictions that lend themselves to being cut off. By postulating a scenario of total isolation from the outside world – including such resources as hospitals and/or mutual-aid centers – emergency managers can create effective action plans robust enough to respond when either a single resource or multiple resources are lost.

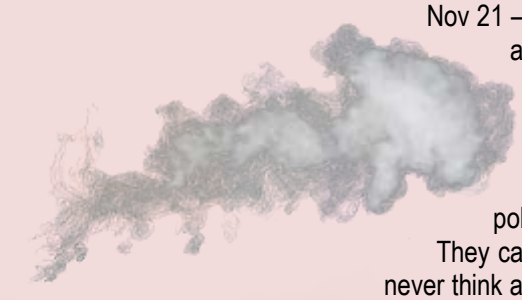
In the late 1990s, the New York City Fire Department deployed spare paramedic equipment sets by following, in part, this same type of analysis. The Department deployed the equipment by using several factors based not on population or call volume but, rather, on the likelihood that a particular area could become isolated, and/or one of several bridges was lost or at least temporarily not accessible.
By involving other agencies in the planning process, emergency managers can both gather and evaluate the information needed to develop mutually acceptable interagency agreements and procedures. For example, the Department of Public Works may use the information to determine the priority levels required for opening specific routes based on such factors as: (a) the usefulness of each route; (b) the ease of access available to emergency vehicles; and/or (c) the relative isolation of the various areas served by each route.
Isolation is one risk that planners must evaluate, and a scenario they should plan for even if it seems unlikely. Although most U.S. communities may never experience the "island-effect" that Cornwall lived through, planning for such worst-case situations can nonetheless improve the overall response effort needed when any or all resources are no longer fully available.

Joseph Cahill *is the Director of Medicolegal Investigations for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.*

Wildfire smoke is becoming a nationwide health threat

By Richard E. Peltier

Source: http://www.homelandsecuritynewswire.com/dr20181121-wildfire-smoke-is-becoming-a-nationwide-health-threat



Nov 21 – The impacts of recent forest fires in California reach well beyond the burned areas. Smoke from the Camp Fire created hazardous air quality conditions in San Francisco, more than 170 miles to the southwest – but it didn't stop there. Cross-country winds carried it across the United States, creating hazy conditions in locations as far east as Philadelphia.

As an air pollution exposure scientist, I worry about the extreme levels of air pollution that rise from these fires and affect many people across great distances. They can create unhealthy conditions in far-flung locations where residents probably never think about wildfires. But since major wildfires are becoming increasingly common, I believe it is important for all Americans to know some basics about smoke hazards.

A complex and unpredictable threat

Forest fires do not discriminate about what they burn. Along with woody materials from forests and homes, they consume homes' contents, which may contain plastics, petroleum products, chemicals and metals. This produces thick plumes of smoke that contains very large quantities of particles and gases. Many of these airborne chemicals are known to be quite toxic to humans.
Smoke plumes travel great distances, affecting communities hundreds of miles away. Winds tend to move from west to east across North America and carry these pollutants with them. Sometimes, depending on local weather conditions, the pollutants can be lifted up to high altitudes where wind speeds are faster and transported very quickly across the country. The pollutants can then descend back to the ground in locations far away from the fires, affecting everyone in their path.
Relatively few studies have analyzed broad public health impacts from wood smoke. Agencies such as the National Institute of Environmental Health Sciences are funding some

research on this issue, but it can take a long time to produce convincing science, especially on subjects that are so unpredictable.

We do know that this kind of smoke contains chemicals that are toxic, including polycyclic aromatic hydrocarbons, heavy metals, black carbon (soot), acids and oxidizing compounds. Exposure to some of these compounds can lead to lung irritation, cancer, hypertension, cardiovascular disease and even death. We know this because researchers have studied smoke exposure in firefighters for many years, and it's likely that the risks also apply to people who aren't firefighters.

When the smoke moves in

Research has shown that many health effects from air pollution occur well after exposure has occurred. Sometimes these problems occur within a few hours, but in other cases it can be days or weeks later. This means that people may not feel the impacts of smoke inhalation until well after the smoke clears.

The most effective strategy is to limit exposure to poor-quality air through steps such as avoiding the outdoors when possible, closing windows and doors, and running central heat or air conditioning systems, which for the most part recirculate indoor air. For outdoor protection, the best option is an N95 facemask, which is designed to fit snugly and filter out very small particles. Inexpensive cloth masks do not provide effective protection.

However, it can be difficult to achieve a good fit with N95 masks, and these masks are not very effective at removing toxic gases from smoke, which easily pass through the filter material. Avoiding exposure in the first place is the best strategy.

Communities that are frequently exposed to wildfire smoke should consider creating locations where they can provide high-quality air filtration, such as a school or community center. These sites could offer safer conditions for people who are especially vulnerable to air pollution, such as children, the elderly and people with respiratory ailments, in the same way that cities set up heating and cooling centers during extreme weather conditions.

Many factors appear to be increasing the number and scale of wildfires, including development patterns and forest management practices. But the biggest driver is likely to be climate change, which is making ecosystems hotter and drier. This suggests that all Americans, wherever they live, will need to become more aware of wildfires and their long-range health effects.

Richard E. Peltier *is Associate Professor of Environmental Health Sciences, University of Massachusetts Amherst.*

What Gets Measured, Gets Done - The Long and Winding Road of Preparedness Measurement

By Timothy Beres

Source: https://www.domesticpreparedness.com/resilience/what-gets-measured-gets-done-the-long-and-winding-road-of-preparedness-measurement/

December 2009 – For the state and local organizations that have been involved in federal efforts, or efforts of their own, to measure preparedness, that task is not taken lightly. There have been many top-down federally directed efforts to measure preparedness. Most of these initiated at the direction of Congress or the Government Accountability Office (GAO) in an effort to determine the nation's current state of preparedness, the gaps in that preparedness, and the effectiveness of federally funded preparedness programs.

These efforts are already underway, because those who have been given the responsibility for preparedness programs care about the preparedness of the nation and want to improve upon those programs and preparedness efforts, rather than imposing unreasonable work requirements on those participating in preparedness assessment.

However, that does not mean that these efforts have not been burdensome. The measurement pendulum has taken great swings between *what* should be assessed and *how* to assess (subjectivity vs. objectivity), and the result has been a half dozen or so approaches that: (1) have yielded very little in answering the question "How prepared is the nation?"; but (2) have also produced a great deal of frustration. The same frustration is felt by those –

from Congress to the Executive Branch and from the police station to the firehouse – who are most involved in the assessment process. In short, although a great amount of effort has been expended, a comprehensive report on National Homeland Security Preparedness has still not resulted from these assessment efforts.

In addition, although there may be problems with the data itself, analysis efforts have also been lacking. In fact, the analytic efforts to provide something useful to the federal government, and back to the states and local communities involved, have only just begun. Even if all the data provided was reliable, the current system of self assessment is a static process that is not comprehensive by any definition and therefore provides only a brief snapshot – which quickly fades – of the current state of preparedness.

The What, How, and Why of Measurement Parameters

However, the field of preparedness measurement is rapidly evolving. And, while self assessment will continue to be a part of the measurement framework, other ideas and methods are being developed to tackle the seemingly intractable problems of what to assess, and how.

Many current discussions are grounded in three simple principles: (1) measure only what really matters; (2) what is measured should be just as relevant and meaningful to operational personnel as it is to political leaders; and (3) *how* it is measured should lead to an understanding of predicted performance, not simply produce an exhaustive inventory of operational assets and activities undertaken.

What adherence to these principles should lead to is a preparedness assessment process that does not attempt to measure everything? Measurement should be focused primarily, if not exclusively, on the critical enabling capabilities and, within that broad field, only the key indicators of performance – with special focus on those areas that are not regularly used or practiced.

Utilizing risk analysis can help apply focus to determining the specific critical capabilities that an area may need. However, it seems clear that, without being able to demonstrate certain general capabilities as defined in the Target Capabilities List (TCL) – e.g., in incident management, planning, communications, and information-sharing – then having specific site- and/or team-based capabilities may not matter. If sophisticated teams that are involved in a large-scale response are unable to communicate, they also may be unable to effectively operate during the incident. Efforts therefore should be focused on reaching consensus in determining the subset of "make it or break it" capabilities that are needed by the nation and that will, as a minimum, have jurisdictions prepared *not* to fail. Tightly focusing measurement on the most critical activities creates an opportunity for a comprehensive national approach to preparedness measurement that is not only meaningful but manageable as well.

Three Approaches, Capability Models, and Meaningful Evaluations

Comprehensive preparedness measurement should take advantage of three approaches: self assessments; quantitative measurement; and performance-based evaluations. The first approach, self assessments, can generate very important and useful data because the information developed comes from those who know their individual circumstances the best. It should be recognized, though, that there have been several problems with self assessments in the past – overly burdensome tools, for example, as well as tight time frames, unreliable technology, inadequate guidance, and "gaming" of the assessments – all of which resulted in, at best, questionable results. In order for reliable, accurate, and useful data to be generated, capability assessments must, first of all, be meaningful to those being assessed. The goal of future self-assessments and the collection of data must therefore be to support operational planning and programmatic decision-making at the level of those who are being assessed.

Quantitative capability models can be developed both to assist with planning and resource allocation and to help determine capability gaps. Such models can provide an independent baseline estimate – based upon national averages, demographic information, and risk criteria – of the levels of capability required for a given jurisdiction. The same models can use quantitative data to inform investment decisions: (a) by determining the scalability of a capability to a given scenario, thus generating capability calculators; and (b) by estimating the full life-cycle costs of achieving a given level of a particular capability,identifying capability gains from investments, and optimizing the placement of new operational teams and capacity at all levels.

The evaluation of exercises and real-world events should be used to assess actual performance. An effective performance-testing program at the national level would not only gather consistent data but also analyze after-action reports to determine what happened (and why it happened), and compare findings across different exercises and events to

identify trends and common points of failure. Moreover, it would assess holistically how capabilities integrate both horizontally and vertically. Past experience – Hurricane Katrina is perhaps the best example – has shown that the national response system frequently breaks down in complex events at the horizontal and vertical seams between capabilities. Consequently, performance evaluations must include the analysis not only of individual capabilities themselves but also of the connections across capabilities as a portfolio. All of this should be done not in an effort to judge or cast blame but, rather, to understand priority issues as quickly and directly as possible.

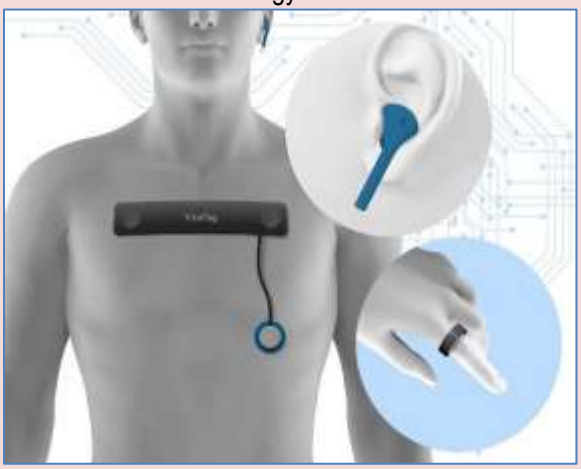
Without a comprehensive approach for measuring preparedness, the nation will continue to struggle to understand the current state of preparedness across all regions, and for all hazards. Some areas may over-prepare relative to their true risk-based capability needs; others may under-prepare; and still others may prepare for the wrong things altogether.

***Timothy Beres**, vice president, CNA Safety and Security, is responsible for that organization's safety and security research and analysis program in the fields of public safety, criminal justice, homeland security, emergency management, and emergency public health. Prior to joining CNA he held senior leadership positions in the Department of Homeland Security and the Department of Justice. He is responsible for, among other accomplishments: development of the first risked-based preparedness grant program - the Urban Areas Security Initiative (UASI); establishing the first communications and terrorism prevention technical assistance programs for state and local jurisdictions; developing a national Weapons of Mass Destruction training program for state and local first responders; managing establishment of the Center for Homeland Defense and Security at the Naval Post Graduate School; initial implementation of Homeland Security Presidential Directive 8 (HSPD-8); and creation of the first transit security grant program.*

VitalTag to give vital information in mass casualty incidents

Source: http://www.homelandsecuritynewswire.com/dr20181213-vitaltag-to-give-vital-information-in-mass-casualty-incidents

Dec 13 – When mass casualty incidents occur — shootings, earthquakes, multiple car pile ups — first responders can easily be overwhelmed by the sheer number of victims. When every second counts, monitoring all the victims in a chaotic situation can be difficult. Researchers at the U.S. Department of Energy's Pacific Northwest National Laboratory developed a stick-on sensor that measures and tracks a patient's vital signs to help first responders quickly triage, treat and transport the injured.



The patent-pending **VitalTag is a low-cost suite of sensors that detects, monitors and wirelessly transmits vital signs, including blood pressure, heart rate, respiration rate and other metrics such as blood oxygen levels, shock index and data from a single-lead electrocardiogram.**

VitalTag adheres to a patient's sternum and connects seamlessly via Wi-Fi to securely transmit patient data to a mobile device or laptop in real time. Responders can view each patient's medical status and location on an incident map. And, should vital signs change for the worse, the system can also send an alert. This comprehensive view could enable emergency medical technicians and paramedics to tend to more patients faster, armed with more detail than ever before.

PNNL notes that VitalTag was developed as part of a broad Department of Homeland Security Science and Technology Directorate program called the Responder Technology Alliance. RTA, which is managed by PNNL, helps to advance the development of emerging technologies critical to the responder community.

"First responders told us they need a device to continuously monitor patients in demanding environmental conditions," said Grant Tietje, a former first responder who manages RTA at PNNL. "VitalTag provides a wearable, cost-effective health monitoring solution."

VitalTag consolidates expensive and bulky emergency response equipment into a wearable medical device that allows simultaneous monitoring of multiple patients, enhancing responders' situational awareness and improving resource management.

PNNL data scientist Luke Gosink and his team worked to embed intelligence into the monitoring devices. They developed machine learning algorithms to interact with sensor hardware and created an intuitive user interface that helps first responder do more.

"It is a resource multiplier," said Gosink. "Yes, ambulances have these types of equipment but usually only a few of each. With VitalTag, many more patients can be monitored simultaneously and continuously. More situational awareness, like that achieved with VitalTag, can result in better patient outcomes."

PNNL is partnering with the occupational medicine company AnovaWorks to validate the efficacy of the prototype. AnovaWorks, which operates employer-based health care clinics including one at PNNL, will conduct a limited evaluation assessment to compare and evaluate whether measurements from the monitoring sticker are consistent with the readings taken in a clinical setting using standard medical devices.

The data will support discussions with potential commercial partners on the feasibility and utility of the patient monitoring sticker. PNNL is looking for partners interested in licensing the patent-pending technology. The VitalTag technology is versatile and adaptable to a wide-range of applications including monitoring:

- high-performance athletes during training
- military warfighters
- medically vulnerable populations during evacuations of healthcare facilities
- veterinary medicine.

PNNL notes that this is a fielded prototype technology that has not yet been approved by the FDA and is not commercially available.

Mass Gathering Medicine: Lessons from the Hajj

By Sonali Ganguly, MD, MA and Matt S. Friedman, MD

Source: http://epmonthly.com/article/mass-gathering-medicine-lessons-from-the-hajj/

2015 – This year's Hajj – the annual Islamic pilgrimage to Mecca –has been making headlines as one of the deadliest in history. Between a crane collapse and a deadly stampede, there were over 800 traumatic deaths before the end of September. Already one of the most studied mass-gatherings in the world, this year's events put special focus on the need for advanced mass gathering preparedness. Here are a few lessons that we've learned already.

Every year, more mass gatherings occur throughout the United States and emergency physicians (EPs) are often at the front lines of response to these events. Mass Gathering Medicine (MGM) is the field of study that analyzes the management of these events in order

to employ strategies to effectively enhance the delivery of health care. And it's a good thing, because poorly managed mass gatherings can have significant morbidity and mortality. In the past, inadequate crowd control has resulted in deadly stampedes and sub-par sanitation facilities have caused mass outbreaks of communicable disease [1,2,3].

Given this increasing reality, emergency physicians need to ground themselves in MGM principles and be prepared to take an active role to ensure adequate preparation and staffing of mass gatherings within their facility's catchment area.

Interestingly, much of the MGM literature is based on international data. Examining strategies implemented in countries with extensive experience in mass gatherings can provide essential framework for mass gatherings here in the US. The Hajj in Saudi Arabia is an annual five-day gathering that amasses millions of pilgrims in and around Mecca. Hajj often takes place in punishing heat, with many pilgrims arriving by foot, so the potential for illness and injury is great. What makes the Hajj so unique for physicians is that it is the oldest studied mass gathering, with reports on medical care and disease outbreaks appearing in the medical literature since the 1800s [4].

The Hajj (Arabic for 'pilgrimage') is the fifth pillar of Islam and is considered obligatory for those with the financial and physical means to complete it. The number of pilgrims completing the journey between five holy sites in Islam has grown steadily since its inception over thirteen hundred years ago [5]. Travelers perform this pilgrimage during the final month of the Islamic (lunar) calendar, traveling to a new site each day over several kilometers of desert. Travel by bus or rail is possible, however demand overwhelms capacity each year and many travelers undertake the pilgrimage on foot [6].

Since pilgrims originate from almost 200 nations, health care organizers have to employ a robust surveillance system with frequent updates. After deadly outbreaks of meningococcemia during the 2000 Hajj, health organizers devoted significant resources to surveilling communicable disease threats, which could have devastating impacts on the crowded confines of the Hajj. From this surveillance arose a requirement of meningococcal, yellow fever, and polio vaccinations for pilgrims who travel from countries where these diseases are prevalent [7]. The Hajj is the only mass gathering that requires vaccinations, though certain countries require yellow fever vaccinations in any travelers from endemic regions.

Recent global public health threats such as MERS-CoV and Ebola have tested Saudi Arabia's surveillance systems. Hajj authorities responded to early MERS-CoV outbreak mortality by aggressively advising vulnerable populations to avoid the Hajj and disseminating information about hand hygiene, masks, and isolation for persons with respiratory symptoms [6,7]. Two MERS-CoV hospital admissions and zero associated deaths were reported amongst Hajj visitors during the 2014 pilgrimage [8]. During the recent Ebola epidemic in 2014, the Hajj health ministries prohibited travel from Liberia, Sierra Leone, and Guinea – the three nations from where the vast majority of disease burden originated [9]. No cases of Ebola were reported during the 2014 Hajj.

The Hajj's sophisticated healthcare system is overseen by a dedicated subsection of the Saudi Arabian Ministry of Health. This includes 25 hospitals, more than a 100 health centers including emergency health centers, and 100 ambulances. A comprehensive public health surveillance system enabled the Hajj organizers to recognize heat stroke as a significant cause of morbidity, which was noticeably reduced after cold water, sun cover, and air misters were provided along pilgrimage routes [6,10,11].

Other incidents provided the impetus for Hajj organizers to redesign portions of the pilgrimage to minimize risk to pilgrims. In 1975 and 1997, cooking stoves caused tent colony fires that resulted in hundreds of deaths and thousands of injuries. All tents have subsequently been replaced with a permanent city of fireproof tents designed and used solely for the Hajj, complete with a fire-suppression system. Personal tents and cooking within tents are no longer permitted [6].

Stampedes, in particular, have been the cause of multiple mass casualty incidents (MCIs) at the Hajj resulting in thousands of fatalities. In 1990, 1,426 pilgrims were killed in a tunnel stampede at Mecca. Hajj attendance has steadily grown, and multiple stampedes in subsequent years have resulted in hundreds more deaths. In response, event organizers arranged for camera installations along the Hajj route. Information gleaned from this surveillance led to the construction of a multi-story bridge that can carry millions of pilgrims simultaneously, as well as a redesign of structures and spaces integral to Hajj rituals [12]. Crowd control has vastly improved with a reduction of crowd convergence points through enforcement of unidirectional flow, staggered entry, and multiple entry/exit points. Since these measures have been enacted, no stampedes have been reported. However, just last month in September 2015, a large crane collapsed on the Grand Mosque

in Mecca killing 107 people and wounding scores more. A severe rainstorm and strong winds are believed to have caused the collapse. These tragedies underscore the vital role of medical preparedness to efficiently respond to the injured and improve system-based errors learned from these MCIs.

While masses typically gather in the US for different purposes than the religious mass gathering discussed here, with radically different psychosocial factors at play [14], the Hajj remains the best studied and arguably best MGM preparedness effort in the world. Studies reveal that the challenges faced by the Hajj are in fact the same challenges facing mass gatherings the world over: crowd control, ingress/egress and event site access, control of infectious disease transmission, fire/stampede prevention, medical preparedness and situational response [15].

Here are a few key lessons that American physicians can learn from this, the most-studied mass gathering in history, on how to enhance MGM preparedness efforts in the United States:

- All aspects of preparedness affect medical usage rates (MUR). Without adequate crowd control, safety and security protocols (including fire prevention), waste and sanitation facilities, potable drinking water/food, and good communication to attendees and between staff members, MCIs can occur that will overwhelm healthcare resources.
  – Utilize harm-reduction public service announcements (PSA) via multiple avenues, including websites and social media, to communicate vital information to attendees.
- Mass gatherings have a high incidence of environment-specific medical challenges, from zoonotic and vector-borne diseases to heat exhaustion. EPs should be knowledgeable about environmental challenges unique to their catchment area, and suggest simple preventative measures for these.
  – Consider provision of sun cover, distribution of free potable water, and frequent watering of event grounds, especially cement, when attendees are exposed to hot, humid environments for prolonged periods of time.
  – Be aware of potential zoonoses and vector-borne diseases in the area and push for protection of bathing/cooking/drinking water sources from contamination, removal of standing water, and liberal pesticide use to ensure adequate vector control [16].
- In planning the layout of event grounds and resources, consider the distribution of attendees over the course of the event and organize necessary facilities accordingly.
  – The geographic positioning of medical facilities and providers is vital, and suboptimal positioning can have significant deleterious effects. Pay special attention to ensuring clear pathways of ingress and egress for first responders/ambulances as this has repeatedly proven a challenge for mass gatherings of all types.
  – Crowd control is of critical importance, as trauma from stampedes is a significant cause of MCIs and increases high acuity MUR. Reduce points of crowd convergence by creating spaces with unidirectional flow, staggered entry, and dedicated entry and exit points. Exit points should be twice as large as entry points.
- Medical complaints are largely low acuity at mass gatherings, with a small percentage of high acuity, resource intensive utilization. Prepare accordingly.
- Multiple critical care transporting units are likely unnecessary. While access to aeromedical transport may be essential, the majority of providers will treat low acuity conditions such as musculoskeletal complaints, lacerations, asthma, and urinary tract infections [17].
- Event organizers and local health officials should invest time and resources in collecting data from their event to aid preparation for future events and implementing a surveillance system to rapidly identify adverse health events.
- Most importantly, advocate for your healthcare organization, your community, and the potential patients resulting from a nearby mass gathering. Seek out event organizers and ensure that mass gathering medicine preparedness is optimal. Your ED will likely be overwhelmed if it's not!
  – Do not first become aware of a nearby mass gathering when the injured patients start to arrive in your ED.

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

Sonali Ganguly, MD, MA *is a senior EM resident at Maimonides Medical Center. She has staffed multiple EDM festivals and other mass gatherings.*

Matt S. Friedman, MD *is a board-certified EMS and Emergency Medicine physician. He completed an EMS fellowship with the Fire Department City of New York (FDNY). He is currently the Associate Medical Director of Prehospital Care at Maimonides Medical Center in Brooklyn, NY. He also serves as the Lead House Physician for Yankee Stadium, Madison Square Garden and the US Open. Dr. Friedman is the acting medical director for numerous annual mass gatherings and large music festivals in NYC.*

Analyzing Emergency Evacuation Strategies for Mass Gatherings using Crowd Simulation and Analysis framework: Hajj Scenario

Imran Mahmood
Center for Research in Modeling, Simulation & Vision (Crimson), National University of Sciences and Technology, Pakistan
imran.mahmood@seecs.edu.pk

Muhammad Haris
Center for Research in Modeling, Simulation & Vision (Crimson) National University of Sciences and Technology, Pakistan

Hossam Sarjoughian
Arizona Center for Integrative Modeling & Simulation (ACIMS), School of Computing, Information, and Decision Systems Engineering, Arizona State University, USA

Source: https://www.anylogic.com/upload/iblock/c65/c65a320d2c830d8e9d176e12b770f297.pdf

A mass gathering, as defined by World Health Organization is: "A planned or unplanned event at a specific location, attended by a huge number of people for a common purpose. This number is sufficient enough to strain the planning and response resources of the community, state or a nation hosting that event".

The increasing influx of large numbers of people to mass gathering events may give rise to complex disastrous situations, thus require extreme planning and operational support for Public Safety & Security (PSS) preparedness by the organizers of mass gatherings or the governmental entities in general.

Hajj is one of the largest mass gatherings, where about 3 million Muslims gather in Makkah (Saudi Arabia), from over 140 countries, each year for a minimum of five days and up to 40 days. Following an exponential rise in the past decade, Makkah becomes the site of extreme crowd densities with huge inflow of crowd and quite vulnerable to serious disasters including stampede, accidents, construction failures, fires and communicable hazards. Factors that magnify these risks include: extended stays at Hajj sites, extreme heat, densities above 6 or 7 persons per square meter, individuals' inability to move at concentrated regions and jostle to find breath, groups swept along in waves, struggling to avoid falling and being trampled, thus hundreds of deaths can occur as a result. Moreover, the advanced age of many pilgrims with premorbid health status adds to the mortality risks. In the past, these disasters took place many times during Hajj. In July 1990, 1426 people were killed in a crowd crush as a result of improper crowd control. In 1997, 343 pilgrims were killed and 1,500 injured in a fire incident. Similarly, in 2006, 346 deaths took place in stampede in Mina valley while throwing stones at pillars. In 2015, crane fell in the courtyard of Masjid-Al-Haram (grand mosque) causing a total of 512 casualties. Again, in September 2015 more than 2000 pilgrims were crushed due to stampede at Mina.

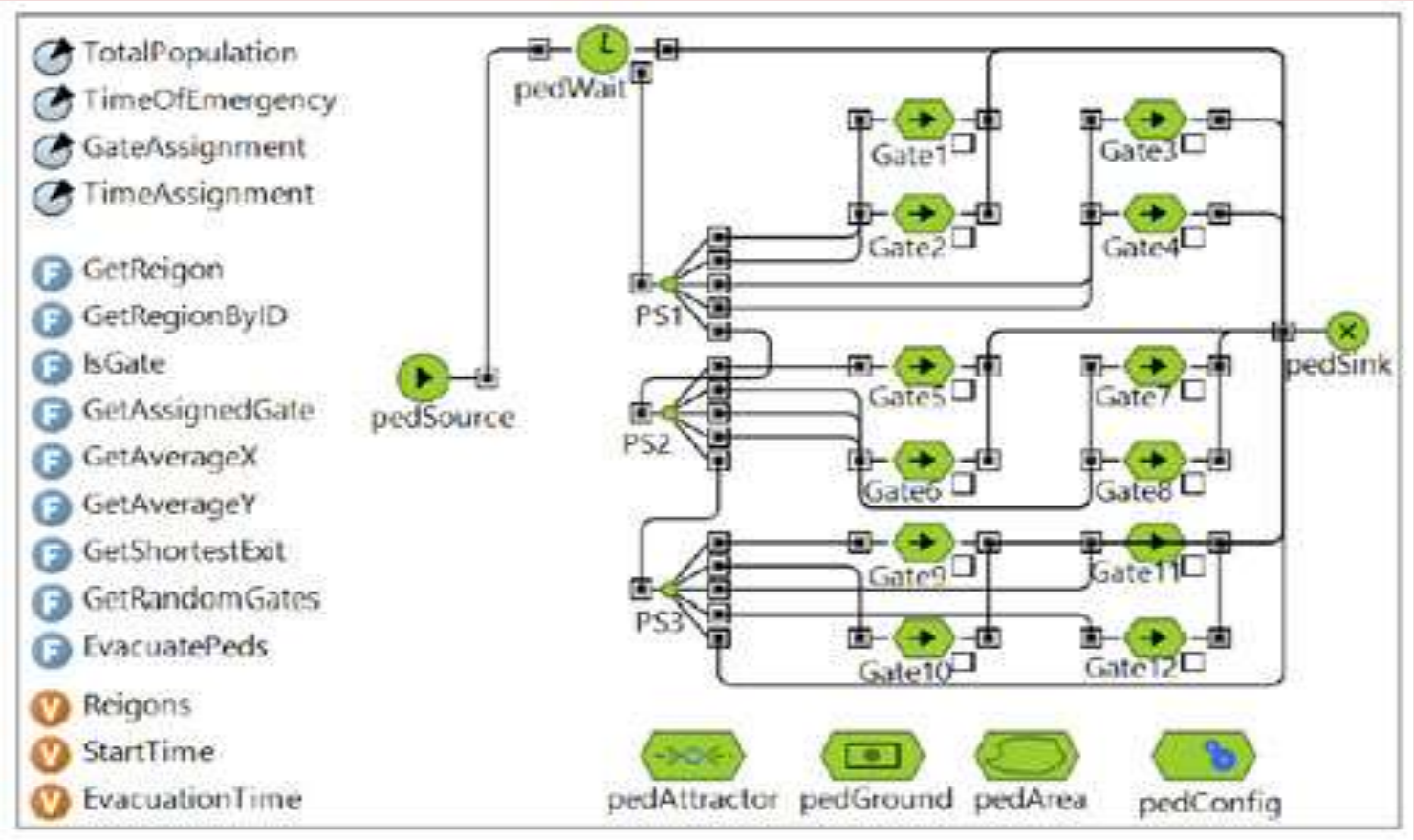
The disasters can be prevented through proper crowd management & control strategies and is usually expressed as a governmental responsibility under PSS departments. An effective PSS infrastructure for crowd management & control consists of the following key components:

- Monitoring;
- Mitigation;
- Preparedness & Incidence Response;
- Recovery.

Monitoring involves a continuous process of observing real-world activities and supervising the crowd flow. Mitigation concerns preemptively preventing possible emergencies, planning exit points & escape routes etc. Preparedness deals with the timely preparations to handle dangerous situations such as firefighting, construction failures, or natural disasters. Incidence response involves timely rescue operations, emergency evacuations, crowd management, shelter and medical services during crisis. Recovery deal with the actions taken to return to a normal state. An efficient PSS infrastructure relies on smart planning and decision support systems that can

provide quick and accurate identification and assessment of optimal strategies to be used for a real-world situation under a specific context.

With the advent of modern Modeling and Simulation (M&S) paradigms, there has been an increasing trend in the use of Modeling and Simulation in PSS planning and decision support. Crowd dynamics



simulation models are now becoming useful in replicating scenarios of safety/mission critical systems in a risk-free, low cost, time independent and harmless experimental environment where modelers can exhaust trials of different nature to gain the insights of the system, compare different alternatives or to find best design parameters. Crowd modeling and simulation plays a vital role in solving evacuation problems. Modeling crowd behavior and the movement of each individual in a crowd can help reduce the number of deaths in a building or a public area. The population is growing exponentially which is making public places busier and causing crowd related disasters.

Crowd Modeling and Simulation in AnyLogic

In recent years, crowd modeling and simulation technologies have gained tremendous momentum for investigating crowd dynamics. Crowd simulations can be distinguished into two broad areas. The first focuses on the realism of behavioral aspects like crowd evacuation simulation, sociological crowd models, or crowd dynamics models. The second area aims at a high-quality visualization of a crowd with a convincing visual result and an emphasis on rendering and animation methods. Another classification of crowd simulation is based on the size of the crowd and the approach used. Simulated crowd sizes may vary from tens or hundreds to a couple of hundred thousand or millions of individuals. Usually large crowds are treated as a whole (macro-scale) where the global trend of the crowd is the focus due to the high computational needs. For smaller crowds (microscale), individual behavior is modelled in detail to support the investigation of crowd dynamics at an individual level. In this paper, we place a balance between both extremes and use an intermediate approach (mesoscale). The crowd simulation size is reasonably large (10,000) but still possesses some unique individual attributes and behavior that can be incorporated when globally examining the crowd dynamics.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
ASYMMETRIC
THREATS

National security in the Fourth National Climate Assessment

Source: http://www.homelandsecuritynewswire.com/dr20181130-national-security-in-the-fourth-national-climate-assessment

Nov 30 – On Friday, 23 November 2018, the Fourth National Climate Assessment Volume II was released. NCA4 Vol II, Impacts, Risks, and Adaptation in the United States, assesses a range of potential climate change-related impacts, with an aim to help decision makers better identify risks that could be avoided or reduced. The assessment follows Vol I, the Climate Science Special Report (CSSR), which was released in November 2017. Together, these reports meet the requirements of the Global Change Research Act, which mandates a quadrennial assessment of our understanding of global change and its impacts on the United States.

The last NCA3 was released in 2014. The Center for Climate and Security (CCS) notes that one of the main "Topics for Consideration in Future Assessments" was "National Security." As such, there was a significant increase in the coverage of national security matters in this latest National Climate Assessment. This is consistent with assessments coming from both the Department of Defense and the National Intelligence Council during this Administration.

Below is a list of only the explicit mentions of climate change impacts on national security and the military in the report. The full assessment also covers broader human, food, water, and energy security matters, which can certainly have national security implications, so we encourage readers interested in climate and security to explore the whole report.

National security in the Fourth National Climate Assessment

The text below contains direct excerpts from the "Report-in-Brief" and the individual chapters, highlighting explicit mentions of climate change impacts on "national security" and the "military."

Report-in-Brief (PDF)

Summary findings

3 Interconnected Impacts: (p. 13)

10 Infrastructure: "Our Nation's aging and deteriorating infrastructure is further stressed by increases in heavy precipitation events, coastal flooding, heat, wildfires, and other extreme events, as well as changes to average precipitation and temperature. Without adaptation, climate change will continue to degrade infrastructure performance over the rest of the century, with the potential for cascading impacts that threaten our economy, ***national security***, essential services, and health and well-being." (p. 17)

Overview:

Human Health and Well-Being: "Combined with other stressors, sea level rise, coastal storms, and the deterioration of coral reef and mangrove ecosystems put the longterm habitability of coral atolls in the Hawai'i and U.S.-Affiliated Pacific Islands region at risk, introducing issues of sovereignty, human and ***national security,*** and equity." (Ch. 27: Hawai'i & Pacific Islands, KM 6) (p. 27)

Box 1.4: How Climate Change around the World Affects the United States: "Natural variability and changes in climate increase risks to our ***national security*** by affecting factors that can exacerbate conflict and displacement outside of U.S. borders, such as food and water insecurity and commodity price shocks. More directly, our ***national security*** is impacted by damage to U.S. military assets such as roads, runways, and waterfront infrastructure from extreme weather and climate-related events (Figures 1.8 and 1.9). The U.S. ***military*** is working to both fully understand these threats and incorporate projected climate changes into long-term planning. For example, the Department of Defense has performed a comprehensive scenario-driven examination of climate risks from sea level rise to all of its coastal ***military*** sites, including atolls in the Pacific Ocean" (Ch. 16: International, KM 3) (p. 28)

Mitigation: "Recent studies suggest that some of the indirect effects of mitigation actions could significantly reduce—or possibly even completely offset—the potential costs associated with cutting greenhouse gas emissions. Beyond reduction of climate pollutants, there are many benefits, often immediate, associated with greenhouse gas emissions reductions, such as improving air quality and public health, reducing crop damages from ozone, and increasing

energy independence and ***security*** through increased reliance on domestic sources of energy" (Ch. 13: Air Quality, KM 4; Ch. 29: Mitigation, KM 4) (p.31)
Adaptation: "Effective adaptation can also enhance social welfare in many ways that can be difficult to quantify, including improving economic opportunity, health, equity, ***national security***, education, social connectivity, and sense of place, while safeguarding cultural resources and enhancing environmental quality." (pp. 32-33)
What Has Happened Since the Last National Climate Assessment? – New Aspects of This Report – New Chapters: "Public input also requested greater international context in the report, which has been addressed through two new additions. A new chapter focuses on topics including the effects of climate change on U.S. trade and businesses, ***national security***, and U.S. humanitarian assistance and disaster relief (Chapter 16). A new international appendix (Appendix 4) presents a number of illustrative examples of how other countries have conducted national climate assessments, putting our own effort into a global context."

Chapter 4: Energy Supply, Delivery, and Demand (Full chapter)
Key Message 1 Nationwide Impacts on Energy: The Nation's energy system is already affected by extreme weather events, and due to climate change, it is projected to be increasingly threatened by more frequent and longer-lasting power outages affecting critical energy infrastructure and creating fuel availability and demand imbalances. The reliability, ***security***, and resilience of the energy system underpin virtually every sector of the U.S. economy. Cascading impacts on other critical sectors could affect economic and national security." (page 70 Executive Summary)
State of the Sector: The Nation's economic security is increasingly dependent on an affordable and reliable supply of energy. Every sector of the economy depends on energy, from manufacturing to agriculture, banking, healthcare, telecommunications, and transportation.[2] Increasingly, climate change and extreme weather events are affecting the energy system (including all components related to the production, conversion, delivery, and use of energy), threatening more frequent and longer-lasting power outages and fuel shortages.[3] Such events can have cascading impacts on other critical sectors[43,44] and potentially affect the Nation's economic and ***national security*** *(*see Ch. 17: Complex Systems*)*.
Box 4.2: Changing Dimensions of Energy Security: "There is a trend of decreasing net imports (imports minus exports) of petroleum. In 2016, U.S. net imports reached a new low equal to about 25% of U.S. petroleum consumption, down from 60 percent in 2005.[59,61] This significant decline is the result of several factors, including the exploitation of vast domestic shale oil reserves and, to a lesser extent, reduced demand levels and expanded biofuel production. While this shift has potential ***national security*** benefits, there is an accompanying altered geographic distribution of our energy production assets and activities that could result in changes in exposure to the effects of extreme weather and climate change."
Key Message 3 Improving Energy System Resilience: "The Nation's economic security is increasingly dependent on an affordable and reliable supply of energy. Every sector of the economy depends on energy, from manufacturing to agriculture, banking, healthcare, telecommunications, and transportation. Increasingly, climate change and extreme weather events are affecting the energy system, threatening more frequent and longer-lasting power outages and fuel shortages. Such events can have cascading impacts on other critical sectors, potentially affecting the Nation's economic and ***national security***. At the same time, the energy sector is undergoing substantial policy, market, and technology-driven changes that are projected to affect these vulnerabilities." (page 71)

Chapter 7 Ecosystems, Ecosystem Services, & Biodiversity (Full chapter)
Ecosystem Services at Risk: "A reduced supply of critical provisioning services (food, fiber, and shelter) has clear consequences for the U.S. economy and ***national security*** and could create a number of challenges for natural resource managers.[104]

Chapter 8 Coastal Effects (Full chapter)
Case Study: Messages in Action – Norfolk, Virginia: "Low-lying Norfolk—Virginia's second-largest city—is enduring serious physical, financial, and social impacts as the frequency of high tide flooding accelerates due to rising local sea level.[6] High tide flooding threatens access routes, historical neighborhoods, personal and commercial property

integrity and value, and ***national security***, given that Norfolk houses the world's largest naval base. The city has begun to invest in mitigation and adaptation actions,[117] but recent estimates indicate it will cost hundreds of millions of dollars to improve storm water pipes, flood walls, tide gates, and pumping stations.[118] Natural and nature-based infrastructure projects such as the Colley Bay living shoreline have improved water quality, mitigated erosion, and restored habitats.[119] Additional planned projects include constructing berms, reclaiming filled waterways and wetlands, and raising roads and structures. City officials have identified the neighborhoods of The Hague and Pretty Lake as top priorities for flood mitigation, but in other areas of the city where containment will be more difficult, residents face the possibility of abandoning their homes (Figure 8.7).[118,120]… Given that the city is home to Naval Station Norfolk and other ***national security*** facilities, the Department of Defense has also contributed to plans for the city's future (Ch. 1: Overview, Figure 1.8). Naval Station Norfolk supports multiple aircraft carrier groups and is the duty station for thousands of employees.[122] Most of the area around the base lies less than 10 feet above sea level,[123] and local relative sea level is projected to rise between about 2.5 and 11.5 feet by the year 2100 under the Intermediate-Low global SLR scenario (considered likely under the lower [RCP4.5] and very low [RCP2.6] scenarios) and the Extreme SLR scenario (considered worst case under a higher scenario, RCP8.5), respectively.[36] The Navy is studying how flooding in Norfolk and Virginia Beach affects ***military*** readiness when sailors and other employees who live off-base are unable to reach the naval station for work.[124] Ultimately, the lessons learned in Norfolk—both the successes and challenges—are transferable to other coastal communities across the United States and its territories."

Chapter 14 Human Health (Full chapter)

Box 14.2 Transboundary Transmission of Infectious Diseases: "Outbreaks occurring in other countries can impact U.S. populations and ***military*** personnel living abroad and can sometimes affect the United States. For example, the 2015–16 El Niño, one of the strongest on record,[44] may have contributed to the 2014–16 Zika epidemic in the Americas.[31,45,46,47,48] Warmer conditions may have facilitated expansion of the geographic range of mosquito populations and increased their capacity to transmit Zika virus.[40] Zika virus can cause a wide range of symptoms, including fever, rash, and headaches, as well as birth defects. The outbreak began in South America and spread to areas with mosquitoes capable of transmitting the virus, including Puerto Rico, the U.S. Virgin Islands, Florida, and Texas."

Chapter 16: Climate Effects on U.S. International Interests (Full chapter)

Introduction: The global impacts of climate (climate change, variability, and extreme events) are already having important implications for societies and ecosystems around the world and are projected to continue to do so into the future.[1,2,3] There are specific U.S. interests that can be affected by climate-related impacts outside of U.S. borders, such as climate variability (for example, El Niño/La Niña events), climate extremes (for example, floods resulting from extreme precipitation), and long-term changes (for example, sea level rise). These interests include economics and trade (Key Message 1), international development and humanitarian assistance (Key Message 2), ***national security*** (Key Message 3), and transboundary resources (Key Message 4). While these four topics are addressed separately, they can also affect each other. For example, climate-related disasters in developing countries not only have significant local and regional socioeconomic impacts, but they can also set back U.S. development investments, increase the need for U.S. humanitarian assistance, and affect U.S. trade and ***national security***. U.S. citizens have long been concerned about the welfare of those living beyond U.S. borders and their vulnerability to the global impacts of climate.[4,5]

Economics and Trade: "In addition to local impacts on U.S.-owned assets abroad, climate change is expected to lead to large-scale shifts in the availability and prices of a wide array of agricultural,[12,13] energy,[14,15] and other goods, with corresponding impacts on the U.S. economy. These impacts occur on a wide range of timescales, ranging from months to multiple decades. For example, the prices of agricultural and mining commodities and manufactured goods are affected by year-to-year and decadal climate variations in the availability of irrigation water for agriculture or hydroelectric power.[16,17,18,19]International price changes affect U.S. businesses abroad, as well as U.S. exports and imports. An example is the damaging effect that a series of short-term climate extremes in 2010 and 2011 had on global wheat production. These extremes included drought in Russia, Ukraine, and the United States and damaging precipitation in Australia. A corresponding reduction in wheat production, in combination with high demand,

low stocks, trade policies, and other factors, contributed to a spike in global wheat prices.[20] This benefited U.S. wheat exports while increasing the cost of flour and bread in the United States.[21] This example highlights the complex interactions that often arise through major impacts of overseas climate change, variability, or extremes on U.S. interests (see Key Message 3 for a discussion of some of the ***security*** implications from the 2010–2011 drought).[22]Where these impacts increase global market prices, U.S. purchasers and consumers tend to be harmed, whereas U.S. producers tend to benefit. The opposite is generally true for impacts that drive prices down."

International Development and Humanitarian Assistance: "Many developing countries depend heavily on agriculture as a major source of jobs and a large percentage of their gross domestic product (GDP). Drought can have impacts on food production and security at multiple scales. At the national level, the loss of food and income and the need to help farmers through bad years can set back development. At the household level, drought can wipe out crops and financial assets and leave families vulnerable to starvation."

Key Message 3 Climate and National Security: "Climate change, variability, and extreme events, in conjunction with other factors, can exacerbate conflict, which has implications for U.S. ***national security***. Climate impacts already affect U.S. ***military*** infrastructure, and the U.S. ***military*** is incorporating climate risks in its planning." (p. 107)

Climate change and extremes increase risks to ***national security*** through direct impacts on U.S. military infrastructure and by affecting factors, including food and water availability, that can exacerbate conflict outside U.S. borders.[59] [60] Droughts, floods, storm surges, wildfires, and other extreme events stress nations and people through loss of life, displacement of populations, and impacts on livelihoods.[61] [62] Increases in the frequency and severity of such events, as well as other aspects of climate change, may require a larger ***military*** mission focus on climate-sensitive areas such as coasts, drought-prone areas, and the Arctic.[60]

Climate change is already affecting ***U.S. Department of Defense*** (DoD) assets by, among other impacts, damaging roads, runways, and waterfront infrastructure.[63] DoD is working to both fully understand these threats and incorporate projected climate changes into long-term planning to reduce risks and minimize impacts. There are many examples of DoD's planning and action for risks to its assets from climate change. DoD has performed a comprehensive scenario-driven examination of climate risks from sea level rise to all of its coastal military sites,[64] including atolls in the Pacific Ocean.[65] In the Arctic, the U.S. Coast Guard and Navy are pursuing strategies to respond to the changing geopolitical significance resulting from the projected absence of summer sea ice in the next few decades. *(*Ch. 2: Climate, KM 7*)*.[66] [67] [68] [69]

The risks climate change may hold for ***national security*** more broadly are connected to the relationships between climate-related stresses on societies and conflict. Direct linkages between climate-related stress and conflict are unclear,[70] but climate variability has been shown to affect conflict through intermediate processes, including resource competition, commodity price shocks, and food insecurity.[71] [72] The potential for conflict increases where there is a history of civil violence, conflict elsewhere in the region, low GDP or economic growth, economic shocks, weak governance, and lack of access to basic needs.[61] For example, droughts around the world in 2010 contributed to a doubling of global wheat prices in 2011 and a tripling of bread prices in Egypt.[73] This and other factors, including national trade policy and poverty, contributed to the civil unrest that ultimately resulted in the 2011 Egyptian revolution.[73] While the 2010 droughts were not the sole cause of the revolution, they contributed to destabilization of an already unstable region. Likewise, drought in Somalia has forced herders to sell livestock they could not provide for, reducing their incomes and leading some to join armed groups.[74] Water scarcity and climate-related variations in water availability can increase tensions and conflict between countries.[75] In these and other instances, conflict was related to stress from climate-related events, but non-climatic factors also had an important role.[76] [77] [78] [79] [80] [81] [82] [83] However, in some cases, water scarcity and variability can result in cooperation rather than conflict.[61] [84]

Human migration is another potential ***national security*** issue. Extreme weather events can in some cases result in population displacement. For example, in 1999 the United States granted Temporary Protected Status to 57,000 Honduran and 2,550 Nicaraguan nationals in response to Hurricane Mitch.[85] In 2013, more than 4 million people were internally displaced by Typhoon Haiyan in the Philippines,[86] and the United States committed 13,400 military personnel to the relief effort (Figure 16.3).[87] Six months after Typhoon Haiyan, more than

200,000 people remained without adequate shelter.[88] While neither Hurricane Mitch nor Typhoon Haiyan was solely attributable to climate change,[89] tropical cyclones are projected to increase in intensity, which would increase the risk of forced migration.[2,49] Slower changes, including sea level rise and reduced agricultural productivity related to changes in temperature and precipitation patterns, could also affect migration patterns.[61] However, whether migration in response to climate change will generally cause or exacerbate violent conflict is still uncertain. *(*Ch. 27: Hawai'i & Pacific Islands, KM 6*)* [90,91]

Key Message 4 Transboundary Resources: "U.S. international interests, such as economics and trade, international development and humanitarian assistance, ***national security***, and transboundary resources, are affected by impacts from climate change, variability, and extreme events. Long-term changes in climate could lead to large-scale shifts in the global availability and prices of a wide array of agricultural, energy, and other goods, with corresponding impacts on the U.S. economy. Some U.S.-led businesses are already working to reduce their exposure to risks posed by a changing climate…

Climate change, variability, and extreme events increase risks to ***national security*** through direct impacts on U.S. military infrastructure and, more broadly, through the relationship between climate-related stress on societies and conflict. Direct linkages between climate and conflict are unclear, but climate variability has been shown to affect conflict through intermediate processes, including resource competition, commodity price shocks, and food insecurity. The U.S. ***military*** is working to fully understand these threats and to incorporate projected climate changes into long-term planning." (page 108)

Box 16.2 Benefits of International Scientific Cooperation on Climate Research: "*knowledge of climate impacts in regions and sectors of interest to the United States*, which can be used to inform decisions about humanitarian and development assistance, ***national security***, and transboundary resource management;[51,137]"

Box 16.3 How Well Are Climate Risks to U.S. International Interests Understood and Addressed? "There is high confidence that climate change, variability, and extreme events can result in profound consequences for U.S. international interests relating to economy and trade (Key Message 1), development and humanitarian assistance (Key Message 2), ***national security*** (Key Message 3), and managing shared resources across our borders (Key Message 4). Projections of climate change indicate that these impacts will continue throughout the century and will likely accelerate in the future.[3]

Despite this level of confidence, the mechanisms by which climate impacts beyond American borders can affect U.S. interests are not uniformly well understood. Some of this uncertainty arises because these impacts are part of complex systems, and understanding how climate change, variability, and extremes affect such systems can be challenging *(*Ch. 17: Complex Systems*)*. For example, as noted in Key Message 3, the connections between climate and ***national security*** are complex because ***national security*** can be affected through intermediate processes such as resource competition. Such processes are challenging to model and forecast because they can be affected by such difficult-to-predict factors as policy decisions, human behavior, and climate surprises.[147]"

Chapter 17: Sectorial Interactions, Multiple Stressors, and Complex Systems (Full chapter)

Key Message 3 Management of Interacting Systems: "Despite the challenge of managing system interactions, there are opportunities to learn from experience to guide future risk management decisions *(*Ch. 28: *Adaptation, KM 3)*. The financial sector has invested significantly in understanding and managing systemic risks—including those associated with climate change and climate policy.[68] Mechanisms include risk assessment, financial disclosures, contingency planning, and the development of regulations and industry standards that recognize system interdependencies. Another example is that of the ***Department of Defense*** (DoD), which integrates consideration for the implications of climate change and variability for food, water, energy, human migration, supply chains, conflict, and disasters into decision-making and operations around the world.[69] In so doing, the DoD focuses on enhancing preparedness, building partnerships with other public and private organizations, and including climate change in existing planning processes.[69,70] These strategies are relevant to any organization attempting to enhance its resilience to climate change."

Chapter 18 Northeast (Full chapter)

Background "Service infrastructure in the Northeast is at increasing risk of disruption, resulting in lower quality of life, economic declines, and enhanced social inequality.[17] Interdependencies across critical infrastructure sectors such as water, energy,

transportation, and telecommunication (and related ***climate security*** issues) can lead to cascading failures during extreme weather and climate-related disruptions (Ch. 17: Complex Systems).[17,59,60]"

Chapter 19 Southeast (Full chapter)
Case Study: Prescribed Fire: "With wildfire projected to increase in the Southeast,[6,191] prescribed fire (the purposeful ignition of low-intensity fires in a controlled setting), remains the most effective tool for reducing wildfire risk.[4,195] ***Department of Defense*** (DoD) lands represent the largest reservoirs of biodiversity and native ecosystems in the region.[117] ***Military*** activities are a frequent source of wildfires, but increases in prescribed fire acres (Figure 19.19) show a corresponding decrease in wildfire ignitions for DoD.[4] Climate resilience by DoD is further achieved through restoration of native longleaf pine forests that occupy a wide range of site types, including wetland and well-drained soils—the latter leading many to characterize this forest as being drought resistant.[196,197,198,199] In addition to proactive adaptation through prescribed fire, ***DoD*** has been a leader in climate strategies that include regional conservation planning, ecosystem management, endangered species recovery, and research funding."

Chapter 23: Southern Great Plains (Full chapter)
Coastal Areas, Bays, and Estuaries: "The Texas coast, with 6.5 million people contributing over $37 billion to the region's economy, relies on its natural features, bays, and estuaries that serve as storm barriers to protect coastal infrastructure, and on its climate amenities to spur ecosystem services, such as fishing, ecotourism, and the ocean economy. These coastal ecosystems provide protection not only for people but also for 25% of the Nation's refining capacity, four crucial ports, much of the strategic petroleum reserves, and strategic ***military*** deployment and distribution installations. This protection was clearly on display with the recent impacts of Hurricane Harvey, where it has been estimated that natural coastal habitats protected about $2.4 billion worth of property in Texas and thousands of lives, with the suggestion that these habitats are potentially our first lines of defense.[130]"

Chapter 26 Alaska (Full chapter)
Key Message 5 Economic Costs Marine Vessel Traffic: "Northward progression of the late-summer sea ice edge creates opportunities for increased vessel traffic of various types (including cargo and tanker ships, tour boats, and government vessels, including ***military***)[226] to pass through the Bering Strait to or from the Northern Sea Route, the Northwest Passage,[228] and, by mid-century, directly across the Arctic Ocean.[229,230] As the Arctic Ocean opens, the Bering Strait will have increased strategic importance.[231] Lack of deep-water ports, vessel services, search and rescue operations, environmental response capabilities, and icebreaking capacity will impede expansion of vessel traffic.[225,226,230,232,233] Significant effects are likely several decades away, and new transarctic shipping will likely have little economic effects within Alaska in the near term but would bring environmental risks to fisheries and subsistence resources.[234] New oil and gas exploration and development in new areas within the U.S. economic zone are unlikely, as the Arctic Ocean waters that are not already accessible are generally off the U.S. continental shelf.
Key Message 6 Adaptation: "At the federal level, there are several key motivations for Arctic Strategies created by various U.S. Government agencies, including 1) recognizing the need to adapt to a changing climate, 2) identifying critical research gaps, 3) creating a vision for regional resilience, and 4) acknowledging the need to safeguard ***national security*** under changing environmental conditions.[264,265,266]"

Chapter 27 Hawai'i. and U.S.-Affiliated Pacific Islands (Full chapter)
Background: "For example, Hawai'i has the highest average electricity rate in the United States (more than twice the national average),[28] and more than 85% of food is imported on most islands (see Ch. 17: Complex Systems and Ch. 20: U.S. Caribbean, Background and KM 5 for more information on the importance of regional supply chains).[29,30,31] Though the islands are small, they are seats for key ***military*** commands, with forces stationed and deployed throughout the region providing strategic ***defense*** capabilities to the United States.
Despite the costs and risks, Pacific Islanders have deep ties to the land, ocean, and natural resources, and they place a high value on the environmental, social, and physical benefits

associated with living there. Residents engage in diverse livelihoods within the regional economy, such as tourism, fishing, agriculture, ***military*** jobs, and industry, and they also enjoy the pleasant climate and recreational opportunities. Important challenges for the region include improving food and water security, managing drought impacts, protecting coastal environments and relocating coastal infrastructure, assessing climate-induced human migration, and increasing coral reef resilience to warming and acidifying oceans."

Figure 27.9: Potential Economic Loss from Sea Level Rise, O'ahu, Hawai'i Figure 27.9: This map highlights potential economic losses (in 2015 dollars) in the exposure area associated with 3.2 feet of sea level rise on the island of O'ahu, Hawai'i. Potential economic losses are estimated from impacts to land and residential and commercial infrastructure. Highly impacted areas at risk of large economic losses include the U.S. Pacific Command and ***military*** infrastructure concentrated in Pearl Harbor (black circle) and the vulnerable tourist areas surrounding Waikīkī (dashed black circle). Source: adapted by Tetra Tech Inc. from the Hawai'i Climate Change Mitigation and Adaptation Commission 2017.[42]

Key Message 6 Cumulative Impacts and Adaptation: "Sea level rise, the deterioration of coral reef and mangrove ecosystems (see Key Message 4), and the increased concentration of economic activity will make coastal areas more vulnerable to storms (see Key Message 3).[196] Pacific Islands already face underlying economic vulnerabilities and stresses caused by unsustainable development, such as the use of beaches for building materials that results in coastal erosion or the waste disposal on mangroves and reefs that undermines critical ecological functions. The compounding impacts of climate change put the long-term habitability of coral atolls at risk, introducing issues of sovereignty, human and ***national security***,[197] and equity,[198] ,[199] ,[200] a subject of discussion at the international level."

Chapter 28: Reducing Risks Through Adaptation Actions: (**Full chapter**)

Introduction Individuals, business entities, governments, and civil society as a whole can take adaptation actions at many different scales. Some of these are changes to business operations, adjustments to natural and cultural resource management strategies, targeted capital investments across diverse sectors, and changes to land use and other policies. Adaptation actions can yield beneficial short-term and/or longer-term outcomes in excess of their costs, based on economic returns, ecological benefits, and broader concepts of social welfare and ***security***.

Key Message 3 Adaptation Entails Iterative Risk Management: Iterative risk management is consistent with most of the elements in the many climate adaptation efforts and approaches currently in use,[42] ,[43]including climate vulnerability assessment, iterative risk assessment, and adaptive management as often practiced by federal and other land and resource management agencies,[44] as well as disaster risk management.[45] Using a comprehensive framework helps highlight commonalities and differences across the approaches used by different jurisdictions and sectors, facilitating comparison and learning among their users. It also situates climate adaptation squarely within the broad range of other risk management activities, such as in the financial, engineering, environmental, health, and ***national security*** sectors.[2]

Key Message 4 – Benefits of Proactive Adaptation Exceed Costs: "Proactive adaptation initiatives—including changes to policies, business operations, capital investments, and other steps—yield benefits in excess of their costs in the near term, as well as over the long term. Evaluating adaptation strategies involves consideration of equity, justice, cultural heritage, the environment, health, and ***national security***. (p. 165)"

Broader Measures of Well-Being: Benefit–cost analysis provides one important, but not the sole, means to evaluate alternative adaptation actions. Effective adaptation can provide a broad range of benefits that can be difficult to quantify, including improvements in economic opportunity, human health, equity, ***national security***, education, social connectivity, and sense of place, while safeguarding cultural resources and practices and enhancing general environmental quality.

"In general, adaptation can generate significant benefits in excess of its costs. Benefit–cost analysis can help guide organizations toward actions that most efficiently reduce risks, in particular those that, if not addressed, could prove extremely costly in the future. Beyond those attributes explicitly measured by benefit–cost analysis, effective adaptation can also enhance social welfare in many ways that can be difficult to quantify and that people will value differently, including improving economic opportunity, health, equity, ***security***, education, social connectivity, and

sense of place, as well as safeguarding cultural resources and practices and environmental quality.
A significant portion of climate risk can be addressed by mainstreaming; that is, integrating climate adaptation into existing organizational and sectoral investments, policies, and practices, such as planning, budgeting, policy development, and operations and maintenance. Mainstreaming of climate adaptation into existing decision processes has already begun in many areas, such as financial risk reporting, capital investment planning, engineering standards, ***military*** planning, and disaster risk management. Further reduction of the risks from climate change, in particular those that arise from futures with high levels of greenhouse gas emissions, calls for new approaches that create conditions for altering regulatory and policy environments, cultural and community resources, economic and financial systems, technology applications, and ecosystems. (p. 166)"

Key Message 5 New Approaches Can Further Reduce Risk

Existing Mainstreaming: "Mainstreaming climate adaptation into existing decision processes has begun in many areas, in particular those with well-developed risk management processes such as financial risk reporting, capital investment planning, engineering standards, ***military*** planning, and disaster risk management… Other sectors of government and industry are also starting to consider climate risk a major systemic risk. In its 2018 Global Risks Report, the World Economic Forum listed the top five environmental risks—including extreme weather events and temperatures and failures of climate change mitigation and adaptation—in terms of both likelihood and the impact on the global economy.[116] The U.S. ***military*** now routinely integrates climate risks into its analysis, plans, and programs,[117] with particular attention paid to climate effects on force readiness, ***military*** bases, and training ranges (Ch. 16: International, KM 3).[118] [119] Naval Station Norfolk, for example, has replaced existing piers with double-decker piers that are elevated by several more feet and thus more resilient to rising sea levels and extreme weather events." (Ch. 1: Overview, Figure 1.8)

"Pause" in global warming was never real, new research proves

Source: http://www.homelandsecuritynewswire.com/dr20181220-pause-in-global-warming-was-never-real-new-research-proves

Dec 20 – An international team of climate researchers reviewed existing data and studies and reanalyzed them. They concluded there has never been a statistically significant pause' in global warming. This conclusion holds whether considering the `pause' as a change in the rate of warming in observations or as a mismatch in rate between observations and expectations from climate models.

Their papers are published n *Environmental Research Letters*.

Dr. James Risbey, from CSIRO Australia, is the lead author of one of studies, which reassessed the data and put it into historical context.

He said: "Many studies over the past decade have claimed to find a pause or slowdown in global warming and have typically posited this as evidence that is inconsistent with our understanding of global warming."

The study examined the literature on an alleged 'pause'. It looked at how the 'pause' had been defined, the time intervals used to characterize it, and the methods used to assess it. The study then tested historical and current versions of the earth's global mean surface temperature (GMST) datasets for pauses, both in terms of no warming trend and a substantially slower trend in GMST.

Dr. Risbey said: "Our findings show there is little or no statistical evidence for a 'pause' in GMST rise. Neither the current data nor the historical data support it. Moreover, updates to the GMST data through the period of 'pause' research have made this conclusion stronger. But, there was never enough evidence to reasonably draw any other conclusion.

"Global warming did not pause, but we need to understand how and why scientists came to believe it had, to avoid future episodes like this. The climate-research community's acceptance of a 'pause' in global warming caused confusion for the public and policy system about the pace and urgency of climate change.

"That confusion in turn might have contributed to reduced impetus for action to prevent greenhouse climate change. The full costs of that are unknowable, but the risks are substantial. There are lessons here for the science, and for the future."

The group's companion study looks at the alleged mismatch

between the rate of global warming in observations and climate models.

Bristol says that the team carried out a systematic comparison between temperatures and projections, using historical GMST products and historical versions of model projections from the times when claims of a divergence between observations and modelling were made.

The comparisons were made with a variety of statistical techniques to correct for problems in previous work.

Professor Stephan Lewandowsky, from the University of Bristol's School of Psychological Science, is this paper's lead author. He said: "We found the impression of a divergence – i.e. a divergence between the rate of actual global warming and the model projections – was caused by various biases in the model interpretation and in the observations. It was unsupported by robust statistics."

Despite this, the authors point out that by the end of 2017, the 'pause' was the subject of more than 200 peer-reviewed scientific articles. Many of these articles do not give any reason for their choice of start year for the 'pause', and the range spans 1995 to 2004.

Professor Lewandowsky said: "This broad range may indicate a lack of formal or scientific procedures to establish the onset of the 'pause'. Moreover, each instance of the presumed onset was not randomly chosen but chosen specifically because of the low subsequent warming. We describe this as selection bias.

"This bias causes a problem. If a period is chosen because of its unusually low trend, this has implications for the interpretation of conventional significance levels ("p-values") of the trend. Selection of observations based on the same data that is then statistically tested inflates the actual p-value, giving rise to a larger proportion of statistical false positives than the researcher might expect. Very few articles on the 'pause' account for or even mention this effect, yet it has profound implications for the interpretation of the statistical results.

"This is important, because some of the biases that affect the datasets and projections were known, or knowable, at the time."

When the researchers reanalyzed the data, accounting for the selection bias problem, they found no evidence for a divergence between models and observations existed at any time in the last decade.

They also offer some possible explanations why some scientists believed climate warming lagged behind modelled warming.

Co-author Professor Kevin Cowtan, from the University of York, UK, said: "One cause may be a that surface temperature data providers struggle to communicate the limitations of the data to climate scientists. This is difficult because users need to focus their expertise in their own problem areas rather than on the temperature data.

"Additionally, there can be delays of several years in updating surface temperature datasets. It takes time to find a bias, find a solution, and then for a paper to be published before most providers update their datasets. This process is good for transparency, but it may leave users in the position where they download data with knowable biases and unwittingly draw incorrect conclusions from those data.

Co-author Professor Naomi Oreskes, from Harvard University, USA, added "A final point to consider is why scientists put such emphasis on the 'pause' when the evidence for it was so scant. An explanation lies in the constant public and political pressure from climate contrarians. This may have caused scientists to feel the need to explain what was occurring, which led them inadvertently to accept and reinforce the contrarian framework."

University of Bristol climate scientist Dr. Dann Mitchell, from the School of Geographical Sciences, who was not involved with either study, said: "As climate scientists we often look back at previous bodies of evidence and wonder why certain topics were so prominent in discussion; the so-called climate hiatus being an excellent example of this. Given the fast pace of increasing climate change understanding, the conclusions of this paper will be very relevant for the inevitable future 'apparent' climate contradictions that emerge over time."

— Read more in Stephan Lewandowsky et al., "The 'pause' in global warming in historical context: (II). Comparing models to observations," Environmental Research Letters (19 December 2018) (DOI: 10.1088/1748-9326/aaf372); and James S Risbey et al., "A fluctuation in surface temperature in historical context: reassessment and retrospective on the evidence," Environmental Research Letters (19 December 2018).