2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

June 2018

www.cbrne-terrorism-newsletter.com

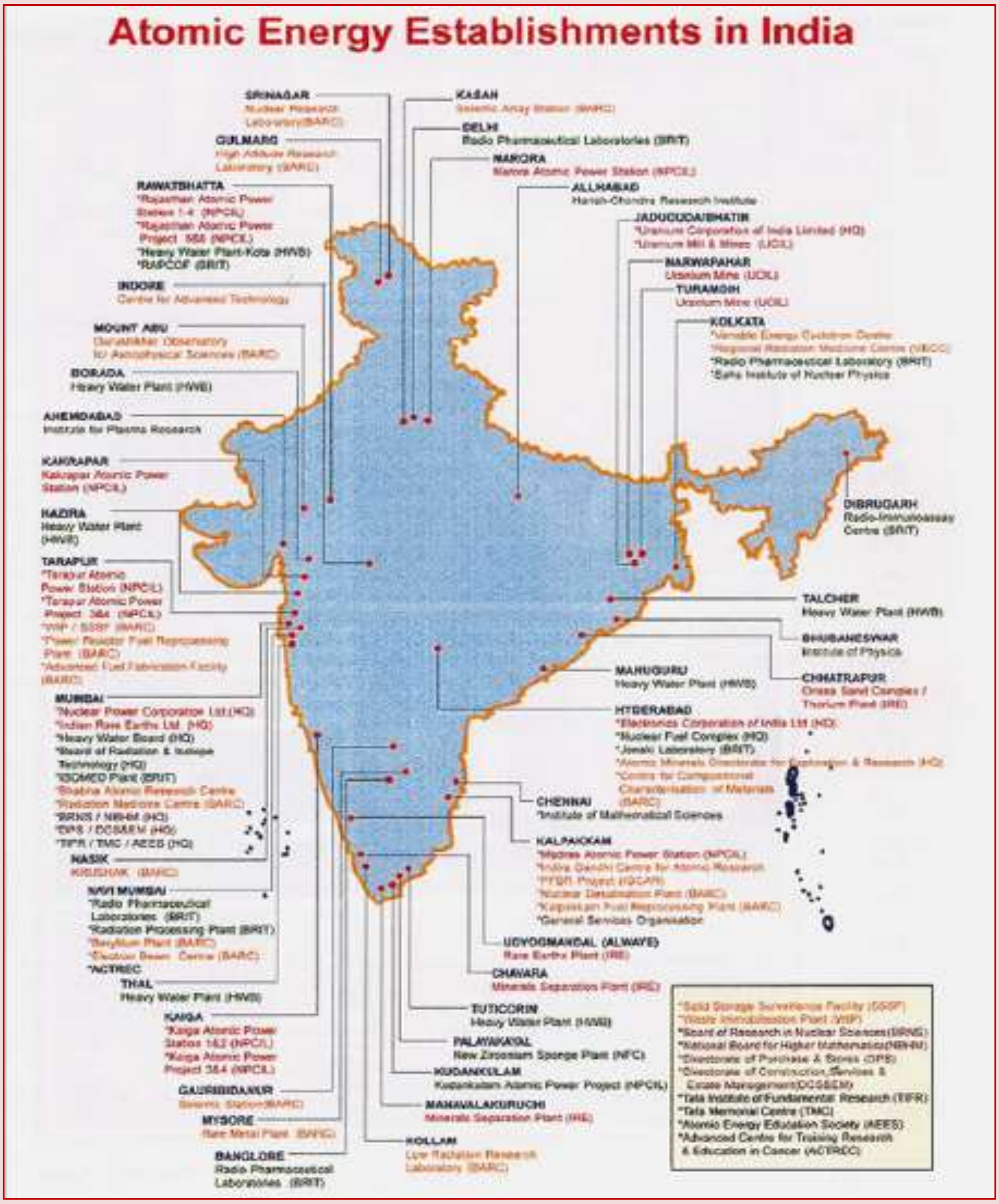
International CBRNE INSTITUTE
CBRNE-Terrorism Newsletter

DIRTY R-NEWS

India's nuclear security preparedness

By Colonel H R Naidu Gade – Indian Army Veteran
Source:https://issuu.com/deltabusinessmedialimited/docs/critical_infrastructure_protection__3bbb3929222f83?e=6269486/61566624

May 2018 – India presently operates about twenty-two nuclear power stations, a number of nuclear fuel cycle facilities related to fuel reprocessing, mining & milling and fabrication and a few nuclear research & development establishments. Additionally, there are about sixty thousand radiological facilities involving use of radiation-generating units or use of radioisotopes in the field of research, industry, medicine, and agriculture. The Indian civil nuclear facilities are spread over more than fifty-odd locations and an unknown number of locations house the strategic and related assets of India's strategic forces. India also has a large pool of both civil and military-oriented scientific manpower with highly specialised knowledge in nuclear sciences and technologies.


Atomic Energy Establishments in India
SRINAGAR
Nuclear Research Laboratory(BARC)
GULMARG
High Altitude Research Laboratory (BARC)
RAWATBHATTA
*Rajasthan Atomic Power Station 1-4 (NPCIL)
*Rajasthan Atomic Power Project 5&6 (NPCIL)
*Heavy Water Plant-Kota (HWB)
*RAPCOF (BRIT)
INDORE
Centre for Advanced Technology
MOUNT ABU
Gurushikhar Observatory for Astrophysical Sciences (BARC)
BORADA
Heavy Water Plant (HWB)
AHEMDABAD
Institute for Plasma Research
KAKRAPAR
Kakrapar Atomic Power Station (NPCIL)
HAZIRA
Heavy Water Plant (HWB)
TARAPUR
*Tarapur Atomic Power Station (NPCIL)
*Tarapur Atomic Power Project 3&4 (NPCIL)
*WIP / SSSF (BARC)
*Power Reactor Fuel Reprocessing Plant (BARC)
*Advanced Fuel Fabrication Facility (BARC)
MUMBAI
*Nuclear Power Corporation Ltd.(HQ)
*Indian Rare Earths Ltd. (HQ)
*Heavy Water Board (HQ)
*Board of Radiation & Isotope Technology (HQ)
*ISOMED Plant (BRIT)
*Bhabha Atomic Research Centre
*Radiation Medicine Centre (BARC)
*BRNS / NBHM (HQ)
*DPS / DCS&EM (HQ)
*TIFR / TMC / AEES (HQ)
NASIK
KRUSHAK (BARC)
NAVI MUMBAI
*Radio Pharmaceutical Laboratories (BRIT)
*Radiation Processing Plant (BRIT)
*Beryllium Plant (BARC)
*Electron Beam Centre (BARC)
*ACTREC
THAL
Heavy Water Plant (HWB)
KAIGA
*Kaiga Atomic Power Station 1&2 (NPCIL)
*Kaiga Atomic Power Project 3&4 (NPCIL)
GAURIBIDANUR
Seismic Station(BARC)
MYSORE
Rare Metal Plant (BARC)
BANGLORE
Radio Pharmaceutical Laboratories (BRIT)
KASAH
Seismic Array Station (BARC)
DELHI
Radio Pharmaceutical Laboratories (BRIT)
NARORA
Narora Atomic Power Station (NPCIL)
ALLHABAD
Harish-Chandra Research Institute
JADUGUDA/BHATIN
*Uranium Corporation of India Limited (HQ)
*Uranium Mill & Mines (UCIL)
NARWAPAHAR
Uranium Mine (UCIL)
TURAMDIH
Uranium Mine (UCIL)
KOLKATA
*Variable Energy Cyclotron Centre
*Regional Radiation Medicine Centre (VECC)
*Radio Pharmaceutical Laboratory (BRIT)
*Saha Institute of Nuclear Physics
DIBRUGARH
Radio-Immunoassay Centre (BRIT)
TALCHER
Heavy Water Plant (HWB)
BHUBANESWAR
Institute of Physics
CHHATRAPUR
Orissa Sand Complex / Thorium Plant (IRE)
MANUGURU
Heavy Water Plant (HWB)
HYDERABAD
*Electronics Corporation of India Ltd (HQ)
*Nuclear Fuel Complex (HQ)
*Jonaki Laboratory (BRIT)
*Atomic Minerals Directorate for Exploration & Research (HQ)
*Centre for Compositional Characterisation of Materials (BARC)
CHENNAI
*Institute of Mathematical Sciences
KALPAKKAM
*Madras Atomic Power Station (NPCIL)
*Indira Gandhi Centre for Atomic Research
*PFBR Project (IGCAR)
*Nuclear Desalination Plant (BARC)
*Kalpakkam Fuel Reprocessing Plant (BARC)
*General Services Organisation
UDYOGMANDAL (ALWAYE)
Rare Earths Plant (IRE)
CHAVARA
Minerals Separation Plant (IRE)
TUTICORIN
Heavy Water Plant (HWB)
PALAYAKAYAL
New Zirconium Sponge Plant (NFC)
KUDANKULAM
Kudankulam Atomic Power Project (NPCIL)
MANAVALAKURUCHI
Minerals Separation Plant (IRE)
KOLLAM
Low Radiation Research Laboratory (BARC)
*Solid Storage Surveillance Facility (SSSF)
*Waste Immobilisation Plant (WIP)
*Board of Research in Nuclear Sciences(BRNS)
*National Board for Higher Mathematics(NBHM)
*Directorate of Purchase & Stores (DPS)
*Directorate of Construction,Services & Estate Management(DCS&EM)
*Tata Institute of Fundamental Research (TIFR)
*Tata Memorial Centre (TMC)
*Atomic Energy Education Society (AEES)
*Advanced Centre for Training Research & Education in Cancer (ACTREC)

The threats

India, like other nuclear powers, faces threats in the realm of nuclear security from terrorist organisations hostile towards India and operating out of its neighbouring country Pakistan. These organisations like the Lashkar e Taiba (LeT) and Jaish e Mohammad (JeM), have declared interest in acquiring nuclear capabilities.

▶▶ **You can read the rest of this interesting article at source's URL.**

Underwater Drone to be Equipped with Nuclear Warhead

Source: https://i-hls.com/archives/83112

May 21 – Russia is developing a powerful underwater drone that can carry a nuclear **warhead with a capacity of up to 2 megatonnes**. As tass.com reports, Russia's Poseidon underwater drone currently under development "is primarily designed to destroy reinforced naval bases of a potential enemy", a source in the Russian defense sector said.

"It will be possible to mount various nuclear charges on the 'torpedo' of the Poseidon multipurpose seaborne system, with the thermonuclear single warhead similar to the Avangard charge to have the maximum capacity of up to 2 megatonnes in TNT equivalent," the source said.

Thanks to its nuclear powerplant, the Poseidon will approach the target for an intercontinental range at a depth of over 1 km and at a speed of 60-70 knots (110-130 km/h), the source said.

The **Poseidon drone** will join the Russian Navy under the existing armament program for 2018-2027 and will be carried by a new specialized submarine currently under construction at the Sevmash Shipyard.

The project of developing the Poseidon drone was unveiled by Russian President Vladimir Putin in his State of the Nation Address to the Federal Assembly on March 1. The Russian leader said that these drones could be armed with both conventional and nuclear munitions and would be capable of destroying enemy infrastructure, carrier-led naval task forces and other objectives.

According to the chief naval commander, the trials of the drone's basic element, the small-sized nuclear powerplant, have already been carried out.

Poseidon drones together with their carriers make part of the so-called oceanic multipurpose system. The drone got its name following the results of open voting on the website of Russia's Defense Ministry.

Fukushima-Daiichi radioactive particle release was significant: Study

Source: http://www.homelandsecuritynewswire.com/dr20180525-fukushimadaiichi-radioactive-particle-release-was-significant-study

May 25 – **Scientists say there was a significant release of radioactive particles during the Fukushima-Daiichi nuclear accident.**

The researchers identified the contamination using a new method and say if the particles are inhaled they could pose long-term health risks to humans.

The new method allows scientists to quickly count the number of cesium-rich micro-particles in Fukushima soils and quantify the amount of radioactivity associated with these particles.

The research, which was carried out by scientists from Kyushu University, Japan, and the University of Manchester, UK, was published in *Environmental Science and Technology*.

Manchester says that in the immediate aftermath of the Fukushima Daiichi nuclear accident, it was thought that only volatile, gaseous radionuclides, such as cesium and iodine, were released from the damaged reactors. However, in recent years it has become apparent that small radioactive particles, termed cesium-rich micro-particles, were also released. Scientists have shown that these particles are mainly made of glass, and that they contain significant amounts of radioactive cesium, as well as smaller amounts of other radioisotopes, such as uranium and technetium.

The abundance of these micro-particles in Japanese soils and sediments, and their environmental impact is poorly understood. But the **particles are very small and do not dissolve easily, meaning they could pose long-term health risks to humans if inhaled.**

Therefore, scientists need to understand how many of the micro-particles are present in Fukushima soils and how much of the soil radioactivity can be attributed to the particles. Until recently, these measurements have proven challenging.

The new method makes use of a technique that is readily available in most Radiochemistry Laboratories called Autoradiography. In the method, an imaging plate is placed over contaminated soil samples covered with a plastic wrap, and the radioactive decay from the soil is recorded as an image on the plate. The image from plate is then read onto a computer.

The scientists say radioactive decay from the cesium-rich micro particles can be differentiated from other forms of cesium contamination in the soil.

The scientists tested the new method on rice paddy soil samples retrieved from different locations within the Fukushima prefecture. The samples were taken close to (4 km) and far away (40 km) from the damaged nuclear reactors. The new method found cesium-rich micro-particles in all of the samples and showed that the amount of cesium associated with the micro-particles in the soil was much larger than expected.

Dr. Satoshi Utsunomiya, Associate Professor at Kyushu University, Japan, and the lead author of the study says "when we first started to find cesium-rich micro-particles in Fukushima soil samples, we thought they would turn out to be relatively rare. Now, using this method, we find there are lots of cesium-rich microparticles in exclusion zone soils and also in the soils collected from outside of the exclusion zone”.

Dr. Gareth Law, Senior Lecturer in Analytical Radiochemistry at the University of Manchester and an author on the paper, adds: “Our research indicates that significant amounts of cesium were released from the Fukushima Daiichi reactors in particle form.

“**This particle form of cesium behaves differently to the other, more soluble forms of cesium in the environment.** We now need to push forward and better understand if cesium micro-particles are abundant throughout not only the exclusion zone, but also elsewhere in the Fukushima prefecture; then we can start to gauge their impact.”

The new method can be easily used by other research teams investigating the environmental impact of the Fukushima Daiichi accident.

Dr Utsunomiya adds: “we hope that our method will allow scientists to quickly measure the abundance of cesium-rich micro-particles at other locations and estimate the amount of cesium radioactivity associated with the particles. This information can then inform cost effective, safe management and clean-up of soils contaminated by the nuclear accident.”

— Read more in Ryohei Ikehara et al., “Novel Method of Quantifying Radioactive Cesium-Rich Microparticles (CsMPs) in the Environment from the Fukushima Daiichi Nuclear Power Plant,” Environmental Science and Technology *(21 May 2018).*

Novel biomarkers reveal evidence of radiation exposure

By Medical College of Wisconsin

Source: https://www.sciencedaily.com/releases/2012/05/120522135259.htm

Researchers at the Medical College of Wisconsin have identified novel biomarkers that could be used to confirm exposure to damaging radiation in large groups of people potentially exposed to unknown and variable doses for the purpose of triage and treatment.

The findings are published in the May 1 issue of *Radiation Research.* John E. Baker, PhD, professor of surgery, biochemistry, pharmacology and toxicology at the Medical College of Wisconsin, is the lead author of the study.

There is an urgent need for rapid, accurate and sensitive diagnostic platforms to confirm exposure to radiation and estimate the dose absorbed by individuals -- whether that exposure is a result of radiological terrorism, nuclear power plant accident, or nuclear warfare. Clinical symptoms do not provide adequate diagnostic information to triage and treat life-threatening radiation injuries; furthermore, the United States has been found to be ill-suited to evaluate and triage large groups of patients with potential radiation exposure.

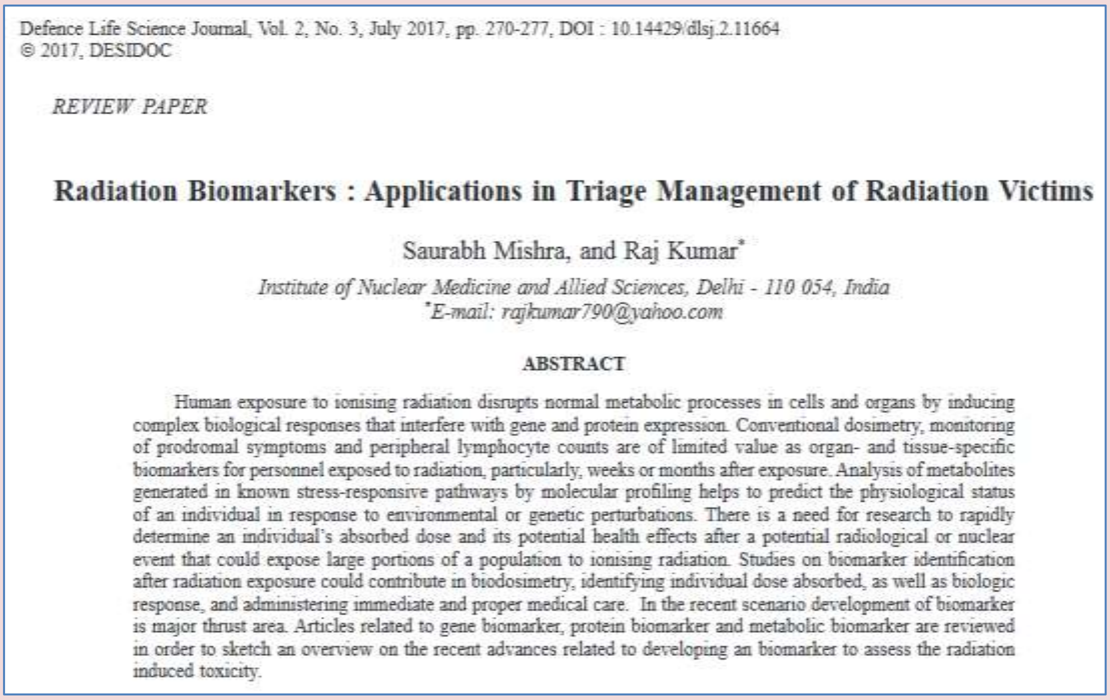
In this study, researchers examined the microbes found in rat feces before and after exposure to radiation. **Changes were identified in the levels of 212 genomically distinct bacteria, of which 59 are found in humans.** Those changes persisted at **least 21 days following the exposure to radiation**. One particular type of microbe, Proteobacteria, increased almost one-thousand fold four days following irradiation.

"If there were to be a radiological terrorism scenario, there could be hundreds of thousands of people that would be present around the ground zero area, and limited medical resources available to evaluate their exposure levels," explained Dr. Baker. "Analyzing microbial signatures in those patients would be a non-invasive way to obtain results in a timely fashion, and allow us to commit resources to patients in need of intervention."

The study was funded and data generated with US federal funds from the NIH Human Microbiome Project, the Common Fund, National Institute of Allergy and Infectious Diseases grant 1R01AI080363, and from grants from Tricorder Diagnostics and the Foundation for Heart Science.

The PhyloChip™ assay, developed by Second Genome, was utilized in this study to examine specific bacterial taxa.

Other authors of the study include Vy Lam, PhD; John E. Moulder, PhD; Nita H. Salzman, MD, PhD, the Medical College of Wisconsin; and Eric A. Dubinsky, PhD; and Gary L. Andersen, PhD; from Lawrence Berkeley National Laboratory in California. Dr. Andersen has an affiliation with Second Genome.



Defence Life Science Journal, Vol. 2, No. 3, July 2017, pp. 270-277, DOI : 10.14429/dlsj.2.11664
© 2017, DESIDOC

REVIEW PAPER

Radiation Biomarkers : Applications in Triage Management of Radiation Victims

Saurabh Mishra, and Raj Kumar*

Institute of Nuclear Medicine and Allied Sciences, Delhi - 110 054, India
**E-mail: rajkumar790@yahoo.com*

ABSTRACT

Human exposure to ionising radiation disrupts normal metabolic processes in cells and organs by inducing complex biological responses that interfere with gene and protein expression. Conventional dosimetry, monitoring of prodromal symptoms and peripheral lymphocyte counts are of limited value as organ- and tissue-specific biomarkers for personnel exposed to radiation, particularly, weeks or months after exposure. Analysis of metabolites generated in known stress-responsive pathways by molecular profiling helps to predict the physiological status of an individual in response to environmental or genetic perturbations. There is a need for research to rapidly determine an individual's absorbed dose and its potential health effects after a potential radiological or nuclear event that could expose large portions of a population to ionising radiation. Studies on biomarker identification after radiation exposure could contribute in biodosimetry, identifying individual dose absorbed, as well as biologic response, and administering immediate and proper medical care. In the recent scenario development of biomarker is major thrust area. Articles related to gene biomarker, protein biomarker and metabolic biomarker are reviewed in order to sketch an overview on the recent advances related to developing an biomarker to assess the radiation induced toxicity.

Source:https://pdfs.semanticscholar.org/42f2/7928a6192c499e651d6a193c39178f0d1bb8.pdf

Radiation Triage Mask

Source: https://www.flintbox.com/public/project/2829/

UOIT researchers have developed a facial mask device for First Responders used on patients exposed to radioactive materials. This device will rapidly determine who has/has not been exposed to radiation, what radioisotope and at what dosage. This device allows for rapid response to facilitate early treatment in the event of mass radiation poisoning. Inhalation is the primary route of entry into the body when exposed to a dirty bomb. This technology is a mask-like device that when placed over a person's nose and mouth will detect radiation. Two radiation detectors placed into this device will detect a) whether radiation exposure has occurred, and b) what radioisotope is involved in a matter of seconds. Knowing what isotope is involved is critical as this determines the type of treatment to follow. Current methods of diagnosing a specific radionuclide can take hours which can render treatment ineffective for certain toxins. Our new device can be easily used by First Responders who often have little or no training in radiation health physics.

Background

In the post 9/11 world the threat of a dirty bomb is no longer a subject for fiction. If an attack were to spread radioactive particles over a wide area, it will be essential for First Responders to quickly know how many people have been exposed, at what level and to what radioisotope. Moreover, in order to be effective, treatment for radiation poisoning needs to start immediately. Just as important is to quickly identify those who have not been exposed so that they do not clog the healthcare system in an emergency. Currently there is no device on the market that can solve this critical triage problem.

Measuring radiation doses in mass-casualty emergencies

Mary Sproull, Kevin Camphausen and Gregory Koblentz

Source: https://thebulletin.org/measuring-radiation-doses-mass-casualty-emergencies11162

October 2017 – For the first time since 1981, when China deployed the DF-5 intercontinental ballistic missile, a new state has gained the capability to target the United States with a nuclear weapon. On July 4 and again on July 28, North Korea launched the Hwasong-14—a two-stage, liquid-fueled ballistic missile that demonstrated the capability to reach the continental United States. The US intelligence community assesses that North Korea has nuclear warheads compact and light enough to fit on the Hwasong-14 and that North Korea will be able to deploy a nuclear-armed intercontinental ballistic missile within one or two years. North Korea demonstrated another new capability on September 3, testing what it claimed was a thermonuclear weapon. While the exact configuration of this "advanced nuclear device" remains unknown, the device's estimated yield is 140 kilotons, so the test represents a quantum leap in the destructive potential of North Korea's nuclear arsenal.

Tensions between the United States and North Korea escalated dramatically in the wake of these missile and nuclear tests. Donald Trump and Kim Jong-un engaged in a frightening war of words. The tensions prompted Hawaii, Guam, and California to increase their preparedness for a possible nuclear strike.

The medical consequences of even a single nuclear detonation would be horrific. According to Jerome Hauer, former director of emergency management for New York City, no city in the United States is prepared for the casualties, chaos, and destruction that would follow a nuclear detonation. Medical management in particular would be complicated by damage to infrastructure and communication systems, lack of sufficient first responders, scarce resources, complicated triage needs, and an overwhelming number of patients.

But Hauer highlights another set of crucial challenges—those associated with the diagnosis and treatment of radiation-related injuries:

> Beyond the difficult front lines of triage, survivors of a nuclear explosion will have a variety of injuries, some well known to modern hospitals but others more difficult to diagnose and develop a plan for. Acute radiation syndrome, in particular, results from exposure to radiation and does not have to coincide with any other injury. It may be the only effect a survivor suffers, and it may not manifest soon after exposure.

Fortunately, new types of diagnostics to address this critical need are being developed in the field of radiation biodosimetry. Radiation biodosimetry is the estimation, through observation of biological variables, of received dose from previous radiation exposure; the new diagnostics use changes in various biological markers to estimate the severity of radiation doses. Progress in radiation biodosimetry science is beginning to translate into advanced, field-deployable technologies. The United States could significantly improve its preparedness for a radiological or nuclear disaster if, while better leveraging its existing capability for biological dosimetry assessments, it also integrated emerging technologies into its radiological emergency planning and response.

Although federal guidelines for radiological emergency planning and response highlight the importance of radiation dose assessment as a core need for medical management of mass radiation exposures, the ability to rapidly and reliably measure radiation exposure in large numbers of victims is extremely limited in the United States. A 2010 review of US preparedness for a large-scale radiological event found that the United States lacked a number of key capabilities required to implement that mission, including:

- executable interagency procedures for medical triage following a radiological event
- adequate biodosimetry laboratory capacity
- a strategic plan to activate surge capacity resources for biodosimetry capability
- operational guidelines for biodosimetry sample handling and reporting
- requirements for short-term and long-term monitoring of individuals exposed to radiation
- establishment and integration of emerging high-capacity biodosimetry technologies

These capabilities would be useful for responding to the detonation of a nuclear weapon, to a "dirty bomb" attack with radioactive material, or to an accident at a nuclear power plant such as the one that occurred at Japan's Fukushima Daichii facility in 2011. In particular, enhancing preparedness for a radiological emergency requires immediate attention in three areas: establishing a surge capacity for biodosimetry labs; developing new biodosimetry assays; and integrating biodosimetry into operational response plans.

Surge capacity

In the United States, limited laboratory and point-of-care diagnostics are available to determine if someone has been exposed to radiation and, if so, to what degree. Moreover, currently available tools are poorly suited for management of a mass-screening scenario. The only point-of-care capabilities now available for biodosimetry assessment are lymphocyte depletion kinetics (measuring the rate of depletion of white blood cells to estimate received radiation dose) and clinical evaluation. Lymphocyte depletion kinetics is not conducive to triage biodosimetry because a baseline sample is needed soon after exposure for comparison with samples collected later at predetermined points in time. Clinical evaluation for dose assessment, such as time to onset of vomiting, can be useful for approximating dose—but can also be confounded by pre-existing medical conditions, psychological factors, and the effects of blast injuries. And clinical exams are of limited utility for large-scale screening due to the need for specially trained health care workers and the amount of time needed to complete exams.

The most widely used biodosimetry diagnostic is a technique not available in a point-of-care setting known as the dicentric chromosome assay. This assay, or diagnostic test, measures the number of abnormal chromosomes caused by radiation exposure to estimate received radiation dose, and is one of many types of cytogenetic assays that measure changes in chromosome structure. (Cytogenetics is "the branch of genetics that studies the structure of DNA within the cell nucleus.") Dicentric chromosome assay is considered the "gold standard" for dose assessment, yet it is ill suited for mass screening because it requires a high level of technical skill, takes considerable time, and must be conducted in an off-site laboratory setting. The United States has only two fully operational cytogenetic biodosimetry laboratories: the Energy Department's Radiation Emergency Assistance Center/Training Site in Oak Ridge, Tennessee and the Defense Department's Armed Forces Radiobiology Research Institute facility in Bethesda, Maryland. (Additional, auxiliary biodosimetry resources are housed at the Naval Dosimetry Center, also in Bethesda.)

To remediate the current shortage of cytogenetic laboratory capacity, the assistant secretary of preparedness and response (an official in the Health and Human Services Department) has proposed establishing a national cytogenetic biodosimetry network. This network would encompass approximately 150 existing clinical cytogenetics laboratories that routinely perform cytogenetic assays to check for birth defects and to detect and diagnose cancer. Ideally, this proposed Integrated Clinical Diagnostics System would increase the nation's biological dose assessment capability and would, to support triage during a radiological event, include the use of dicentric chromosome assay and lymphocyte depletion kinetics.

Automated platforms for cytogenetic biodosimetry are also under development. These platforms, such as the Rapid Automated Biodosimetry Tool, will adapt dicentric chromosome assay and other cytogenetic assays for mass-casualty screening. Increasing the number and capacity of laboratories capable of conducting this type of biodosimetry on a large scale is urgently needed. The Laboratory Response Network under the Centers for Disease Control and Prevention has substantial laboratory resources available for chemical and biological events, but not for radiological events.

New assays

Due to the recognized limitations of current biodosimetry assessment capabilities in the United States, government entities such as the Biomedical Advanced Research and Development Authority and the Radiation and Nuclear Countermeasures Program at the National Institutes of Health have funded research designed to identify novel biomarkers of radiation exposure. This research also facilitates late-stage development of biodosimetry devices that have the potential to quantify received radiation dose in a mass-screening setting. As a result of these funding initiatives, biodosimetry research has evolved from a relatively limited field of cytogenetic assessment (primarily depending on dicentric chromosome assay and evaluation of clinical symptoms) into a robust multidisciplinary field of radiation biology research that uses a variety of methodologies.

Research models of dose assessment, using newly identified radiation biomarkers, have been developed with the goal of developing deployable point-of-care biodosimetry assays. Technologies that can provide a point-of-care capability have entered late-stage development. Novel biomarkers have even been included in human case studies of accidental radiation exposures. For example, following a 2006 radiation accident in Dakar, Senegal, 63 individuals were screened for dose assessment using a combination of classic cytogenetic biodosimetry, analysis of lymphocyte counts, and measurement of new protein and metabolite biomarkers of radiation exposure.

Integrating biodosimetry

New biodosimetry technologies are rapidly emerging, but an important question remains: how these technologies will be used in the medical response to a radiological emergency. That uncertainty can best be addressed through four concrete measures.

First, existing biodosimetry capabilities need to be better integrated into federal radiological emergency planning and response. The first step in that process should be the creation of a concept of operations (a document that describes how a system works—from the perspective of someone who will use the system) for biodosimetry diagnostics in a civilian mass-care setting. Coordinating the federal medical response to a radiological emergency will be complex under the best of circumstances. Concepts of operations for biodosimetry at the triage level have been developed on a preliminary basis, but an interagency concept of operations for deployment of biodosimetry diagnostics in a civilian mass-care setting has not been fully developed. The specialized response teams fielded by the Medical Radiobiology Advisory Team (under the Armed Forces Radiobiology Research Institute), the Energy Department's Radiation Emergency Assistance Center/Training Site, the Health and Human Services Department, and the Veterans Administration's Medical Emergency Radiological Response Team represent vital assets within any response effort for a radiological event—yet they cannot undertake the medical management of large-scale radiological exposure on their own. For a mass-casualty incident involving radiation exposures, emergency preparedness plans need to address the complexity of medical management of radiation injury and establish operational guidelines for first responders and for use of available resources and infrastructure specific to radiation injury.

Second, federal response teams with practical experience in medical management of radiation exposures should be equipped with a deployable point-of-care biodosimetry diagnostic capability. In a mass-casualty event, the availability of point-of-care biodosimetry diagnostics would relieve the "worried well" problem—that is, physically uninjured people who seek medical treatment due to concern that they have been exposed to radiation. Availability of point-of-care biodosimetry diagnostics would also, by differentiating those who have been exposed from those who have received no radiation exposure, reduce the strain on local medical resources. As the technology developed by the Biomedical Advanced Research and Development Authority and the Radiation and Nuclear Countermeasures Program at the National Institutes of Health matures into field-deployable systems, these new capabilities will also need to be integrated into concepts of operation for medical responses to radiological emergencies.

Third, training in medical management of radiation injuries needs to be integrated into the primary and continuing education of health care providers and first responders. This training is essential so that medical caregivers have a working knowledge of how to interpret biodosimetry diagnostics and utilize this information to guide triage and treatment. Formation of a cytogenetic radiation biodosimetry network under the proposed Integrated Clinical Diagnostics System could also provide a surge capacity for appropriately trained medical personnel in the event of a radiological emergency.

Finally, operational point-of-care response plans at the federal, state, and local levels need to be formalized for medical management of mass-casualty radiological events. These plans should better integrate biodosimetry diagnostics into the triage management work flow. Several software platforms, such as the Biodosimetry Assessment Tool produced by the Armed Forces Radiobiology Research Institute and the Radiation Emergency Medical Management web portal (managed by the Health and Human Services Department), use existing biodosimetry techniques—such as time to onset of vomiting, lymphocyte kinetics, and dicentric chromosome assay—for triage management. But these systems are not ideal for mass-casualty care. These improved plans and software platforms should be validated through tabletop and live exercises. Fully integrating biodosimetry into existing deployable medical response teams would help ensure that the complexity of the interagency response during a radiological or nuclear event does not hinder mass screening and the medical management of patients.

Duty to plan

A North Korean nuclear attack is a high-consequence event, but an event of low probability. Then again, a nuclear attack by a foreign nation is not the only radiological emergency in which advanced radiation biodosimetry capabilities would be useful. Radiological emergencies can also include nuclear power plant accidents and "dirty bomb" attacks by terrorists. As Johns Hopkins scholar Dan Hanfling and colleagues have highlighted, the United States has made great strides in emergency management preparedness for nuclear events. These improvements have come through modeling of projected infrastructure impact scenarios, establishing Protective Action Guides for civilians, and developing preliminary concepts of operations for medical management of a nuclear event. Yet gaps remain in interagency planning, communicating with the public, and working toward deployable operational capabilities.

A key gap in US nuclear and radiological emergency preparedness is the lack of advanced dosimetry-based triage management. As Hanfling argues, we have a duty to plan—and "the right planning now will save countless lives after a nuclear attack." Radiation biodosimetry is a critical element of that planning. Indeed, it is the future of radiological emergency management.

***Kevin Camphausen** is chief of the Radiation Oncology Branch at the National Cancer Institute at the National Institutes of Health. Camphausen studies the interaction of novel drugs and radiotherapy in the treatment of glioblastoma multiforme brain tumors—in the laboratory, using preclinical model systems, and in the clinic, running clinical trials. Camphausen guides the branch's clinical/translational program, which studies the role of new agents as both radiation sensitizers and radiation protectors. Camphausen is an internationally recognized leader in his field and an expert in drug-induced tumor radiosensitization.*

***Gregory Koblentz** is an associate professor at and director of the Biodefense Graduate Program in the Schar School of Policy and Government at George Mason University. He is also a member of the Scientists Working Group on Biological and Chemical Security at the Center for Arms Control and Non-Proliferation. He is the author of Strategic Stability in the Second Nuclear Age and Living Weapons: Biological Warfare and International Security.*

***Mary Sproull** is a biologist in the Radiation Oncology Branch of the National Cancer Institute at the National Institutes of Health and a doctoral candidate in the Biodefense Graduate Program at the Schar School of Policy and Government at George Mason University. Her current work at the National Institutes of Health, in the laboratory of Kevin Camphausen, is funded by the Radiation and Nuclear Countermeasures Program/National Institute of Allergy and Infectious Diseases as part of an initiative to develop new radiation biodosimetry models for dose prediction.*

Quick blood test can triage radiation exposure victims, saving lives

Source: https://www.slashgear.com/quick-blood-test-can-triage-radiation-exposure-victims-saving-lives-14383643/

May 2015 – In the rare, but serious, cases of a radiation leak like the Fukushima nuclear plant's meltdown, first responders are tasked with sending radiation victims to triage based on their level of exposure. A new genetics-based blood test could be a faster, more accurate way to assess how individual victims will respond to radiation. Researchers from Harvard Medical School and New York City's Montefiore Medical Center have created a method of identifying long-term damage from radiation, immediately. Their technique involved looking beyond blood cell counts and delving into blood-bound genes.

It is nearly impossible to assess radiation exposure just by eyeballing the victims. Some of radiation's more visible effects don't set in until 24 hours after exposure, but the window for proper care begins to dwindle directly after exposure. Even an early blood test can only indicate the amount of dead white blood cells, which could look the same in fatal and severe–but survivable– cases.

The scientific paper published in the journal, *Science Translational Medicine*, details their discovery, first made using mice. They found that free-floating clumps of genetic material, microRNA can signal how much damage will be done to the body by a dose of radiation, with genetics determining a baseline for how much radiation someone can withstand and still survive.

There are still some roadblocks to developing this test for humans. Money talks when it comes to drug development, and there isn't much money to be made from emergency radiation testing. Researcher Dipanjan Chowdhury concedes, "unlike developing cancer drugs, this is not an area that's considered very lucrative." Perhaps if the testing could be applied to predict how cancer patients would respond to radiation therapy, the discovery could become commonplace alongside chemotherapy.

The Red Forest: Picturing Radiation with Infrared Film

Source: https://toxicnews.org/2018/05/31/the-red-forest-picturing-radiation-with-infrared-film/

Response to nuclear attack: "duct tape and cover"

By Andy Oppenheimer

Source: https://www.cbrneportal.com/response-to-nuclear-attack-duct-tape-and-cover/

June 05 – For the first time since the end of the Cold War, attention on how military and civilian authorities – and the public – would respond to a nuclear attack has resurfaced during recent hostile exchanges between the US and North Korea, and following a false missile alert in Hawaii.

It hardly needs saying that such an attack on any part of the world would be several orders of magnitude more catastrophic than just about all the others in the CBRN pantheon. Aside from a detonation of nuclear bomb out of a nation state's stockpile, a terrorist improvised nuclear device (IND) has risen in the list of threats, as has a cyberattack or natural disaster triggering a nuclear plant meltdown or explosion in the manner of Chernobyl and Fukushima.

The chaos produced by a nationwide natural disaster would be eclipsed by the mother of all WMD. A nuclear explosion from just a 5-kiloton device will kill and injure millions – both in the short and long term. Acute radiation injury and multiple injuries would overwhelm health services. Infrastructure – electricity, water, food and sanitation – would be totally destroyed or damaged, with major civil unrest breaking out and further injury and lost citizens buried below collapsing buildings and fires. Overall, it isimpossible to defend populations and troops against even a single device detonation, let alone a full-scale nuclear war.

Civil Defence

In the UK what rudimentary preparations were – and are – in place used to come under the original term 'civil defence'. In drills of the 1950s and 1960s, American schoolchildren would 'duck and cover' under their desks when the sirens sounded. Upgraded sirens alerted the population to an imminent attack. But as for evacuating them on notice of inbound enemy bombers, US policy is summed up by one historian: "run like hell."

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

***Andy Oppenheimer** AIExpE MIABTI is Editor-in-Chief of CBNW (Chemical, Biological & Nuclear Warfare) and CBNW Xplosive journals, a consultant in CBRNE and counter-terrorism, and author of IRA: The Bombs and the Bullets (Irish Academic Press, 2008).*

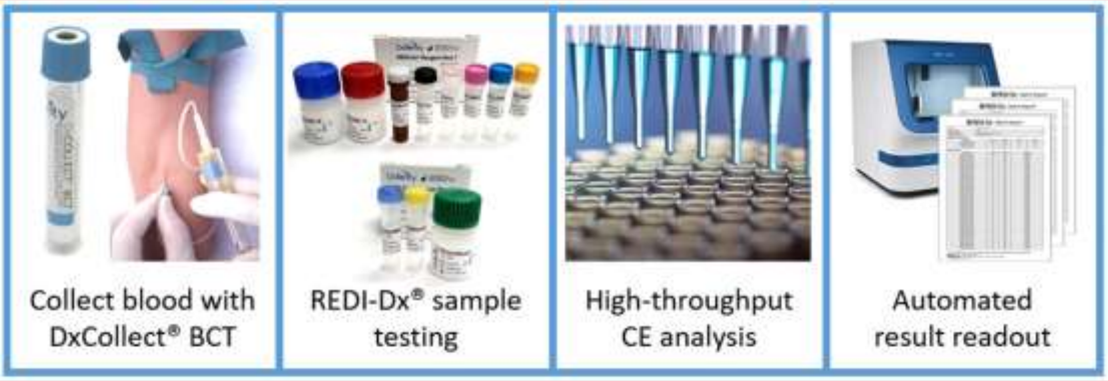
The need for a next generation radiation biodosimetry test

By Dr. Bob Terbrueggen

Source: https://www.cbrneportal.com/the-need-for-a-next-generation-radiation-biodosimetry-test/

June 05 – Rising political tension between the United States and Russia, along with North Korea's recent missile and nuclear tests, have led to a renewed interest in preparedness for a radiological event—the three most commonly planned-for being: a nuclear reactor incident like Fukushima, a radiological dispersal device (dirty bomb), or nuclear detonation.

While significant progress has been made in the development and stockpiling of medical countermeasures to radiation, as well as detailed planning on when and how to use them, a critical unmet need has been the lack of a high throughput radiation biodosimetry test that can be used to determine individualized levels of absorbed radiation post-event. This has now changed in Europe and in many other countries with the CE IVD marking of DxTerity's REDI-Dx®* High Throughput Radiation Biodosimetry Test.


Collect blood with DxCollect® BCT
REDI-Dx® sample testing
High-throughput CE analysis
Automated result readout

Critical support at a crucial time

After a nuclear event, a highly coordinated response with appropriate diagnostic tools and medical supplies will be key to managing the affected population and minimizing loss of life and potentially secondary civil unrest. Although a nuclear reactor incident like Fukushima, a dirty bomb, or nuclear detonation would result in vastly different numbers of individuals requiring medical treatment, the public's deep-set fear of radiation leads to these events being viewed as almost identical, and in each a large number of the "worried well" could overwhelm emergency response personnel and hospitals. A highly coordinated response with appropriate diagnostic tools and medical supplies is key to effectively managing the affected population and allocating scarce medical resources.

Difficulty testing for radiation dose

Clinical guidelines for the triage and treatment of individuals following a nuclear event are based on a combination of physical injury and absorbed radiation dose. An absorbed dose is measured in Gray (Gy), and individuals receiving a dose of greater than 0.7 Gy are likely to experience Acute Radiation Syndrome (ARS). Doses above 2.0 Gy start to require medical treatment, and 50% of people receiving 5 Gy will die without medical treatment. A total body dose of 8 Gy or higher is usually fatal even with intensive medical treatment.

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

***Bob Terbrueggen,** Ph.D., is the Founder and CEO of DxTerity Diagnostics, a molecular diagnostics company based in Los Angeles, California, USA. DxTerity specializes in the development of low cost, high throughput genomic tests. In September 2016, DxTerity was awarded a multi-year, $150 million contract by the Biomedical Advanced Research and Development Authority (BARDA), a division of the U.S. Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response, for the Advanced Development and Delivery of its REDI-Dx® High Throughput Radiation Biodosimetry Test. Prior to founding DxTerity, Bob was Director of Research and Development for Clinical Micro Sensors (CMS) and Motorola Life Sciences. Bob received his Ph.D. in Chemistry from the California Institute of Technology (CalTech), and his BS in Chemistry and Molecular Biology for the University of Michigan. Bob is an inventor on 20 approved U.S. patents and more than 20 pending applications.*

An Integrated Approach Used in Nuclear Security can be Adapted for Protecting Critical National Infrastructure

Source: http://www.torchmarketing.co.uk/wp-content/uploads/2018/05/WSRMayJun18.pdf

If a serious incident were to occur, either through accident or deliberate malicious action, the consequences can have national and international effects, as can be seen from the incidents at Fukushima Daiichi (2011), Chernobyl (1986) and Three Mile Island (1979).

Thus, to help prevent malicious threats against the industry there are international conventions, such as the Convention for the Physical Protection of Nuclear Material (CPPNM) and the United Nations (UN) International Convention for the Suppression of Acts of Nuclear Terrorism. Those conventions led to best relevant practice guidance published by the International Atomic Energy Agency (IAEA) in their Nuclear Security Series (NSS). Among the documents in the NSS are many that will be of value to all organisations that need to protect assets against threats.

INCORPORATING
REPORT
WORLD SECURITY REPORT
COVER STORY
STOPPING FOREIGN TERRORIST FIGHTERS – CAN API AND PNR PLAY A PART?

The nuclear industry uses an approach to threat that articulates the Design Basis Threat (DBT); a national document developed by the State for dutyholders, those companies and organisations that own and operate nuclear facilities, need to design, operate and maintain their Physical Protection System (PPS) to counter threats. Specific documents provide advice and guidance on the development and maintenance of the DBT; and issues such as countering the Insider Threat, a challenging subject relevant to all organisations whatever their focus may be.

All security departments need to understand their assets that need to be protected, and for the nuclear industry that does not just mean the obvious, such as nuclear material (NM) and operational reactors; nuclear power plants or research reactors. It can also involve the systems, structures and components (SSC) that maintain the safety arrangements for the NM, other radioactive materials such as sources, and the computer based systems important to safety (CBSIS) and security (CBSISy).

The cornerstone of every security plan is the identification of Vital Areas at nuclear facilities. This activity is the backbone that indicates the potential amount of material that could be subject to theft, and the potential significance of any unacceptable radiological consequences (URC) through the release of material. It is at this point, where security specialists need their safety colleagues, and those in plant or facility operations, to help in determining the assets to be protected.

The nuclear industry, to prevent nuclear material and other radioactive materials, from becoming a hazard to the public or environment, have three main specialist groups working towards that overall protection strategy; safety, security and safeguards; the Triple S. The aims for the individual specialisms are:

- Safety is aimed at protecting workers and the public from the harmful effects of radiation (or chemicals or other hazards);
- Security is aimed at preventing malicious acts that might harm a nuclear facility (sabotage) or result in the loss (theft) of nuclear materials; And
- Safeguards are aimed at preventing the diversion of nuclear materials from a civil nuclear programme to nuclear weapons purposes.

The 3Ss share the same overall objectives of protection and use similar principles to achieve protection; multiple barriers, defence in depth, decision analysis and consequence assessment. However, if they work predominantly in silos then compromises inevitably occur for operations and costs are inevitably higher than necessary.

However, as Safeguards is a uniquely nuclear consideration it will not be addressed further in this article.

Phasing out nuclear energy could affect safety: Psychologists

Source: http://www.homelandsecuritynewswire.com/dr20180606-phasing-out-nuclear-energy-could-affect-safety-psychologists

June 06 – **The way in which the phase-out of nuclear power plants in Germany is currently planned could negatively influence the safety of the facilities.** Those involved could increasingly favor their own interests as the shutdown date approaches, argue scientists from the University of Basel and the Max Planck Institute for Human Development in Berlin in the journal Behavioral Science & Policy. They base their argument on the possibility of endgame behavior from game theory.

After the reactor disaster in Fukushima in March 2011, the German government decided to **shut down eight power plants with immediate effect**. **The remaining nine facilities were given fixed shutdown dates; the last plant is planned to close in 2022.** The phase-out of nuclear power plants is also being discussed in Switzerland, after the nuclear phase-out initiative – which demanded the shutdown of nuclear power plants after a maximum of 45 years of operation – was rejected in November 2016.

Increasingly self-interested actors?

Basel says that the psychologists examined whether the impending shutdown dates of the operational nuclear power plants is leading to endgame behavior in the nuclear sector, for example in plant workers, managers, operators, suppliers, and authorities.

In game theory, endgame behavior means that players behave increasingly self-interested as a game draws to an end. When transferred into the context of the nuclear industry, this could mean that those involved on every level will increasingly put their own interests first. Such a tendency could have a negative impact on the safety of nuclear power plants.

The scientists used three approaches to examine whether there are indications of endgame behavior in the nuclear industry. They considered the behavior of players in the nuclear industry as portrayed in the public record; statistics on reportable events in nuclear power plants; and the safety behavior of participants in experimental studies.

Three approaches

- In media reports on phasing out nuclear energy in Germany, there is evidence that trust and cooperative behavior between the utilities and government decision-makers has become increasingly precarious since the phase-out decision in 2011. A loss of expertise and motivation in employees in the nuclear industry is also to be expected, caused by the foreseeable decline of an entire industry that many no longer perceive as offering attractive career opportunities.
- Contrary to their hypothesis, in the five years since the phase-out decision in 2011, the psychologists found no statistical increase in reportable events (accidents, malfunctions or other safety-related events in nuclear power plants). This would have been expected according to endgame behavior. However, a phase-out was also agreed back in 2001 between the nuclear utilities and the government. In the five-year period after this first phase-out decision, the number of reportable events rose by 39%.

- In behavior-based experiments, participants took on the role of managers. In several rounds, they had to decide if they wanted to invest in the safety of a power plant or not. If they did not invest, the likelihood of accidents increased. The results showed endgame behavior: by the end of the rounds, less was invested in safety. Only when the definite end point of the rounds was unknown did no endgame behavior emerge.

The human factor

The authors say that these results may be inconclusive, but it is essential to anticipate and analyze potential behavior-based consequences in the phase-out of safety-sensitive technologies and industries. "The human factor must not be overlooked during the concrete implementation of such decisions," says lead author Markus Schöbel. Politically motivated phase-out procedures could introduce new and unanticipated consequences for public safety.

— Read more in Markus Schöbel et al., "Phasing out a risky technology: An endgame problem in German nuclear power plants?" Behavioral Science & Policy 3, no. 2 (2017).

USA Today: Iran Opens New Nuclear Facility For Centrifuge Production

"Iran's nuclear chief on Wednesday inaugurated the Islamic Republic's new nuclear enrichment facility, geared toward producing centrifuges that will operate within the limits of the nuclear deal Tehran signed with world powers. Iranian state television broadcast an interview with Ali Akbar Salehi after nightfall, showcasing the facility at Natanz's uranium enrichment center. In the interview, Salehi said the facility's construction began even before the 2015 deal was signed and that he hopes the first centrifuges — known as old-generation centrifuges — will roll out in a month's time. In a gesture likely directed at the Trump administration's withdrawal from the deal, Iran informed the U.N. nuclear watchdog Tuesday that it would increase its nuclear enrichment capacity yet stay within the provisions of the accord. The landmark agreement, which lifted crippling economic sanctions in exchange for Tehran limiting its uranium enrichment program, has been facing its greatest diplomatic challenges in the wake of President Trump's decision to pull the United States out of it."

Construction Complete on Unit 1 of Barakah Nuclear Plant in UAE

Source: http://www.powermag.com/construction-complete-on-unit-1-of-barakah-nuclear-plant-in-uae/

May 01 – **The first of four nuclear reactors at the Barakah plant in the United Arab Emirates (UAE) was completed in late March, a milestone both for the UAE and for South Korea, which supplied the APR-1400 pressurized water reactor.**

The Barakah Nuclear Energy Plant (Figure 1) is the first nuclear plant in the UAE, and it marks the first time South Korea has exported its nuclear technology. The first APR-1400 entered commercial operation as Unit 3 at the Shin Kori site in South Korea in 2016. The Barakah plant will have generation capacity of about 5,600 MW with all four units in service.

A March 26 ceremony marked the culmination of a nine-year process to build the first nuclear plant in the Arab world. Emirates Nuclear Energy Corp. (ENEC) in December 2009 awarded the construction contract, estimated at about $20 billion, to a consortium led by Korea Electric Power Corp. (KEPCO). Sheikh Mohamed bin Zayed Al Nahyan, crown prince of Abu Dhabi, and South Korean President Moon Jae-in attended the ceremony at Barakah to mark the completion of Unit 1.

"This is a historic moment in our nation's development as we celebrate the construction completion of Unit 1 of the Barakah Nuclear Energy Plant," bin Zayed told WAM, the UAE's official news agency. "The UAE Peaceful Nuclear Energy Program will play a strategic role in the growth of our nation by enhancing our energy security, diversifying our economy, and creating employment opportunities for our people, thereby helping secure the future of generations to come."

The APR-1400 reactor has an expected operating life of 60 years. For Barakah, the reactor's design has been adapted for the UAE's extreme heat. Khaldoon Al Mubarak, chairman of ENEC, told WAM "This milestone is a testament to the vision and commitment of the UAE's leadership and the strength of ENEC's partnership with our prime contractor and joint venture partner, KEPCO. Now, our focus is on the transition to the safe start-up of Unit 1 nuclear operations."

Construction continues on the other three APR-1400 units at the site, which is located in the Dhafrah region of Abu Dhabi. According to ENEC, Unit 2 was more than 92% complete at the end of March. Unit 3 was about 81% complete, and Unit 4 was about 67% complete. Construction of all four units is expected to be complete by 2020.

Pre-operational tests, including cold hydrostatic testing, structural integrity testing, integrated leak rate testing, and hot functional testing, have been completed on Unit 1. The next phase is loading of fuel into the reactor, which will begin after Nawah Energy Co., the plant's operator, receives the operating license from the Federal Authority for Nuclear Regulation (FANR). Bloomberg reported that fuel loading is expected to begin this month, though no date has been set for Unit 1 to begin commercial operation.

The UAE's Ministry of Energy and Industry estimates the nuclear plant will eliminate at least 21 million metric tons of carbon emissions from the country's power generation each year. Current UAE generation comes almost entirely from natural gas-fired power plants; the country has said it wants to transition to generation almost entirely from nuclear and solar power

Detecting the threat of nuclear weapons

By Meg Murphy

Source: http://www.homelandsecuritynewswire.com/dr20180611-detecting-the-threat-of-nuclear-weapons

June 11 – Will the recent U.S. withdrawal from a 2015 accord that put restrictions on Iran's nuclear program make it easier for Iran to pursue the bomb in secret? Not likely, according to Scott Kemp, an associate professor of nuclear science and engineering at MIT.

"The most powerful insights into Iran's nuclear program come from traditional intelligence, not from inspections by the International Atomic Energy Agency," says Kemp, who this week published a commentary article in *Nature* on the interplay of policy and science in North Korea.

But covert nuclear-weapon programs, whether in Iran, North Korea, or elsewhere in the world, are a major unsolved problem, according to Kemp. He recently explained the technical challenges involved in the hunt for clandestine sites. And he floated a possible solution.

What inspectors look for

Inspectors want to search for the secret production of plutonium or highly enriched uranium, says Kemp. Manufacturing an actual explosive device can be accomplished quickly and discreetly once either of these ingredients is secured in enough quantity. "The assembly work can be done in an office building, underground facility, or even in a big kitchen. It's nearly impossible to detect once the program reaches this point."

The good news, relatively speaking, is that manufacturing these explosive materials can leave telltale clues.

"All international efforts to prevent nuclear proliferation focus on preventing the production of plutonium and highly enriched uranium," says Kemp. "The hope is to stop the material from ever being produced in the first place, or at least in sufficient quantities to make a nuclear bomb."

What are the telltale clues of covert production?

"The production of either plutonium or highly enriched uranium is a major operation that requires people and time," says Kemp. The involvement of many people means traditional intelligence has some chance of finding the program. But traditional intelligence can be unreliable, especially in closed societies like North Korea. Technical mechanisms would provide a useful overlay.

Detecting plutonium production, Kemp says, is easier than detecting enriched-uranium production for several reasons. The first clue is the heat signature. "Nearly all plutonium production occurs in nuclear reactors, and they obviously produce a lot of heat," he says. "There are clever things a country could do to hide the heat signature, but they are not simple. Infrared satellites can search for waste heat leaving buildings, or being pumped into rivers or oceans.

A second clue comes from chemical signatures. The processing of reactor fuel to extract plutonium creates chemical effluent, which could be another promising detection pathway. "In addition to plutonium, the nuclear reactor will also produce a mix of other radionuclides — and while most are trapped in the reactor, a few leak out to the environment," says Kemp, "especially the noble gases, such as radioactive isotopes of xenon and krypton."

Scientists may be able to detect these isotopes — xenon-131, xenon-135, and krypton-85 — when they seep into the environment. "Governments already use detectors to look for those small signatures of the operation," he says. "But a country could do all sorts of fancy things, like cryogenically freezing the off-gas, to eliminate the chemical signature if they wanted to. So we may or may not find signs of plutonium production this way."

And what about uranium enrichment? "It also produces a distinct chemical signature," says Kemp, which is caused when uranium hexafluoride (UF6) gas leaks into the atmosphere. The probability of a leak is very small, but it happens. When the gas escapes into open air, water vapor causes it to decompose into hydrofluoric acid and a specific kind of dust-like aerosol. The hydrofluoric acid is not useful in terms of detection. It is too reactive and disappears whenever it touches dirt, or a building, or a tree. "You are not going to detect it at any meaningful distance," says Kemp. But the other byproduct, the dust-like aerosol, is another story.

A new way to track secret nuclear activity

The dust produced by uranium enrichment is an aerosol called uranyl fluoride (UO2F2), and it has a chemical form that is unique to uranium processing operations, says. Kemp. He is interested in working with his colleagues on the engineering faculty to develop detectors that can identify the molecule's distinctive chemical bonds. "There are many techniques for identifying molecules, but the sensitivity required in this case is exceedingly high, and the aerosol form presents a number of other challenges," he says.

"If we could come up with extremely sensitive detectors that are cheap enough to put around a country without a lot of fancy equipment or maintenance, we would make significant inroads into the problem of detecting clandestine uranium-enrichment programs." Imagine, he says, something like small weather stations with a solar-powered box that has a tamper-proof seal on it. It has a tiny fan that blows air over a sensor that searches the telltale U-F bond, and then sends an alert signal if the molecule is detected.

"After a localized detection, you could use weather data to project backward and estimate the most probable places this molecule came from. If you could eventually narrow it down to a few buildings or a couple city blocks, then it would be feasible for international inspectors to request access under existing legal provisions to see what is inside."

A return to the politics

The ongoing presence of the International Atomic Energy Agency, which monitors Tehran's most sensitive factories and research labs, is provided for by the long-established Treaty on the Non-Proliferation of Nuclear Weapons, or NPT, which Iran is unlikely to withdraw from, says Kemp. That means inspection teams can continue to check known nuclear facilities as before.

However, a special provision, called the Additional Protocol, has allowed the IAEA to have wide-ranging access over the past three years, including the right to venture out to investigate tips about suspicious sites. This provision also permits the IAEA to deploy environmental sensors of the kind Kemp wants to build. It is these extra privileges that would be at risk if Iran withdraws from the 2015 accord, says Kemp. The IAEA has used these privileges to make at least 60 visits to facilities that are not part of Iran's declared nuclear program.

"But politics ultimately drives this in the end," he adds. "If inspectors learned something, whether from intelligence or sensors, but were refused the additional access needed to follow up on the lead, then the international community would probably presume the worst. It would therefore still be in Iran's interest to provide follow-up access even if they did not technically have to — that is, unless they were really hiding something."

— Also see R. Scott Kemp, "North Korean disarmament: build technology and trust," Nature (7 June 2018)

Meg Murphy *is Senior Writer & Media Relations Specialist at MIT School of Engineering.*

How North Korea got its nuclear weapons in the first place

Source: https://mic.com/articles/189659/how-north-korea-got-its-nuclear-weapons-in-the-first-place#.Wl6fG0kFW

June 10 – After weeks of uncertainty, the U.S. is set to meet with North Korea Tuesday in a historic summit to address the rogue nation's ongoing nuclear program.

The upcoming negotiations between President Donald Trump and North Korean leader Kim Jong Un come amid a history of escalating nuclear rhetoric between the two countries. Trump promised to respond to North Korea's nuclear threats with "fire and fury," while Kim — whom Trump once dubbed "Little Rocket Man" — has warned of a "nuclear button" in his office at all times as well as threatened missile strikes on the U.S. territory of Guam and the "heart of the U.S."

Conflict over North Korea's nuclear program is nothing new. Former President George W. Bush in 2002 labeled the country part of an "axis of evil" over its desire for weapons of mass destruction, and the United Nations has frequently condemned the country's nuclear program and imposed sanctions in response to nuclear and long-range missile tests that have been ongoing since 2006.

But how did this isolated, cash-strapped nation even acquire nuclear weapons in the first place? The country's nuclear program had been decades in the making prior to announcing it had nuclear weapons in April 2003. Its ambitions date back to the Korean War — and in developing its nuclear program, the Asian nation has had some outside help.

Korean War beginnings

North Korea's relationship with nuclear weapons can be traced back to the Korean War, when the U.S. — which had used the atomic bomb in Japan just a few years earlier — mulled making use of its nuclear weapons once again. President Harry Truman deployed B-29 bombers, which are capable of delivering nuclear bombs, as a sign that the U.S. was prepared and ready to use the weapons if necessary. He also said during a press conference that the U.S. was prepared to use nuclear force if necessary to win the war. Truman's successor, Dwight D. Eisenhower, also considered, but ultimately rejected, using nuclear weapons in Korea.

Though no nuclear weapons were ultimately used in the Korean War, the U.S.' actions had an effect on North Korea, and its leaders' desire to defend the country against a perceived nuclear threat. Under the regime of leader Kim Il-sung, North Korea began reestablishing chemical defense units even before the end of the Korean War, according to the U.S.-Korea Institute at Johns Hopkins University's School of Advanced International Studies. In the war's immediate aftermath, the country also established an Atomic Weapons Training Center to train its military units to conduct operations on an "atomic" battlefield.

Soviet assistance

Another conflict that had a huge impact on North Korea's nuclear ambitions was the Cold War, as the Soviet Union provided help to ally North Korea as the country developed its own nuclear energy program. In the wake of the Korean War, North Korea expanded a program that sent citizens to the Soviet Union to be trained as scientists and engineers, and the two countries signed nuclear cooperation agreements. North Korea was ultimately able to install its own atomic energy research centers in the early 1960s as well as its first nuclear reactor. The USSR also equipped North Korea with some equipment as well as advanced defensive nuclear, biological and chemical training.

Throughout the 1970s and '80s, tension simmered between Moscow and Pyongyang as North Korea rejected attempts by the international community to control its nuclear ambitions. North Korea embarked on the second phase of its nuclear program, which included the construction of new reactors, a radiochemical separation plant and research centers that put North Korea on its way to producing nuclear missile prototypes. In 1985, the Soviets committed to helping North Korea construct a nuclear power plant after the North Korea signed the Treaty on the Nonproliferation of Nuclear Weapons.

North Korea lost its key ally after the fall of the Soviet Union, as President Boris Yeltsin and the Russian government that took power announced it no would no longer honor the country's 1961 treaty of mutual defense and cooperation with North Korea.

Yet North Korea still benefitted from the Soviet's nuclear program. According to *Time* magazine, experts believe that North Korea would not have been able to create its nuclear arsenal without Russian and Ukranian technology, and the country has worked to acquire Soviet-era missile technology since 1991. As a result, North Korean missiles have often emulated Soviet-era missiles; the country's Hwasong-15 missile, which was tested in November 2017, is believed to be based on Soviet designs dating back to the mid-1960s.

It is also believed that North Korea made efforts to recruit former Soviet missile experts, though the Kremlin agreed to prohibit Russian scientists from working on the North Korean program after 60 Russian recruits set to aid North Korea's program were detained at a Moscow airport in 1992. Although *Time* noted it is difficult to prove whether Ukranian scientists went to work in North Korea after the country agreed to give up its Soviet-supplied weapons in 1994, missile designer Yuri Solomonov did note that Russian scientists worked on the North Korean nuclear program in the 1990s.

North Korea may potentially still be receiving help from Russia under current President Vladimir Putin, who ushered a treaty of friendship and cooperation between Russia and North Korea soon after taking office in 2000. The CIA reported the two countries signed a Defense Industry Cooperation Agreement in April 2001, which paved the way for arms sales and transfers to North Korea. The country has denied supporting North Korea's missile program.

There is also speculation over whether Ukraine is currently a source of North Korea's arms. A report released in August 2017 suggested North Korea's missiles could be traced back to a Ukranian factory, though the country denied having a connection to North Korea's missile program. In response to the report, Ukraine released surveillance footage to CNN showing a sting operation on North Korean spies attempting to gain nuclear information in 2011.

Other foreign influences

But Moscow and Kiev haven't been the only one to allegedly lend their assistance to North Korea's nuclear program. North Korea's other major ally, China, has also provided a range of assistance. According to PBS, it is believed that China contributed nuclear expertise and technology that has been incorporated into several of North Korea's missiles. At the same time, North Korean firms in China were used to procure materials for its nuclear program as of 2001, according to the CIA.

Egypt has also been a player in North Korea's nuclear history; the country provided North Korea with Soviet-supplied Scud missiles in the 1970s, which North Korea reverse engineered with help from China and Iran. And Pakistan provided military equipment and technical information that allowed North Korea to enrich uranium in exchange for $3 million in payments, documents published in 2011 by the *Washington Post* revealed. The alliance between North Korea and Pakistan extended to Iran as well, as all three countries shared information and technology, John Schilling, a North Korea expert and aerospace engineer, told the *Washington Post.*

Other countries have lent more inadvertent support. Hibbs told the *Atlantic* that North Korea developed the ability to create a plutonium separation plant after North Korean agents had "chatted up" Belgian scientists at a meeting in Vienna during the 1970s or '80s. A United Nations report in 2016 revealed that North Korea has evaded sanctions to develop its nuclear program by "embedding themselves in the transnational networks of foreign partners to conceal their prohibited activities."

While its efforts include allies in the Middle East, Asia and Africa, it also has involved the U.S.' European allies; Channel 4 reported that the country's "web of secretive front companies" around the world included a south London business that was secretly channeling up to £33 million a year to leader Kim Jong Un. The country has also used secretive tax havens to conceal its financial paper trails, including a firm set up by a British banker and registered in the British Virgin Islands.

As a result of North Korea's complex international network, the UN reported in 2014 that a North Korean missile found in 2012 contained "a number of foreign-sourced components," including items manufactured in the United Kingdom, U.S. and Switzerland. Most of the foreign-sourced items were not expressly prohibited, the report found, and Channel 4 noted the manufacturers were likely unaware the items would be used for North Korea's nuclear program.

North Korea's program is now more domestically based

All of this foreign assistance has allowed North Korea to become the nuclear power it is today. After initially signing both the Nuclear Nonproliferation Treaty in 1985 and an Agreed Framework with the U.S. in 1994, in which North Korea agreed to shut down its plutonium production, the country pulled out of the Nonproliferation Treaty and fully resumed its nuclear activities in 2003. North Korea claimed to have tested its first nuclear missile in 2006, before going on to complete another five nuclear tests through September 2017.

U.S. intelligence agencies cited by the *Washington Post* in March estimated that North Korea now has up to 60 nuclear warheads and has successfully produced a compact warhead capable of fitting in the payload of a ballistic missile.

Over time, the country's nuclear development has become more domestic, rather than relying on international support. Schilling told the *Washington Post* that though the country does need to import some components, North Korea is now "much more efficient and effective" at producing nuclear weapons itself.

"It doesn't need to be done on a large scale, and it doesn't need anyone else's active collaboration, so it would be very difficult to stop," Schilling told the *Post* about the country's nuclear program as it exists now.

While North Korea's nuclear development has been ongoing, its efforts have been ramped up in recent years by Kim Jong Un, who took power in 2013. Scott A. Snyder, a North Korea expert and a senior fellow at the Council on Foreign Relations, told the *Post* that much of North Korea's nuclear developments can now be attributed to Kim's regime and its focus on the nuclear program, as the leader has "stepped on the gas pedal" and made weapons development a key priority.

"When you have a strategic line, a single-minded focus on nuclear and economic development, and you're able to politically mobilize an entire state infrastructure to that end, it provides a lot of potential momentum," Snyder told the *Post*. "That's what Kim Jong Un has done."

The government's new contractor to run Los Alamos includes the same manager it effectively fired for safety problems

By Rebecca Moss

Source: http://www.homelandsecuritynewswire.com/dr20180611-the-government-s-new-contractor-to-run-los-alamos-includes-the-same-manager-it-effectively-fired-for-safety-problems

June 11 – Despite a lengthy record of safety violations, the University of California will continue its 75-year legacy of running Los Alamos National Laboratory, the U.S. Department of Energy and National Nuclear Security Administration announced Friday.

Los Alamos
National Laboratory

A management partnership that includes the university, research and development nonprofit Battelle Memorial Institute and Texas A&M University, the alma mater of Energy Secretary Rick Perry, will be paid $2.5 billion annually to run Los Alamos, the birthplace of the atomic bomb. They're calling their partnership Triad National Security LLC.

The contract could be worth upward of $25 billion over the next decade, with hundreds of millions of dollars more in performance-based bonus fees. Six other corporations will join the team in support roles.

"We are committed to building on the legacy of world-class research, unparalleled innovation and service to public good that have been the hallmark of the laboratory since it was founded in 1943," the University of California said in a joint statement with its new partners.

This is the second time the University of California has effectively maintained control over the laboratory despite concerns about serious mismanagement. In 2003, and again in 2015, the National Nuclear Security Administration said it would seek a new management contractor for the New Mexico lab following significant security breaches, costly accidents and injured employees.

The current management team, which also includes defense contractor Bechtel, amassed more than $110 million in fines and withheld bonuses because of health and safety issues. An electrical accident in 2015 left a worker hospitalized for over a month, and waste packaging errors led to a drum burst in 2014 at the Waste Isolation Pilot Plant in Carlsbad, exposing workers to radiation. The accident caused the storage facility to shut down for nearly three years.

The latest competition to run Los Alamos pitted the University of California's team against one led by its partner Bechtel and another that included the University of Texas system.

Critics of the lab questioned how the university emerged as a winner once again and how any serious overhaul of the lab's problems can occur if part of the existing leadership remains in place. Even the federal government called for a "culture change" at Los Alamos when it solicited bidders for the new lab contract last year.

This is a pivotal time for the lab. Los Alamos is expected to take on new nuclear work, building up to 30 plutonium pits per year. Producing the softball-sized plutonium metal cores, which trigger a reaction inside a nuclear weapon, is dangerous work, and Los Alamos has struggled to safely build even a single stockpile-ready pit in recent years.

The lab's entire plutonium facility was shut down in 2013 after workers nearly caused a deadly accident. Since production restarted in late 2015, workers have violated safety rules meant to prevent a runaway nuclear reaction, and several workers have been exposed to radiation.

Building new pits also requires the lab to handle significantly larger quantities of plutonium, a task that federal officials said would be a "learning curve" for the lab.

In announcing the new contract, Lisa E. Gordon-Hagerty, undersecretary for nuclear security at the Department of Energy and administrator of the National Nuclear Security Administration, called Los Alamos a vital national asset.

"The lab will continue to be a critical resource to ensure the future safety and security of the United States as we begin work on new endeavors," she said in statement.

David Jonas, a Washington, D.C., lawyer who previously served as general counsel of the National Nuclear Security Administration, said he thought Battelle, which will take a leading role alongside the University of California and has experience running seven other national labs, could help create the changes Los Alamos needs.

"We need to give them a chance," he said. "The question is then, if nothing changes, then what? And of course I don't have an answer for that."

Robert Alvarez, who was a senior policy adviser to Bill Richardson when he served as secretary of energy in the Clinton administration, said the lack of a contingency plan points to holes in the Energy Department's oversight system.

"One thing that really hasn't changed much is the lack of safety culture at the lab," Alvarez said. "It's a culture that lacks what you'd call an industrial safety ethos."

Since the Manhattan Project, the Department of Energy has been granted wide leeway to oversee its nuclear activity. Its contractors are largely indemnified from paying damages in the event of serious accidents and are not bound by the same rules as the private nuclear energy industry. The department's primary tools to penalize violations are issuing fines and withholding bonus awards. If all else fails, it can terminate a lab operator's contract, as it did with the current managers of Los Alamos.

"It is a low-risk environment, except when it comes to their reputation," Alvarez said of the contractors. "And even that, they overcome and reformulate into a different consortium — but it is usually the same cast of characters."

The new consortium will give Los Alamos the same primary managers as Lawrence Livermore National Laboratory in California, seen as its rival. UC, Texas A&M and Battelle have run Lawrence Livermore for the last decade.

The main loser in Friday's decision is Bechtel, which had submitted a contract bid under a team it formed with Purdue Unirsity.

A third bidder was the University of Texas and Boeing. A fourth team, first reported by the trade publication Exchange Monitor, included BWXT, Jacobs and Southeastern Universities Research Association.

Terry Wallace, director of Los Alamos National Laboratory, said in a statement that the lab is committed to working with the new management team.

"While the contract change will bring in a new team of parent companies, the laboratory's mission remains the same: to serve the nation in the tradition of excellence that has defined Los Alamos for the last 75 years," he said.

Alvarez said the only tool left to enforce better safety than in the past would be congressional oversight and withholding funds.

But, Alvarez said, "there has been no serious congressional oversight for several years."

***Rebecca Moss** covers energy and the environment, including Los Alamos National Laboratory, for the Santa Fe New Mexican.*

Deal signed to help keep Japan safe from nuclear terrorism during Tokyo 2020

Source: https://www.insidethegames.biz/articles/1061673/deal-signed-to-help-keep-japan-safe-from-nuclear-terrorism-during-tokyo-2020

Feb 2018 – The International Atomic Energy Agency (IAEA) has signed an agreement with the Japanese Government to work together in an effort to keep the 2020 Olympic and Paralympic Games safe from nuclear terrorism.

The agreement between IAEA's director general Yukiya Amano and Japanese Minister for Foreign Affairs Tarō Kōno was signed in Austria's capital Vienna, where the IAEA is based.

"We want to thoroughly cooperate with the IAEA to make sure the Olympics are safe," Kōno was reported as saying by Japan's *Kyodo News* before the meeting.

The IAEA, a United Nations agency, said in a statement that the possible areas of cooperation include it "offering Japanese authorities training courses, workshops, technical visits and exercises related to nuclear security, hosting preparatory technical meetings and lending supplementary radiation detection equipment".

"The know-how of the agency will boost the security of the Games," Norio Maruyama, spokesman for Japan's Minister for Foreign Affairs, told *Agence France-Presse.*

He added that although the agreement is not directly related to a nuclear threat from North Korea, "the uncertainty exists and we must use all means necessary to eliminate this uncertainty".

Relations between North Korea and Japan are severely strained at the moment. **North Korean citizens are currently banned from entering Japan.**

Experts: A 10-year phased denuclearization is safer for both U.S., NK

Source: http://www.homelandsecuritynewswire.com/dr20180613-experts-a-10year-phased-denuclearization-is-safer-for-both-u-s-nk

June 13 – Immediate denuclearization of North Korea is unrealistic, said Stanford scholars in an in-depth report released by the Stanford Center for International Security and Cooperation (CISAC).

Instead, denuclearization should be phased over a 10-year period to allow the United States to reduce and manage risks, said Siegfried Hecker, who authored the study with his research assistant Elliot Serbin and Robert Carlin, a visiting scholar at CISAC.

In the report, the scholars laid out a "roadmap" for denuclearization, recommending what they call a "halt, roll back and eliminate" approach. Their advice – which includes informative color charts and detailed, qualitative analysis – emerged from a longer-term project about the nuclear history of North Korea between 1992 and 2017.

Stanford says that according to the research, the most important steps toward denuclearization include halting nuclear tests, stopping intermediate or long-range missile tests, stopping the production of plutonium and highly enriched uranium, and banning all export of nuclear weapons, materials or technologies to North Korea.

"The roadmap lays out a reasonable timeline for denuclearization, but politics may delay final denuclearization as much as 15 years," said Hecker, who worked at the Los Alamos National Laboratory for almost two decades, where he served as its directors for eleven of those years. He joined CISAC as a senior fellow in 2005.

Building trust and interdependence

In the short term, North Korea and the United States should take steps to build trust and interdependence, which the researchers believe are pivotal for a viable long-term solution like complete demilitarization of North Korea's nuclear program. North Korea, they argue, will likely want to retain some parts of its nuclear program as a hedge should any potential agreement fall apart. This is a manageable risk, they said.

The scholars also encourage Pyongyang to front-load its concrete plan towards permanent nuclear dismantlement to make a phased approach more appealing to the U.S. administration. This would include actions like halting nuclear and missile tests for intercontinental ballistic missiles.

According to Hecker, North Korea's recent demolition of its nuclear test site is a significant step in that direction.

"The so-called 'Libya model' – complete and immediate denuclearization – is not a viable solution," Hecker said. "Our approach leaves each party with a manageable level of risk. Even though it takes longer, it is safer for the world."

Hecker also encouraged the US to recognize North Korea's desire for civilian programs, including energy production, the use of radioactive substances in medical research, diagnosis and treatment, and a peaceful space program. These types of civilian programs can also foster opportunities for a collaborative relationship between the United States and North Korea. Further, increased cooperation – including with South Korea – can help make efforts for verification and monitoring with the International Atomic Energy Agency (IAEA) more reliable. The verification process that will confirm to what extent North Korea dismantles and destroys its military nuclear program is a big issue for negotiations, the scholars said.

Recent reconciliation

Critically, the researchers note that recent détente between North Korea and South Korea provides a window of opportunity to accomplish denuclearization – and that the United States should take advantage of that window smartly. They said they hope that the risk-management approach outlined in the report can maximize chances for a successful agreement.

"In the past, the United States has missed opportunities to manage incremental risk," Hecker said. "Now is the time to pay attention to that history and be prepared to implement a risk-management approach to denuclearization."

— Read more in Siegfried S. Hecker, Robert L. Carlin, and Elliot A. Serbin, Comprehensive History of North Korea's Nuclear Program (CISAC, 2018).

Here's how many nuclear warheads it would take to wipe out the UK

By Jasper Hamill

Source: https://metro.co.uk/2018/06/14/nuclear-war-national-suicide-due-blowback-doomsday-weapons-scientists-warn-7630888/

June 14 – A new study has revealed how many nuclear weapons it would take to wipe out the 66 million people living in the UK.

The scientists calculated the grim consequences of launching just 100 nuclear warheads at China's most populated cities.

More than 30 million people were likely to die just in the initial blast, exceeding the death toll of even a severe pandemic.

The UK is significantly less densely packed than Chinese mega-cities, which means it would take somewhere between 200 and 300 nukes to polish off every human on these fair islands.

However, the research also found that any country that fired more than 100 nuclear warheads at a foe would also wipe out vast numbers of its own citizens.

Scientists found that the 'environmental blowback' of such an attack would lead to unacceptable losses – even if the enemy failed to retaliate – and said firing a large number of nukes would be 'national suicide'.

A major clash involving the use of 1,000 nuclear warheads by the US would result in 50 times more deaths of Americans than occurred in the 9/11 terrorist attacks, said the researchers.

And this was without a single nuclear strike on the US.

The study found that a nuclear arsenal of no more than 100 weapons provided a 'safe' level of deterrence.

A nation that launches nuclear attacks could end up in a very bad way itself due to a 'nuclear autumn'

Nine nations, the US, Russia, the UK, France, China, India, Pakistan, Israel and North Korea, collectively hold an estimated 15,000 nuclear warheads.

The US alone has 6,800 nuclear warheads, of which 1,800 are in active service and deployed.

Russia has 7,000 warheads and the UK 215, according to a report published last year by the US Defence Intelligence Agency.

The effects of 'environmental blowback' include lowered temperatures due to dust from burning cities blocking out sunlight, reduced rainfall, falling food production, the breakdown of supply chains, and increased levels of ultra-violet radiation, said the scientists in the journal Safety.

A 'nuclear autumn' triggered by lack of sun would be less severe than a 'nuclear winter' but would still result in agricultural losses ranging between 10% and 20%, according to the study.

The scientists predicted that food shortages would lead to severe rationing, starvation and numerous deaths due to civil disturbance.

Lead author Professor Joshua Pearce, from Michigan Technological University, said:"With 100 nuclear weapons you still get nuclear deterrence, but avoid the probable blowback from nuclear autumn that kills your own people.

'If we use 1,000 nuclear warheads against an enemy and no-one retaliates, we will see about 50 times more Americans die than did on 9/11 due to the after-effects of our own weapons.'

The September 9 2001, attack on New York by the al Qaida terror group using passenger jets flown into the twin towers of the World Trade Centre cost 2,977 innocent lives.

Americans Are Unprepared for a Nuclear Attack

By Gordon F. Sander

Source: http://www.politico.com/magazine/story/2018/06/11/would-you-know-what-to-do-during-a-nuclear-attack-218675

June 11 – **Let's say it is 2 p.m. on a Sunday afternoon, and you receive an emergency alert on your cellphone indicating that there has been a nuclear explosion in the next town or that an intercontinental ballistic missile is headed your way.**

Would you know what to do?

Most likely not.
"I would say that the United States is probably less prepared for any kind of nuclear detonation than it has been at any time since the Cold War," says Alex Wellerstein, a historian of science and technology at Stevens Institute of Technology in Hoboken, New Jersey. "And that is a dangerous place to be.''

Wellerstein, along with Kristyn Karl, a political psychology professor at Stevens, is pushing for the United States to bring back civil defense, the-all-but-forgotten federal Cold War-era program for preparing and responding to a nuclear event. Exactly what a revamped, 21st-century version of civil defense might look and sound like is the objective of a new project they are directing, called Reinventing Civil Defense. Started in 2016 and funded by the Carnegie Foundation, RCD boasts a diverse, high-powered advisory group that includes everyone from former Secretary of Defense William Perry to nuclear health physicists to screenwriters. The mission: Tell you what to do in the event of a nuclear crisis.

Although they might be aware of Kim Jong Un's threats to incinerate American cities or the latest line of Russia's hypersonic nuclear weapons most Americans—particularly younger ones who did not live through the most dangerous days of the Cold War—have no practical or conceptual idea of how to respond to the warning of an actual nuclear emergency. Witness the scenes of mass panic that took place in Hawaii last January after what, fortunately, turned out to be a false alert of an imminent North Korean attack.

Karl and Wellerstein, along with many other experts, lay much of the blame for this alarming nuclear unpreparedness among the general public on the federal government and its failure to communicate how to prepare for such an eventuality. "The government has given Americans no good sense of what, specifically, to do when the next nuclear crisis occurs," says Michael O'Hanlon, a senior fellow at the Brookings Institution.

To be sure, this is not an easy task. The original version of civil defense (also known as Duck and Cover, after its famed guidance to schoolchildren to protect themselves from a nuclear attack by ducking under their school desks when they saw the tell-tale flash outside) is often remembered as silly and misleading—particularly the impression it gave about how easy it would be to survive a full-scale nuclear war. But Wellerstein and Karl feel that a lot about the original, oft-mocked program was constructive and worth resurrecting—particularly the fact that, at the very least, it did get Americans to think about the unthinkable.

International events seem to be pushing the initiative along. Last fall, after North Korea successfully tested its first intercontinental ballistic missile and threatened to use it against the U.S., "the project took on much higher stakes,'' says Wellerstein, who, at 36, is best known for NUKEMAP, his Google Maps mash-up that allows one to calculate the effect of a nuclear detonation based on factors such as targeted city and nuclear yield.

And Wellerstein doesn't feel this development is necessarily an unwelcome one. For years, "the assumption was that anyone who cared about civil defense had to be either a Cold War holdover or 'a doomsday prepper,'" he says. "Neither Kristyn or I are either of those things," he says. "Basically we just want people to think about nuclear risk—even if they don't want to think about it.''

***

There at least three different types of credible nuclear threats that exist today—two more than during the *Dr. Strangelove* days.

Scenario 1 is the fear that set the original civil defense program in motion—an apocalyptic exchange between the United States and Russia or China involving hundreds of thermonuclear weapons. The U.S. population would theoretically have a 20- to 30-minute warning before the multi-megaton bombs began bursting in air, spreading radioactive fallout in overlapping lethal circles and the lights started going out—for good.

Scenario 2 is the nuclear terrorist scenario, i.e., the detonation of a smaller, 10-kiloton device in a major American city. Those fortunate enough not to be among the tens of thousands killed during the initial blast would have a short time to protect themselves from the subsequent, less serious fallout.

Scenario 3 is the recently emergent North Korea scenario, involving the airburst of a 100- or 150-kiloton device over an American city, perhaps Los Angeles, with, hopefully, a 30-minute warning. The result, according to NUKEMAP,would range from an estimated 195,000 to 241,000 deaths and 510,000 to 629,000 injuries from both the blast and radioactive fallout, depending on the bomb's yield.

Scenarios 2 and 3 are the most likely—and also the ones that the RCD researchers are focused on (for the moment, at least). They are also survivable, if you and emergency management officials know how to respond.

But RCD's first challenge is how to untangle the star-crossed history of the first version of civil defense, says Wellerstein.

It all began with Bert the Turtle—the smiling, helmet-adorned mascot of the first, much-derided civil defense program, which was run by the Federal Civil Defense Administration (the ancestor of the Federal Emergency Management Administration). Bert is the star of a famous 1951 instructional cartoon, called *Duck and Cove*r.

"Bert the Turtle walks down the road," goes the chorus in the famed serial, as our smiling hero confidently sashays down the road in the cartoon. "And Bert the Turtle was very alert, when dangers threatened him he never got hurt. He knew just what to do."

The reason Bert and his fellow Americans knew what to do was that they were familiar with the instructions in the upbeat government pamphlet *Survival Under Atomic Attack.* "You can live through an atom bomb raid and you don't need a Geiger counter or special training to do it!" the leaflet fatuously advised. "You should hide underground if there is time. Otherwise, you should jump into the nearest gutter or ditch. And don't forget to shut the window!"

Since then, the issue and practice of civil defense waxed and waned with the rise and fall of international tensions over the following decades, along with the evolving outlook and experiences of the chief occupants of the White House, as historian Rodric Braithwaite writes in his new history of the nuclear threat, *Armageddon and Paranoia*.

President John F. Kennedy, who took office in January 1961, at the start of the second, tensest decade of the Cold War, was a big booster of civil defense. As part of the program, the president announced the federal government would initiate a $700 million nationwide fallout shelter plan, while also encouraging Americans to build their own fallout shelters. Kennedy's brother Robert was an even greater civil defense enthusiast. He pressed for a scheme that would require all American citizens to practice evacuation and shelter drills once a week.

As Braithwaite writes, "a kind of hysteria" about the subject of civil defense and nuclear safety ensued. At the height of the craziness, in a column for the Catholic magazine *America*, the Rev. L.C. McHugh actually argued that it was permissible "to shoot your neighbors if they tried to break into your fallout shelter."

The high anxiety of those thermonuclear times seeped into popular culture. In "The Shelter," an episode of the popular TV program *The Twilight Zone*, a celebratory party for a doctor who has heeded JFK's advice and built a bomb shelter takes a terrifying turn after a radio broadcast announces unidentified objects heading for the United States. Of course, in those uneasy days, everyone assumes the objects are ICBMs.

Within minutes the amicable group has besieged the shelter to which the doctor has fled with his family, while the latter chastises his hysterical friends for not building their own shelters "because it meant recognizing the kind of world we live in." Just as the frenzied group is about to burst in comes another announcement on the radio: The unidentified objects are in fact harmless satellites.

Eventually, Kennedy's interest in civil defense waned as he became convinced of the impracticality of a nationwide shelter program, as well as the unwinnability of nuclear war. (As Harvard economist and key Kennedy adviser John Kenneth Galbraith wrote in a personal letter to the president, "Those Americans who did manage to survive a nuclear exchange would emerge into a desolate world "with no food, no transportation and full of stinking corpses.") So did the skeptical Congress, which whittled JFK's request for $700 million down to a mere $80 million.

Jimmy Carter tried to inject new life into the civil defense program by creating the Federal Emergency Management Agency in 1979. FEMA consolidated the work of several agencies into one, mixing nuclear preparedness with preparedness for floods, tornadoes and earthquakes. But the nuclear issue took a back seat.

Ronald Reagan, who came into office convinced that the Soviet Union's nuclear arsenal had overtaken that of the United States, conflated civil defense with the national defense. "[The Reagan hawks] believed that civil defense was part of being prepared to fight a nuclear war with the Evil Empire and that being thus prepared *was* necessary for deterrence," Wellerstein says. "So it fit very firmly into their political ideology." Toward that end, in 1982, the Reagan administration proposed a comprehensive civil defense program costing $4.2 billion.

However, Reagan, like Kennedy, lost interest in the program once he became convinced that nuclear war was unwinnable and unsurvivable. Instead, he decided to direct the nation's monies towards building up *other* elements of the national defense—like his proposed missile shield known as Star Wars. Congress lost interest as well.

Thus, in July 1986, in a report to Congress, FEMA could state that "U.S. civil defense capabilities are low and declining." "National survival would be in jeopardy" in the event of a nuclear attack, it declared, while asking for a mere $130 million to keep the network of emergency operation centers established 20 years before at a minimal functioning level—an amount that was further pared down.

By then, says Wellerstein, the concept of civil defense had become so fraught in the public's imagination as to obscure what was useful about it, including and particularly keeping the idea of nuclear risk in the forefront of the public imagination.

"The Cold War perceptions are unfortunately the ones that guide a lot of our discussions about civil defense and nuclear preparedness today," he maintains, "even though the strategic situation of today is very much different than it was then."

Ironically, as Braithwaite writes, "the cheery recommendations in *Duck and Cover* and 'Survival under Atomic Attack' would have been of little use against a strategic bombardment by thermonuclear weapons"—Scenario 1. But they would work, more or less, in the more likely and survivable scenarios 2 and 3.

It seems that Bert the Turtle had the right message at the wrong time.

***

You might be surprised to hear that Uncle Sam has a cogent message about what the public should do in case of a nuclear attack.

The advice is basically a revised version of Duck and Cover: Get Inside, Stay Inside, Stay Tuned.

Broken down, that means once you receive a warning or alert of a nuclear detonation you should get inside the nearest building or other standing (preferably concrete) structure, stay there for at least 12 to 24 hours—the period when the outdoor fallout radiation level is most dangerous and wait for further news from emergency management officials about which areas downwind from the blast are safest to evacuate to next.

One of the chief progenitors of that advice is Brooke Buddemeier, a certified health physicist at Lawrence Livermore Laboratory in California. Buddemeier, who has been on the staff of Livermore since 1989, is also on the advisory board of Reinventing Civil Defense.

Buddemeier concedes that until recently he and his colleagues have been focused on what would happen, and how the public should respond to a Scenario 2 level event—a terrorist attack. But he points out that the same slogan would also apply for a Level 3 event. ''I cannot speak to theoretical yields of any specific nation-state,'' the government scientist says. But, he maintains, the basic message which he and his colleagues at Livermore and their sister federal agencies are trying to put out there *would* work for, say, a Level 3 missile strike on California by parties unknown.

Incidentally, Buddemeier is decidedly not a booster of the bomb shelter business, which has seen a surge on the West Coast in recent months, as fears of a possible North Korean attack have risen. ''I'm glad that people are thinking about emergency/disaster preparedness," he says. ''However, I hope that the concern for the nuclear threat does not result in anxiety, depression or using your savings on expensive preparedness measures." He points out that, even if you had a shelter, most likely you would not be able to reach it in time to protect you and your loved ones.

It all sounds very sensible, if grim. So, *where are these recommendations*? Why haven't we seen them?

It turns out they are located on page 66 of a 130-page document compiled by a federal interagency committee in 2010 known as "Planning Guidance for Response to a Nuclear Detonation." It reads: "The best initial action following a nuclear explosion is to take shelter in the nearest and most protective building or structure and listen for instructions from authorities."

Former Secretary of Defense William Perry says he has "mixed feelings" about civil defense. His own nuclear educational project, the William J. Perry Project, aims to educate the public on the dangers of *all* the aforementioned nuclear scenarios, including the Armaggedon-level Scenario 1 for which he believes the only and best defense is disarmament. "I believe that there is NO level of civil defense that could provide meaningful protection against a large scale nuclear attack," he says.

However, Perry acknowledges, referring to the Level 3, nuclear terrorist scenario, "there *is* much that could be done to lower the casualties of a terror-based nuclear attack," including better educating the public about what to do before, as well as after such an attack. "But we are not doing these things."

Perry was one of the participants in the Preventive Defense Project, a group of leading federal government civilian and military officials, scientists and policy experts who convened in Washington in 2007, five years after the 9/11 attacks, to answer the then much more urgent question, "On the day after a nuclear weapon goes off in a U.S. city, what will we wish we have done to prevent it?"

Perry co-authored the report that came out of the meeting. Entitled "The Day After: Action Following a Nuclear Blast in a U.S. City," the bluntly expressed document called the federal government to account for not yet coming up with a realistic contingency plan for dealing with the aftermath of a nuclear terrorist incident, or "informing the American public of its particulars."

"Remarkably such a plan does not yet exist," wrote the authors, who also included future Secretary of Defense Ashton Carter, "although," they added hopefully, "it is being drafted." Perry, et al., also recommended a new type of fallout shelter program supplied with stocks of food, water and other supplies for several days, somewhere along the lines of the thousands of shelters with which civil defense-minded Switzerland has equipped its towns and cities, as well as a computer modeling system for rapidly measuring radiation to enable both emergency workers and the public to determine the safest zones downwind from the blast.

Ten years later, as Perry notes, it is questionable whether these measures have been taken. Although, the government does have a rapid radiation modeling capability, there has been little movement on the national fallout shelter system idea.

As far as the contingency plan is concerned, in her response to this reporter's query, Michelle Laver, director of strategic communications for the National Nuclear Safety Administration, notes that since 2007 "federal teams have worked together to issue documents on nuclear and radiological response, including the now eight-year-old Nuclear/Radiological Incident Annex."

"Additionally," Laver adds, in the patois of the preparedness bureaucracy, "federal communicators have developed interagency guidance in the form of the Emergency Support Function 15 Standard Operating Procedure and Annex Nuclear to Emergency Support Function 15 External Affairs: Radiological."

Whether either the clunky, hard-to-find "Planning Guidance for a Nuclear Detonation" mentioned above, or the highly technical annex and its addenda comprise the contingency plan called for in "The Day After" is debatable.

What is inarguable is that the public was never informed of its particulars. Or, as Wellerstein notes, "A lot of guidelines on how the government should communicate with the public, but almost no communication with the public. FEMA has suddenly shown a lot of interest in this," he says, "but it's clear that for the last few decades this sort of threat has been on the back burner for them.''

''There is some irony there," he continues, ''in that FEMA was created in part to consolidate and encourage civil defense planning."

***

Finding a better way of conveying crucial nuclear survival advice to the public is the essential challenge that the Reinventing Civil Defense investigators have set themselves.

For the record, Wellerstein emphasizes, RCD is occupied with the communications dimension of the next generation of civil defense, rather than the practical one, as it were. "We are not doing research into what one *ought* to do. We are leaving that to the labs and their experts. We are looking instead into what a communication program might look like. So we take for granted the models used by emergency planning can do what they are supposed to do."

Wellerstein adds that RCD has no formal relationship with the federal government: "Although at least one government employee"—Buddemeier—"is involved in an advisory way and we have been talking to people who work for the government. But, he adds, "we aren't taking money from them and they are not obligated to take anything from us. We hope our work will be useful to the government but our scope is not limited to things FEMA could do."

So what sorts of things *is* RCD doing? For one, there's, "Drawing Doomsday: Using Comics for Civil Defense,'' a graphic novel project designed to "apply the tools of visual storytelling to a reinvented Civil Defense." There's also "Nuclear Worriers: Stories From a Nuclear World"—"a podcast and network for communicating stories relating to nuclear risk and salience among the public." And then there's the darker "Mark 17 User's Manual," "a graphic fictional operation and maintenance guide" to the first 15-kiloton, 1957 model U.S. hydrogen bomb.

Those are just some of the subprojects that the RCD principals have commissioned from the artists and writers they are working with as part of their cutting edge initiative.

"Times have changed, and the way we communicate with each other has changed, too," says Karl, who oversees the new-media end of the RCD. "We believe it is important to meet people where they are. The things that capture our attention, particularly among millennials and younger generations, have also shifted," she explains.

As far as Buddemeier's advice about how your family *can* survive a nuclear detonation, Wellerstein would prefer to alter his adviser's message. "If I had my druthers, I would change the 'can' in 'your family can survive a nuclear detonation' to '*might'* survive. I think any communication about nuclear attacks needs to emphasize that the number of dead would be staggering, even with perfect execution of civil defense procedures."

This, to Wellerstein is one of the reasons it is important for today's civil defense planners to study the Civil Defense messaging of the 1950s and '60s, as the RCD group is now doing. ''One of the ways the early Cold War messaging went wrong is that it overemphasized the ease of surviving a nuclear attack."

"It's a tricky balance," he concedes. Wellerstein also thinks that the ''stay tuned'' part of Buddemeier's mantra may be too hopeful. ''Will people have telephones or the internet after a nuclear detonation? I don't know." He adds, "I am not sure that the government *can* communicate on this as openly as they ought to. But there are many ways for a nongovernmental entity to do this."

The basic problem, Buddemeier and Wellerstein agree, is that the message isn't really getting out there at all, as seen by last January's chaotic scenes in Hawaii.

For his part, Buddemeier continues to be a big fan of RCD. "I think it's a great program," he says, particularly in the way RCD is trying to identify "new and effective means, including apps and games to help bring a little bit of knowledge that can save a lot of lives. I believe it is important to motivate personal preparedness by making it interesting—or even fun—and not by fear."

"'Stop, Drop and Roll' doesn't make you afraid of fire," he adds, "but it can save your life in the unlikely event that your clothes catch fire."

For her part, Michelle Laver, head of strategic communications for the National Nuclear Safety Administration, says that, thanks to January's false alert, federal and state officials ''are working harder to better educate the public in safety measures that can be taken in case of a nuclear incident." Stay tuned.

''There are many things one can say about the [Hawaiian] episode,'' says Wellerstein. ''I worry that a false alarm like that, based on such a basic miscommunication, has undermined public confidence in such warnings.''

But, on the other hand, he says, ''Until recently, if you want to make [the possibility of a nuclear detonation] heard then you really had to come up with complex arguments about why it was still relevant."

Now thanks to recent events, he says, ''we don't have to do that anymore."

"I am not convinced that the scale of the next generation of CD ought to be the same as it was during the Cold War," says Karl. "But if you believe the threat is non-zero and that there are steps we can take to minimize the negative impact on society and save lives, that seems like an easy calculation to me."

***Gordon F. Sander** is a journalist and historian who frequently writes about national security. He also is the author of Serling, a biography of Rod Serling, among other books.*

EDITORIAL TEAM'S COMMENTS: (1) Given our generally poor overall record in responding to "normal" events like hurricanes (though we are getting much better over the last few years) which are almost guaranteed to happen every year, or floods which happen as frequently, focusing on a very low probability, high impact event like a nuke seems a little silly. Perhaps if the country were more generally prepared, resilient and informed about ALL hazards, and actually took action to be self-reliant rather than looking for someone else to save them, we might be better off overall as a nation, not just fail to be prepared for a single massive, low probability high impact incident. (2) If the US is not adequately prepared, then the rest of us are just dead and we are not aware of that!

Human Radiation Detectors Now In Service

Source: https://i-hls.com/archives/66594

Nov 2015 – The problem with nuclear radiation is that by the time you can detect it, it's usually too late. By the time seismographs, infrasound sensors, and radiation readers pick up on a blast, it's already happened. Catching a nuclear weapon before it goes off is a lot trickier. Tricky, but not impossible.

The Department of Homeland Security (DHS) recently announced a program to develop **wearable technologies, similar to smartwatches, that can detect nuclear bomb threats and other radioactive material.** This means, basically, that people will become human radiation detectors.

The project has been in the works for a while; the DHS posted the first notice of the contract in June 2014. The original solicitation called for a system "capable of detecting and identifying radiation/nuclear threats, storing the identification results, and communicating those results in real-time (wired and/or wireless)" to ReachBack, a chemical and radiation threat analysis center. In September, the DHS awarded the $24 million contract to **FLIR** Detection. They are calling it the **"Human Portable Tripwire"** (HPT).

The DHS plans to distribute the HPT device to Coast Guard, Customs and Border Protection, and Transportation Security Administration personnel.

"This device has the capability to identify the source of radiation and allow personnel to take appropriate action," said director of the DHS's Domestic Nuclear Detection Office Huban Gowadia. "These devices are a critical tool for personnel who operate in the maritime environment, at land and sea ports of entry, and within the United States."

According to a 2014 report by Fierce Homeland Security, Gowadia said at a House subcommittee hearing that each device would cost nearly $1 million. "The ceiling on the contract is $24 million and our minimum buy is 26," she said at the time.

"Think of our Border Patrol officers who are sometimes very far removed from the nearest identification device," said Gowadia in the hearing about how the device would be used, according to the report. "So it would be so much more efficient and convenient in their daily operations to have both capabilities built into one. And that's what these systems were designed to do: detect, identify and store for archival and retrieval purposes that information on board that system."

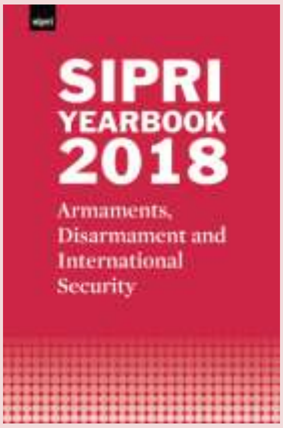
Modernization of nuclear arsenals continues

Source: http://www.homelandsecuritynewswire.com/dr20180618-modernization-of-nuclear-arsenals-continues

June 18 – A new report finds that all the nuclear weapon-possessing states are developing new nuclear weapon systems and modernizing their existing systems. **Nine states—the United States, Russia, the United Kingdom, France, China, India, Pakistan, Israel, and North Korea—possess approximately 14,465 nuclear weapons**. This marked a decrease from the approximately **14,935** nuclear weapons these states were estimated to possess at the beginning of **2017**.

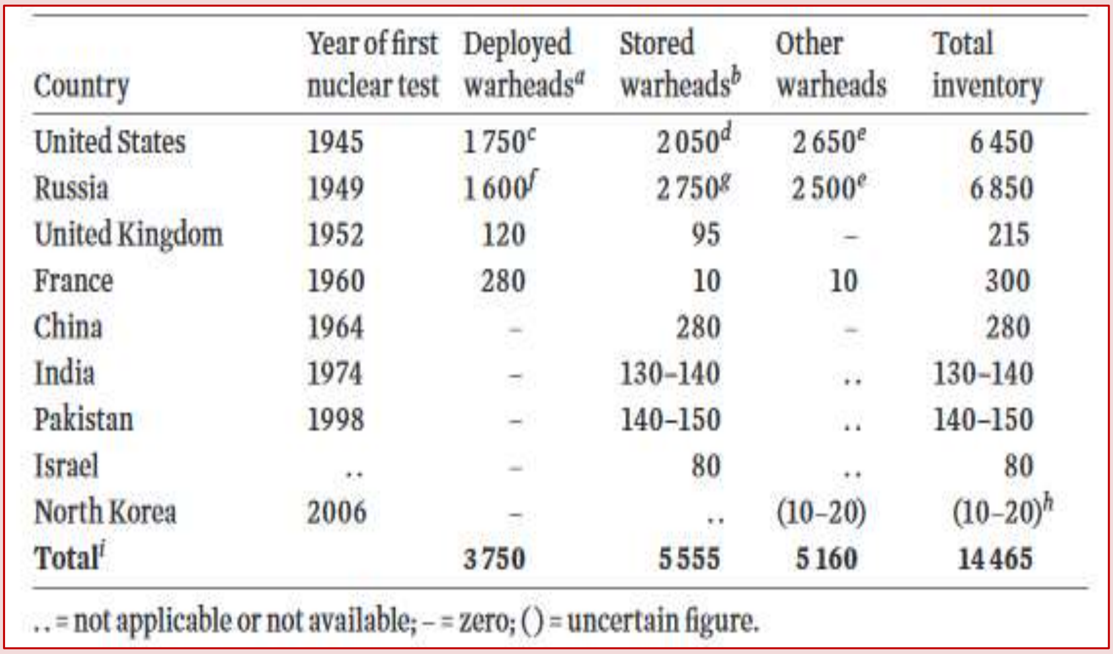
The Stockholm International Peace Research Institute (SIPRI) today (Monday, 18 June) released the findings of SIPRI Yearbook 2018, which assesses the current state of armaments, disarmament and international security. Among the key findings: All the nuclear weapon-possessing states are developing new nuclear weapon systems and modernizing their existing systems.

At the start of 2018 nine states—the United States, Russia, the United Kingdom, France, China, India, Pakistan, Israel, and the Democratic People's Republic of Korea (North Korea)—possessed approximately 14,465 nuclear weapons. This marked a decrease from the approximately 14,935 nuclear weapons that SIPRI estimated these states possessed at the beginning of 2017.



The decrease in the overall number of nuclear weapons in the world is due mainly to Russia and the United States—which together still account for nearly 92 percent of all nuclear weapons—further reducing their strategic nuclear forces pursuant to the implementation of the 2010 Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START).

SIPRI notes that despite making limited reductions to their nuclear forces, both Russia and the United States have long-term programs under way to replace and modernize their nuclear warheads, missile and aircraft delivery systems, and nuclear weapon production facilities. The United States most recent Nuclear Posture Review (NPR), published in February 2018, reaffirmed the modernization programs and approved the development of new nuclear weapons. The NPR also emphasized expanding nuclear options to deter and, if necessary, defeat both nuclear and 'non-nuclear strategic attacks'.



Country	Year of first nuclear test	Deployed warheads[a]	Stored warheads[b]	Other warheads	Total inventory
United States	1945	1 750[c]	2 050[d]	2 650[e]	6 450
Russia	1949	1 600[f]	2 750[g]	2 500[e]	6 850
United Kingdom	1952	120	95	–	215
France	1960	280	10	10	300
China	1964	–	280	–	280
India	1974	–	130–140	..	130–140
Pakistan	1998	–	140–150	..	140–150
Israel	..	–	80	..	80
North Korea	2006	–	..	(10–20)	(10–20)[h]
Total[i]		**3 750**	**5 555**	**5 160**	**14 465**

.. = not applicable or not available; – = zero; () = uncertain figure.

World nuclear forces, January 2018 (SIPRI)

"The renewed focus on the strategic importance of nuclear deterrence and capacity is a very worrying trend," says Ambassador Jan Eliasson, Chair of the SIPRI Governing Board. "The world needs a clear commitment from the nuclear weapon states to an effective, legally binding process towards nuclear disarmament."

The nuclear arsenals of the other nuclear-armed states are considerably smaller, but all are either developing or deploying new nuclear weapon systems or have announced their intention to do so. India and Pakistan are both expanding their nuclear weapon stockpiles as well as developing new land-, sea- and air-based missile delivery systems. China continues to modernize its nuclear weapon delivery systems and is slowly increasing the size of its nuclear arsenal.

In 2017 North Korea continued to make technical progress in developing its nuclear weapon capabilities, including the test of—what was claimed to be—a thermonuclear weapon, in September. North Korea also demonstrated unexpected rapid progress in the testing of two new types of long-range ballistic missile delivery systems.

"Despite the clear international interest in nuclear disarmament reflected in the conclusion in 2017 of the Treaty on the Prohibition of Nuclear Weapons, the modernization programmes under way in the nuclear weapon-possessing states indicate that genuine progress towards nuclear disarmament will remain a distant goal," says Shannon Kile, Senior Researcher with the SIPRI Disarmament, Arms Control and Non-proliferation Program.

— Read more in SIPRI Yearbook 2018 (SIPRI, June 2018)

Enhanced detection of nuclear events thanks to deep learning

Source: http://www.homelandsecuritynewswire.com/dr20180622-enhanced-detection-of-nuclear-events-thanks-to-deep-learning

June 22 – A deep neural network running on an ordinary desktop computer is interpreting highly technical data related to national security as well as — and sometimes better than — today's best automated methods or even human experts.

The progress tackling some of the most complex problems of the environment, the cosmos and national security comes from scientists at the Department of Energy's Pacific Northwest National Laboratory who presented their work at the 11th MARC conference — Methods and Applications of Radioanalytical Chemistry — in April in Hawaii. Their work employs deep learning, in which machines are enabled to learn and make decisions without being explicitly programmed for all conditions.

PNNL says that the research probes incredibly complex data sets from the laboratory's shallow underground lab, where scientists detect the faintest of signals from a planet abuzz in activity. In the laboratory buried 81 feet beneath concrete, rock and earth, thick shielding dampens signals from cosmic rays, electronics and other sources. That allows PNNL scientists to isolate and decipher signals of interest collected from anywhere on the planet.

Those signals signify events called radioactive decays, when a particle such as an electron is emitted from an atom. The process is happening constantly, through both natural and human activity. Scientists can monitor changes in levels of argon-37, which could indicate prior nuclear test activity, and argon-39, whose levels help scientists determine the age of groundwater and learn more about the planet.

The lab has accumulated data on millions of radioactive decay events since it opened in 2010. But it's a noisy world out there, especially for scientists listening for very rare signals that are easily confused with signals of a different and frequently routine origin — for instance, a person flipping on a light switch or receiving a call on a cell phone.

PNNL scientist Emily Mace, who presented at MARC, is an expert in interpreting the features of such signals — when an event might indicate underground nuclear testing, for example, or a rapidly depleting aquifer. Much like physicians peruse X-rays for hints of disease, Mace and her colleagues pore over radioactive decay event data regularly to interpret the signals — their energy, timing, peaks, slopes, duration, and other features.

"Some pulse shapes are difficult to interpret," said Mace. "It can be challenging to differentiate between good and bad data."

Recently Mace and colleagues turned for input to their colleagues who are experts in deep learning, an exciting and active subfield of artificial intelligence. Jesse Ward is one of dozens of deep learning experts at the lab who are exploring several applications through PNNL's Deep Learning for Scientific Discovery Agile Investment. Mace sent Ward information on nearly 2 million energy pulses detected in the Shallow Underground Laboratory since 2010.

Ward used a clean sample set of 32,000 pulses to train the network, inputting many features of each pulse and showing the network how the data was interpreted. Then he fed the network thousands more signals as it taught itself to differentiate between "good" signals that showed something of interest and "bad" signals that amounted to unwanted noise. Finally, he tested the network, feeding it increasingly complex sets of data that are difficult even for experts to interpret.

The network he created interprets pulse shape events with an accuracy that equals and sometimes surpasses the know-how of experts like Mace. With straightforward data, the program sorted more than 99.9 percent of the pulses correctly.

Results are even more impressive when the data is noisy and includes an avalanche of spurious signals:

- In an analysis involving 50,000 pulses, the neural network agreed 100 percent of the time with the human expert, besting the best conventional computerized techniques which agreed with the expert 99.8 percent of the time.
- In another analysis of 10,000 pulses, the neural net correctly identified 99.9 percent of pulses compared to 96.1 percent with the conventional technique. Included in this analysis were the toughest pulses to interpret; with that subset, the neural network did more than 25 times better, correctly classifying 386 out of 400 pulses compared to 14 of 400 for the conventional technique.

"This is a relatively simple neural network but the results are impressive," said Ward. "You can do productive work on important scientific problems with a fairly primitive machine. It's exciting to consider what else is possible."

The project posed an unexpected challenge, however: The shallow underground lab is so pristine, with most spurious noise signals mitigated before they enter the data stream, that Ward found himself asking Mace for more bad data.

"Signals can be well behaved or they can be poorly behaved," said Ward. "For the network to learn about the good signals, it needs a decent amount of bad signals for comparison."

The problem of culling through vast amounts of data looking for meaningful signals has a raft of implications and extends to many areas of science. At PNNL, one area is the search for signals that would result from dark matter, the vast portion of matter in our universe whose origin and whereabouts is unknown. Another is the automatic detection of breast cancers and other tissue anomalies.

"Deep learning is making it easier for us to filter out a small number of good events that are indicative of the activity of interest," said Craig Aalseth, nuclear physicist and PNNL laboratory fellow. "It's great to see deep-learning techniques actually doing a better job than our previous best detection techniques."

Nuclear Sites Receive Counter-Drone Defense

Source: https://i-hls.com/archives/83620

June 21 – One of the US premier nuclear weapons labs now has the capability to disable drones or any other unauthorized unmanned aircraft systems flying over its restricted airspace in a swath of northern New Mexico. The airspace over the lab received an additional no drone zone designation by the Federal Aviation Administration.

The system is Government authorized and is currently in an operational testing phase. Officials at the Los Alamos National Laboratory say they're testing the new system that could serve as a model for other federal installations.

"All airspace over the laboratory is protected right now against unauthorized drone or UAV flights," said Michael Lansing, head of the lab's security operations. "We can detect and track a UAV and if it poses a threat we have the ability to disrupt control of the system, seize or exercise control, confiscate, or use reasonable force to disable, damage or destroy the UAV."

The lab worked with the National Nuclear Security Administration and the FAA to implement the system. The NNSA received authorization from Congress last year to implement enhanced security measures to protect its sites from drones, according to pressherald.com.

"Implementation guidance by NNSA focuses on high-level actions to be taken to detect, identify, track and mitigate drones that pose a threat to NNSA covered facilities," said Lewis Monroe, director of NNSA's Office of Security Operations and Programmatic Planning.

The lab's Counter-UAV program will serve as a blueprint for other programs planned for other sites in the US.

Under separate authority, the FAA has established "no drone zones" for sites with Category I Special Nuclear Materials. NNSA has also developed signage to advise UAV operators about specific airspace boundaries where they may not fly their aircraft and that violating the airspace will have severe consequences, according to lanl.gov.

TSA AIRPORT SCREENING
SORRY, SIR... YOU'RE ALLOWED ONLY ONE CARRY-ON...
GATE 5
TSA
DAVE GRANLUND ©METROWEST DAILY NEWS www.davegranlund.com

International CBRNE INSTITUTE
CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

Wearable Drone Detection Device Exposed

Source: https://i-hls.com/archives/83039

May 18 – Infantry troops can now carry a portable drone detection device on their body. MyDefence is launching its third product in the WINGMAN series of wearable drone detection platforms – the WINGMAN 103. The system has been engineered to meet the requirements of elite forces. With its ultra-lightweight and rugged exterior, the technology is the only truly wearable drone detection platform that can withstand extreme operational conditions, according to suasnews.com.

The small and light form allows dismounted soldiers to wear the WINGMAN 103 on their uniforms or backpacks using the MOLLE clip-on system.

The system is designed to withstand extreme conditions with operating temperatures from -30°C to +65°C and is dust- and waterproof. Its detection range reaches 1-2 km, depending on environmental conditions, providing situational awareness and early-warning on threats.

It is designed to be used with standard external clip-on batteries with 14 hours of operation.

Together with the WINGMAN 103, the company also introduced the external Active Antenna (AA100), a special-designed quad-band active antenna that provides 360 degrees of coverage on the 433MHz, 1.2Ghz, 2.4GHz and 5.8Ghz frequency bands. The AA100 is plug-n-play and does not require an external power source, as the antenna is powered by the WINGMAN.

The antenna is dust- and waterproof and is designed specifically for drone detection with its built-in filters and low noise amplifiers.

Canada – Mississauga explosion: Suspects 'detonate IED' in restaurant

Source: http://www.bbc.co.uk/news/world-us-canada-44248453

Canada
Saskatchewan
Québec
Ontario
North Dakota
Michigan
Maine
Wyoming
Iowa
Mississauga
Utah
Kansas
North Carolina
Texas
worldatl

May 25 – A homemade bomb has exploded at a restaurant in Mississauga, Canada's sixth largest city, injuring 15 people.

Local police say two suspects entered the Bombay Bhel restaurant in the city late on Thursday and detonated the improvised explosive device.

Ambulance services said that three of the 15 people taken to hospital had "critical blast injuries".

Two male suspects fled the scene immediately after the explosion in the city.

Amazon in the dock over the Manchester bomber: Terrorist who killed 22 people bought chemicals for his suicide device online using fake names with NO security checks

Source: http://www.dailymail.co.uk/news/article-5777493/Amazon-dock-Manchester-bomber-bought-chemicals-online.html

May 27 – **Manchester bomber Salman Abedi was able to buy materials for his suicide device on Amazon**, the Mail can reveal.

Counter-terrorism chiefs believe the 22-year-old extremist used fake names to buy key components on the online marketplace.

He then assembled the bomb at home before detonating it at an Ariana Grande concert in May last year, killing 22 people including seven children.

Last night Amazon was in the dock after it emerged there were no proper security checks and officials were not alerted about the purchases.

Manchester bomber Salman Abedi was able to buy materials for his suicide device on Amazon, potentially by using fake names, the Mail can reveal

The online retailer faced further questions after the Daily Mail was still able to buy several components which could help make a device like the one used by Abedi a year after the attack.

The ingredients, which are used with other chemicals to make an improvised explosive device, were purchased within ten minutes and without any security questions. It is not clear whether Abedi bought his materials directly from Amazon or through one of many third-party sellers on the site.

But Government sources last night said they want the web giant to alert the security agencies when customers are ‘filling up their baskets’ with bomb-making materials.

Abedi’s Amazon history and that of people close to him have formed part of a police and security service investigation lasting months.

One line of inquiry is that he bought one item on the website as far back as January last year – five months before the attack – using the name of a family member.

The explosive device has been described as being a relatively sophisticated construct made with nails, nuts and bolts. It was revealed last year that he used hydrogen peroxide to make the explosive TATP – dubbed the Mother of Satan for its instability – and the same as that used in the 7/7 attacks on London.

The Parsons Green attacker, Ahmed Hassan, 18, also used Amazon to make the bomb he left on a crowded London Tube train in September.

His trial earlier this year heard how he detonated a device made from TATP, after packing it with metal items bought from Aldi and Asda and had hydrogen peroxide delivered to a friend’s address to avoid suspicion.

Emergency services respond to the attack at the Manchester Arena last year after Abedi had bought chemicals online and detonated the device at an Ariana Grande concert

Another ingredient was bought from Amazon. TATP is typically used by terror groups because it can be made using commonly available chemicals. Along with hydrogen peroxide, which is used in hair dyes, it includes other chemicals which the Mail will not name.

Three of the ingredients used to make up TATP were purchased by the Mail on Thursday within minutes without warnings or security checks that may have halted the transaction. Hamish de Bretton-Gordon, former head of Nato’s Rapid Reaction Chemical, Biological, Radiological and Nuclear Battalion, said Amazon needed to step up security checks. He said: ‘For Abedi to be able to buy this stuff on Amazon seems crazy to me. There needs to be more regulation to stop this happening.

‘Amazon should really have a role to play in making sure these items are not sold to people who could then fashion a bomb.’

Admiral Lord West, a former security minister, said: ‘Surely there are some things where if someone wants to buy them it should flag up a warning. Amazon needs to look at this and monitor what is being bought on its site.’ Former security minister John Hayes said: ‘It is time these companies such as Amazon step up to the mark and put the national interest ahead of any commercial interest.

‘They should be encouraged to do and if this doesn’t work they should be made to do so.’

Last December David Anderson QC, the former independent reviewer of terror legislation, published a report on the four terrorist attacks in Britain between March to June 2017. He said there needed to be increased cooperation between MI5 and the police and the private sector ‘to improve the detectability and even the preventability of purchases of potential explosives precursors by would-be terrorists, as undertaken before the Manchester and Parson’s Green attacks’.

Abedi’s Amazon history and that of people close to him have formed part of an police and security service investigation lasting months

Although he did not specifically mention Amazon, it is understood the Government is now working with the web giant to help stop attacks using items bought online. As well as using Amazon, Abedi downloaded material from other websites about the chemical compound used in the bomb.

And he also watched a bomb-making tutorial on YouTube before the attack. The bomb-making video ‘cookbook’ showed a masked extremist in a kitchen explaining how to build explosives with easy to obtain ingredients.

The products Abedi purchased were both legal and widely available. An Amazon spokesman: ‘We share suspicious transaction reports with the Home Office counter terrorism team, but we cannot comment on the specific security measures that we have in place.’

Earlier this month it emerged Amazon was selling terrorist recruitment material and bomb-making manuals on its site, including books by Osama Bin Laden.

Landmines made by Isis undo progress made by Princess Diana campaign

Source: https://www.theguardian.com/global-development/2018/may/31/landmines-made-by-isis-undo-progress-made-by-princess-diana-campaign

May 31 – The international campaign against landmines championed by the late Princess Diana has been driven into sharp reverse by the growing use of homemade devices in countries like Syria and Iraq.

Mine clearance groups are testing experimental mechanical systems to deal with the issue after Stan Brown, the US state department’s leading authority on landmine clearance, warned that a new generation of improvised explosives are more labour intensive, costly and complex to remove.

The marked rise in casualties caused by mines, which follows years of gains in global clearance efforts, has been blamed on semi-industrial production of the devices by Islamic State in Syria and Afghanistan.

The international campaign against landmines, which first came to prominence when Diana, Princess of Wales became a figurehead for the movement, has made significant progress in clearing the legacy of mine contamination in countries as diverse as Mozambique, Angola and Cambodia.

“We’d seen overall cases of mine casualties, which in the late 1990s were running at 9,000 a year – with 88% of those civilians and 40% children – drop to under 4,000,” said Brown. “But in 2015 and 2016 with Syria, Iraq and Yemen we have seen those figures rising again to 6,000 in 2016.”

The annual Landmine Monitor report, released in December by the Nobel prize-winning International Campaign to Ban Landmines, put the figure even higher, recording 8,605 casualties in 2016, among whom nearly 2,100 people were killed.

In December, Loren Persi, of Landmine Monitor, blamed a handful of conflicts for the reversal. “A few intense conflicts, where utter disregard for civilian safety persists, have resulted in very high numbers of mine casualties for the second year in a row,” said Persi.

An Isis explosive made to resemble a child’s toy is seen at Summel Exhibition Centre in Duhok. Photograph: Alessandro Rota for the Observer

The production and use of landmines have fallen since 1999, when the mine ban treaty came into force, outlawing the use, stockpiling, and transfer of mines. But Syria has not been a signatory country, while non-state groups have increasingly used the devices.

Brown maintained that global anti-mining efforts continue to make significant progress in terms of clearing minefields left as the legacy of the cold war, but said the recent increase comes primarily from homemade landmines manufactured by Isis.

Containing far larger amounts of explosives than conventional anti-personnel devices – sometimes in the order of 10-15kg in comparison with 200 grams – these homemade incendiaries have been laid in their thousands as barrier mines around locations like the Iraqi city of Fallujah.

Though often relatively simple devices, the mines – usually victim detonated by a homemade pressure plate – require far higher investment in clearance training and technology.

A young girl in the Syrian city of Deir ez-Zor who was injured by an Isis booby trap. Photograph: Louise Annaud/MSF

“One of the of problems of these kinds of improvised explosive devices [IEDs] is that it is difficult to define the scale of the problem.

“When you look at expertise required for traditional landmine decontamination, it is straightforward to take local civilians and educate them in clearing.

“These kind of IEDs require a much more sophisticated level of knowledge, someone in the explosive ordinance disposal field with many years of experience.”

One issue, explained Brown, is that during the period of Isis’s self-declared “caliphate” – covering large swathes of territory, from Mosul in Iraq to Raqqa in Syria – the group was able to produce and deploy huge numbers of its own landmines relatively unmolested.

The Halo Trust, the largest organisation working in humanitarian mine clearance, will begin working to clear the huge Isis-created barrier minefield around Fallujah later this summer.

Halo, which has in the past largely relied on locally trained mine clearance personnel, is among the groups experimenting with fresh approaches to clearing the new generation of crude mines. The methods under consideration include a modified, reinforced rock crusher, usually used in quarrying.

James Cowan, Halo’s chief executive, is anxious to make a distinction between a wider class of IEDs, some of which were built to booby trap buildings and target vehicles, and Isis’s homemade landmines.

“What we are seeing in the Middle East and Afghanistan is a proliferation of homemade mines with one factor: the ability of Islamic State, in particular, to produce them in their own factories.

“While the Taliban has been a cottage industry, the Islamic State really was semi-industrial.

“If you look at Fallujah as an example, there is a 15km long mine belt around it. We are talking about tens of thousands of mines.”

Where Cowan disagrees with Brown, however, is over the question of who should be involved in the clearing.

“I think donors and the international community are missing a trick by not channelling more support into local people. It is more cost effective, the deminers are more accepted by the local people, and they need less security support than former foreign military personnel who are paid large sums.”

Afghanistan seizes truck carrying 10 tonnes of explosives from Pakistan

Afghan border police have seized a truck carrying 9,800 kilograms of ammonium nitrate, an ingredient of improvised explosives, at Torkham crossing with Pakistan, officials said Sunday.

98 kg explosives meant for Bangladesh outfit seized in Bengal

Murshidabad police arrested two youths on Thursday night and seized bomb making chemicals weighing 98 kg that was allegedly being sent to a banned militant outfit in Bangladesh.

The Washington Post: Islamic State Suicide Bomber Strikes Meeting Of Afghan Clerics Who Had Just Condemned Terrorism

June 05 – “A suicide bomber killed 14 people Monday outside a large gathering in Kabul during the holy month of Ramadan where top religious figures had just condemned suicide attacks as violations of Islam. The radical Islamic State group claimed the attack on a website linked to it, denouncing the meeting of ‘tyrant clerics’ and their condemnation of suicide attacks. The attack occurred near the main entrance to a large tented compound in the Afghan capital, where about 2,000 Muslim clerics had assembled to deliberate on the war and attacks by the Taliban and the Islamic State, which are battling the Afghan government as well as U.S. and allied troops. The group, called the Afghan Ulema Council, had issued an unprecedented religious edict earlier in the day that said the insurgency in Afghanistan has no religious basis. It also declared that suicide attacks, often used by Taliban and Islamic State insurgents, are ‘haram,’ or forbidden by Islam.”

Counterinsurgency & Emergency Management

By Roger Parrino & Terry Hastings

Source: https://www.domesticpreparedness.com/resilience/counterinsurgency-emergency-management/

June 06 – Counterinsurgency and emergency management are two seemingly unrelated concepts, yet they have a lot in common in terms of the strategies necessary to succeed. In each case, empowerment is the ultimate key to success. For counterinsurgency, it is about empowering the host country and, for emergency management, it is about empowering local jurisdictions. Although empowerment is the central theme, the strategies to achieve empowerment include diplomacy, relationship building, and trust.

According to the U.S. military's counterinsurgency doctrine, counterinsurgency involves civilian and military efforts designed to defeat and contain insurgency and address its root causes. As it relates to the United States, counterinsurgency is generally an action that occurs overseas in response to some type of military conflict, such as the wars in Iraq and Afghanistan. Emergency management, on the other hand, is most often a domestic activity aimed at preparing for, responding to, and recovering from some type of emergency or disaster. Although counterinsurgency and emergency management are very different, they require many of the same strategies and ultimately rely on empowering others to succeed.

Strategy 1: Diplomacy

Diplomacy is the ability to deal with people and understand the various personalities, processes, and politics necessary to navigate a situation. It involves understanding rules and customs and requires an ability to employ different tactics based on different situations, with the goal of negotiating a successful outcome. Knowing when to employ different approaches is the key, as some situations call for direct confrontation while others warrant a more subtle and nuanced course of action.

When engaged in counterinsurgency, diplomacy is critical as military officials often find themselves in hostile territory trying to differentiate friend from foe. One misread of a situation could alienate important allies and jeopardize the mission. The same holds for emergency management, especially when other agencies or levels of government are deployed in support of a local jurisdiction. For example, even if the state or federal government has the resources to assume control of the disaster, it is generally not a good idea to marginalize the local officials and more effective to include them in the decision-making process.

This is especially true in a home-rule state, such as New York, where local officials have significant authority. Effective emergency managers are able to quickly size up the situation and coordinate with the various agencies and jurisdictions, working to establish a unified command structure and common objectives. In doing so, they need to exercise diplomacy and manage the personalities, processes, and politics to get the job done.

Strategy 2: Relationship Building

Diplomacy is important because it is the pathway to relationship building. Since military might can only go so far, long-term success with counterinsurgency requires the ability to develop effective relationships in the host country. Military officials need relationships with local government agencies, tribal groups, nonprofit organizations, religious leaders, and many others. Likewise, emergency managers must take whole community approach when it comes to preparing for, responding to, and recovering from disasters.

In each case, the government is a key player but only part of the solution. Many public, private, and nongovernment organizations have important roles to play. Building relationships with various stakeholders takes time. However, when dealing with emergencies or counterinsurgency, agencies cannot afford to operate unilaterally. Accordingly, a premium must be placed on building relationships and alliances, ideally during "peace time" or before the emergency.

Roger Parrino with members of the Afghan Army in Nawzad, Afghanistan (Source: Roger Parrino, 2009).

Strategy 3: Trust

Building effective relationships leads to trust, which may be the most important factor as it relates to the concept of empowerment. All disasters start and end locally, meaning that local agencies are generally the first to respond and the local community is left to manage the recovery long after the Federal Emergency Management Agency (FEMA) and other agencies are gone. The same holds true for counterinsurgency, in that the host country eventually is responsible for managing its affairs, and the occupying force seeks to play a diminished role over time.

In each case, the goal is not to take over the situation, rather it is to provide support and guidance to help others help themselves. The host country must trust the military and vice versa, and the same is true for emergency managers deployed to assist a local jurisdiction. Once trust is established, both sides can begin working together toward a common goal, whether responding to a disaster or helping a country restore order after an armed conflict.

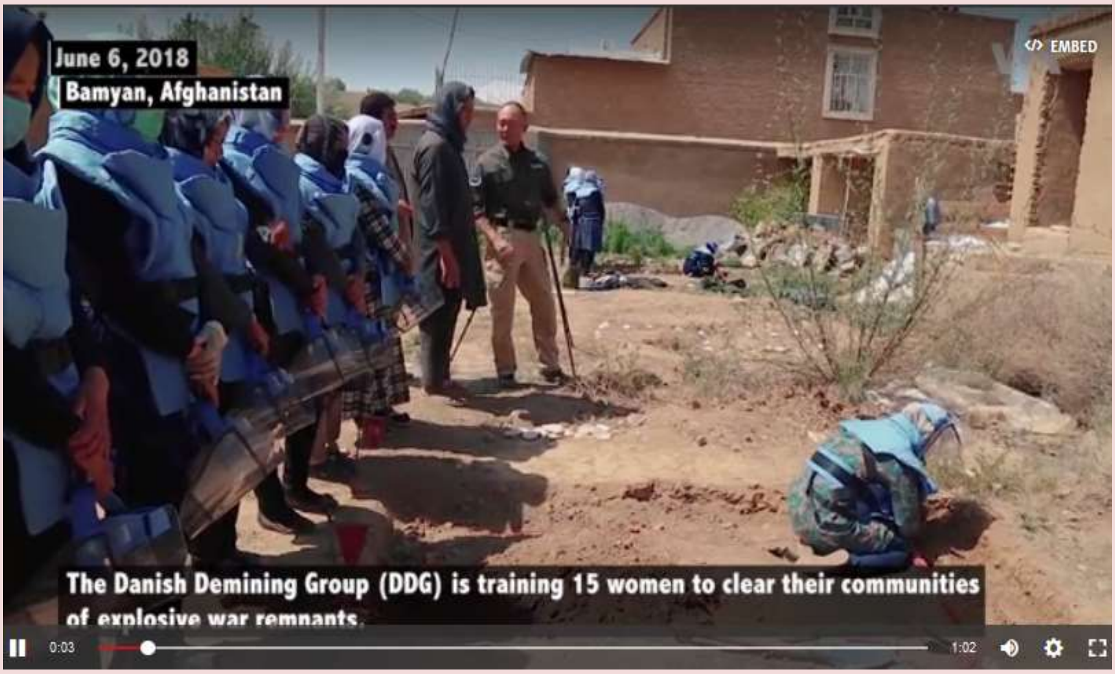
Although very different in many ways, emergency management and counter-insurgency are similar when it comes to the strategies and skills necessary to succeed. Empowerment is the key for each effort. Having an open mind and willingness to learn from others is a hallmark of maturity. Therefore, as the discipline of emergency management continues to mature, it is important to continuously consider new ideas and approaches.

***Roger Parrino** is the commissioner of the New York State Division of Homeland Security and Emergency Services (DHSES). Prior to joining DHSES, he most recently served as senior counselor to U.S. Department of Homeland Security Secretary Jeh Johnson. He has also worked as a civilian adviser to the U.S. Marine Corps, during which time he served four combat deployments in Iraq and Afghanistan.*

***Terry Hastings** is the senior policy advisor for DHSES and an adjunct professor for the College of Emergency Preparedness, Homeland Security and Cybersecurity at the State University of New York at Albany.*

First Group of Afghan Female Deminers Being Trained

Video: https://www.voanews.com/a/first-group-afghan-female-deminers-being-trained/4428109.html


June 6, 2018
Bamyan, Afghanistan
EMBED
The Danish Demining Group (DDG) is training 15 women to clear their communities of explosive war remnants.
0:03
1:02

June 06 – A group of Afghan female deminers is being trained in Bamyan province in central Afghanistan. Many civilian casualties in Afghanistan are attributed to explosive remnants of war and other improvised explosive devices. The Danish Demining Group pledges to train more women to help them clear their communities of remnants of war if the initiative is approved in the male-dominated country. Zafar Bamyani reports.

Trained bees make first warzone discovery of lost explosives confirms Scots scientist

Source: http://www.deadlinenews.co.uk/2018/06/15/trained-bees-make-first-warzone-discovery-of-lost-explosives-confirms-scots-scientist/

June 15 – Trained bees have been successfully used for the first time to find mines in a former Yugoslavian warzone, a Scottish scientist has revealed.

The honey bees led mine clearance teams to unexploded ordnance in Croatia after they were trained to hone in on the smell of explosives.

Dr Ross Gillanders of St Andrews University helped design equipment which detects if bees are returning to the hive with tiny traces of explosives.

Once confirmed, footage from drones was used to pinpoint the spot at which the bees picked up the traces.

The bees could prove more effective than sniffer dogs in some circumstances because they can work for longer and are cheaper to use. A dog's performance can also be adversely affected by its treatment.

The promising early results of the ongoing trials in Croatia hold out hope that more of the millions of abandoned mines around the world could be cleared up more quickly, sparing thousands of people from being killed or injured.

The use of bees to detect explosives is being researched by academics in Scotland and Croatia.

Real-world tests started in Croatia in November last year, funded by NATO Science for Peace and Security, and using bees from local hives.

Dr Gillanders, a research fellow in the department of physics at St Andrews, today (Thu) confirmed the bees had found mines and other explosives lost during Croatia's four-year struggle for independence from Yugoslavia which started in 1991.

The project borrows standard Apismellisera Carnica honeybees which are trained over two days by placing sugar syrup on top of TNT.

"Basically we teach them by a version of reward like you do with dogs," said Dr Gillander.

"The bees fly out of their hive to go about their normal day to day job of finding pollen but instead of finding pollen they find explosives. It's the sugar syrup, which draws them out.

"The training takes two days and is much faster and more efficient than training a dog. However, after three days the bees realise that they aren't getting reward from the TNT and as a result are disinterested in it and look for other things.

"After three days we have to re-train the honeybees to detect the explosives."

Honeybees have a bigger advantage over sniffer dogs when it comes to finding explosives as dogs only work for 15 minutes at a time. Dogs, which are more expensive to train,see it as a "game" and quickly get bored.

Bees will work tirelessly and are not affected by the chemical compounds found in explosives, unlike dogs. They can get to areas that that are more difficult to get to than dogs.

Dr Gillanders, a physicist, designed the equipment that tests the bees for explosives when they return to the hive.

The bees go through a special canvas-type material which is then exposed to light.

"A drop in light emission (like a light dimmer switch) confirms the presence of explosives," said Dr Gillanders.

Once explosives are confirmed, the team go back to records from a drone which accompanies the bees on their expeditions, hovering a couple of metres above.

The behaviour of the bees recorded by the drone indicates the precise moment they discovered explosive traces, pinpointing the buried mines.

The types of mines the bees are being trained to detect are Yugoslavian PMA-2 and PMA-3 mines, and some Russian/Soviet mines.

The bees do have drawbacks, however. Rain and darkness will normally deter the bees from going out on their life-saving missions.

Precise details of the tests are being kept under wraps for now but Dr Gillanders said the use of bees looked "promising".

The academic revealed there had so far been just one casualty from the testing – PhD student James Glackin, who was strung three times while driving 6,000 bees to the test site.

There are an estimated 110 million land mines lost across the world which kill or injure between 15,000 to 20,000 people annually.

Remarkable video shot (watch at sources URL) from a drone shows how the movement of the mine-hunting bees can be detected by infra red.

The clip was captured by a high-definition camera attached to a drone, which follows the bees around in the test site.

The screen on the left shows the bees repeatedly flying around an area where they have detected explosives. The fact the bees are staying in the same place, rather than moving on, indictates a likely positive result.

The right hand side of the screen shows yellow circles darting about. These are bees which have been picked up by infrared to help track their movement. The right hand side of the screen is blacked out to help observe the tracking.

Dr Gillanders explained this was a first as bees "are very small and very fast, which makes them difficult to track".

EUROPOL Te-Sat 2017: Explosives

Source: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017

Even though terrorists use a wide range of readily available weapons, explosive devices continue to be used in terrorist attacks, due to their high impact and symbolic power.

In 2016, the transfer of terrorist tactics, techniques and procedures (TTPs) from the current conflict zones and illicit spread of bomb-making knowledge and instructions has been observed. The availability of explosive precursors has facilitated the use of Home-Made Explosives (HMEs). Of particular concern are improvised explosive device (IED) attacks on soft targets and the use of suicide person-borne IEDs (PBIEDs).

IMPROVISED EXPLOSIVE DEVICES (IEDS)

Jihadist terrorist IED attacks generally aimed at soft targets, with the main intention of causing a large number of civilian casualties. In recent years, targets included air and rail transport facilities, commercial premises and major sports events.

Two distinct trends have been observed with regards to jihadist terrorists' use of IEDs in the EU. Firstly, IEDs have been reported to show similarities in design and construction with IEDs used in conflict zones. Some elements of these IEDs appeared to have been modified based on available resources and circumstances in the EU. For example, HMEs and improvised components were used in place of military components that are difficult to procure. Such devices have been more prevalent in attacks by terrorist groups and lone-actors directed by IS. These incidents commonly required additional logistical support and specific knowledge in the manufacturing of larger amounts of HMEs. Nonetheless, these IEDs were not particularly sophisticated but relatively reliable and simple to use. Bomb-making knowledge, in some cases, was transferred to the attackers through direct contact and experience (facilitated by foreign terrorist fighters and returnees). In other cases, knowledge and guided instructions have been transferred via 'remote assistance' using various social media and online communication channels.

Secondly, more rudimentary IEDs have been used by jihadist terrorists recently. These mostly consisted of readily available explosive components, such as gas cylinders, pyrotechnic articles and ammonium nitrate-based products. Such IEDs can be constructed without any specific expertise, preparation, extensive planning or logistical support. They have been primarily used by small terrorist groups or self-radicalised lone-actor terrorists inspired by IS. It is also notable that IS has started to promote the use of readily available flammable products to construct basic improvised incendiary devices (IIDs) and commit arson attacks – a new simple terrorist tactic recommended for lone-actors.

Regarding the potential use of alternative and more sophisticated types of IEDs, the current trend in using weaponised unmanned aerial vehicles (UAVs) in the Syria/Iraq conflict zone might also inspire other jihadist supporters and expand the use of this kind of tactic outside this area of operation.

Additionally, as seen in recent attacks in Egypt and Somalia, threats posed to civil aviation by IED attacks are still present. Main threats emanate from the use of concealed and hardly detectable IEDs and facilitation by affiliates working as airport employees to bypass security checks. Groups and individuals belonging to the extreme right-wing scene maintained their affinity to weapons and explosives. This was illustrated by the significant increase in the number of incidents involving arson and explosives, as well as seized explosive devices. In addition to common types of IIDs/IEDs such as Molotov cocktails and improvised pipe bombs, these groups tend to use military-grade explosive devices.

Left-wing and anarchist groups have predominantly carried out arson attacks using flammable liquids and IIDs, such as Molotov cocktails and gas cylinders. Nevertheless, an increase has been noted in the number of terrorist attacks in which perpetrators constructed and delivered postal IEDs/IIDs filled with incendiary or low-explosive charges, such as gunpowder. In general, all devices have been constructed from improvised material readily available on the open market.

The attack methodologies and capabilities used by Dissident Republican (DR) groups in Northern Ireland (UK) varied across groups. Many attacks involved firearms or small IEDs such as pipe bombs but they have also employed larger and/or potentially more destructive devices such as vehicle-borne IEDs (VBIEDs) and explosively formed projectiles (EFPs).

There have been four DR IED attacks in 2016 including a fatal IED attack on a prison officer. All groups retain access to a range of firearms and explosives and there is an ever-present threat of under-vehicle IED attacks.

HOME-MADE EXPLOSIVES

HMEs have been the most common type of explosive used in recent terrorist IED attacks. The explosive used in most of the attacks was triacetone triperoxide (TATP), a home-made explosive that remains the explosive of choice for terrorists. The internet continues to be a crucial resource for loneactor terrorists to gain bomb-making skills. Internet websites, forums, social networks and the Darknet facilitate access to bomb-making knowledge and information.

MILITARY EXPLOSIVES

The availability of explosives in current and former conflict areas such as the Western Balkans and Ukraine, and the illicit trafficking of explosives into the EU, is believed to present a significant threat. Terrorists are known to have acquired hand grenades, rocket launchers and high-grade plastic explosives and detonators from organised crime groups (OCGs).

In addition to trafficking explosives, other methods of obtaining military explosive ordnance include thefts from military explosives storage facilities and the illegal collection of explosive remnants of war (ERW) and unexploded ordnance (UXO) from former battle zones.

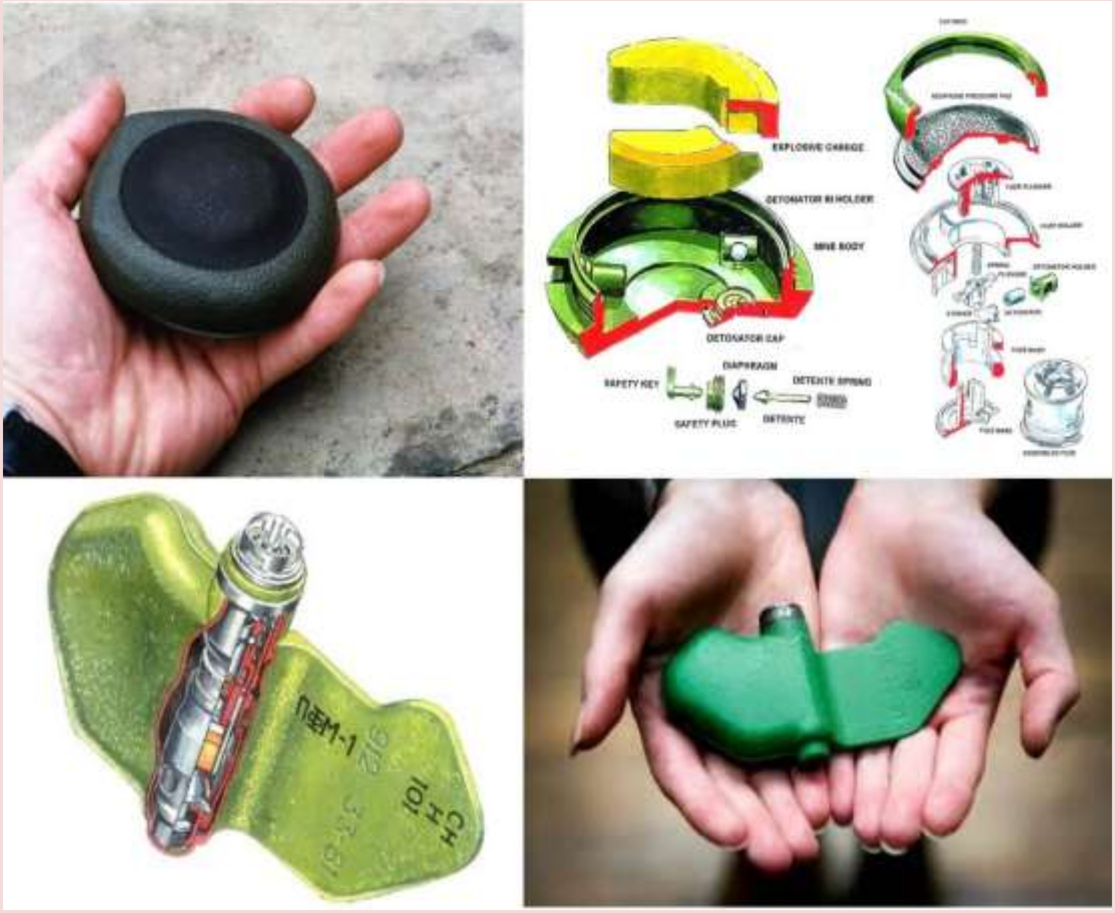
COMMERCIAL EXPLOSIVES

Commercial pyrotechnic articles and gunpowder continue to be misused for terrorist purposes as a source of explosive compounds for constructing IEDs. These pyrotechnics are widely available, and the use of pyrotechnic mixtures in IEDs is promoted in jihadist terrorist publications. This threat might increase in the future. Misuse of pyrotechnics has been observed in most EU countries. The pyrotechnic articles have been used in various forms: in the original state; modified; Or by extracting the pyrotechnic mixture and utilising it in IEDs. Pyrotechnics have largely been used in small-scale bomb attacks. The most frequently used types have been the categories F3 and F2, which are sold to the general public. However, it appears that the misuse of professional category F4 flash bangers has increased in the recent period.

Drones could be used to detect dangerous "butterfly" landmines

Source: http://www.homelandsecuritynewswire.com/dr20180621-drones-could-be-used-to-detect-dangerous-butterfly-landmines

June 21 – Drones could be used to detect dangerous "butterfly" landmines in remote regions of post-conflict countries, according to new research from Binghamton University, State University at New York. It is estimated that there are at least 100 million military munitions and explosives of concern devices in the world, of various size, shape and composition. Millions of these are surface plastic landmines with low-pressure triggers, such as the mass-produced **Soviet PFM-1 "butterfly" landmine**. Nicknamed for their small size and butterfly-like shape, these mines are extremely difficult to locate and clear due to their small size, low trigger mass and, most significantly, a design that mostly excluded metal components, making these devices virtually invisible to metal detectors. Critically, the design of the mine combined with a low triggering weight have earned it notoriety as "the toy mine," due to a high casualty rate among small children who find these devices while playing and who are the primary victims of the PFM-1 in post-conflict nations, like Afghanistan.



Binghamton says that researchers at Binghamton University have developed a method that allows highly accurate detection of "butterfly" landmines from low-cost commercial drones. Assistant Professor of Energy Geophysics Alex Nikulin and Director of the Geophysics and Remote Sensing Laboratory Timothy de Smet used mounted infrared cameras to remotely map the dynamic thermal conditions of the surface and recorded unique thermal signatures associated with the plastic casings of the mines. During an early-morning experiment, they found that the mines heated up at a much-greater rate than surrounding rocks, and they were able to identify the mines by their shape and apparent thermal signature. Results indicate that this methodology holds considerable potential to rapidly identify the presence of surface plastic MECs during early-morning hours, when these devices become thermal anomalies relative to surrounding geology.

"We believe our method holds great potential for eventual wide-spread use in post-conflict countries, as it increases detection accuracy and allows for rapid wide-area assessment without the need for an operator to come into contact, or even proximity of the minefield," said Nikulin. "Critically, once further developed, this methodology can greatly reduce both costs and labor required for mine clearing operations across post-conflict regions."

The use of cost- and time-efficient remote sensing techniques to detect plastic MECs such as the butterfly mine from unmanned aerial vehicles has enormous potential that warrants further study, wrote the researchers.

"We are actively pursuing this project further and are in the process of field testing and calibrating our methodology," said De Smet. "Ultimately, we hope to develop a fully autonomous multi-drone system that would require minimum input from the operators."

— Read more in Timothy S. de Smet and Alex Nikulin, "Catching "butterflies" in the morning: A new methodology for rapid detection of aerially deployed plastic land mines from UAVs," The Leading Edge 37, no. 5 (May 2018).

FOR CRYING OUT LOUD!! I'M NOT CARRYING A BOMB!! IT'S JUST MY BIOLOGICAL CLOCK TICKING!!
EXIT
TICK TICK TICK
POLICE
CARTOONSTOCK .com
Search ID: tzun292

ICI
International
CBRNE
INSTITUTE

CBRNE-Terrorism Newsletter

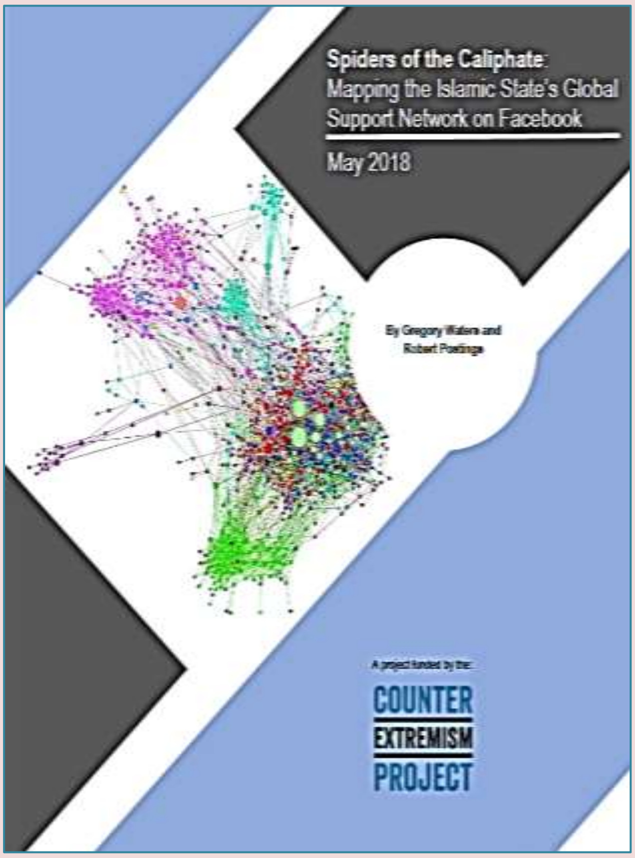
CYBER NEWS

Spiders of the Caliphate

Mapping the Islamic State's Global Support Network on Facebook

By Gregory Waters and Robert Postings

Source:https://www.counterextremism.com/sites/default/files/Spiders%20of%20the%20Caliphate%20%28May%202018%29.pdf?utm_source=press%20release&utm_medium=email&utm_campaign=SpidersCaliphate&utm_term=Facebook



May 2018 - This report analyzes the strength of the Islamic State's (IS) network on Facebook using online network measurement tools and uncovers the myriad of ways in which IS operates on Facebook. To do so, we mapped the accounts and connections between 1,000 IS-supporting Facebook profiles with links to 96 countries on every continent except Antarctica using the open-source network analysis and visualization software, Gephi. It should be noted, however, that hundreds of additional pro-IS profiles were excluded from the dataset. This is because while we were able to identify the IS supporting Facebook accounts, there was no information on those users' locations. Therefore, this data represents only a portion of IS's support network on the platform.

Our analysis of online IS communities globally, regionally, and nationally suggests that IS's online networks, in particular on Facebook, are growing and can be utilized to plan and direct terror attacks as well as mobilize foreign fighters for multiple areas of insurgency. Secondly, IS's presence on Facebook is pervasive and professionalized, contrary to the tech company's rhetoric and efforts to convince the public, policymakers, and corporate advertisers from believing otherwise. Our findings illustrate that IS has developed a structured and deliberate strategy of using Facebook to radicalize, recruit, support, and terrorize individuals around the world. According to our observations, it appears that IS utilizes a limited number of central players who work to magnify the group's presence on the platform, and also works to strengthen its networks so that no one individual IS Facebook account (node) serves as an irreplaceable connection (edge) to other pro-IS accounts located elsewhere.

Gregory Waters *received his BA with Honors in Political Economy and Foreign Policy in the Middle East from the University of California, Berkeley, in 2016. Since then he has researched and written about the Syrian Civil War and extremist groups, primarily utilizing Syrian community Facebook pages for his projects. He has worked as a research consultant at the Counter Extremism Project since June 2017 and currently writes about Syria for the International Review and has previously been published by Bellingcat and openDemocracy.*

Robert Postings *received his BA with Honors in History from Oxford Brookes University in 2016. He currently writes about the Islamic State for the International Review. He has written articles using analysis of IS supporters on social media to gauge their reaction to major events and studying the widespread hacking of Facebook accounts by Islamic State supporters.*

Cyber and international law in the 21st century

Source: http://www.homelandsecuritynewswire.com/dr20180525-cyber-and-international-law-in-the-21st-century

May 25 – The U.K. Attorney General Jeremy Wright, QC MP, on 23 May 2018 set out the U.K.'s position on applying international law to cyberspace. **This is the first time a government minister has set out the U.K. view on record.**

Here is the transcript of his presentation:

I am particularly pleased to be speaking here, at Chatham House Royal Institute for International affairs, which has a longstanding record of engaging governments, the private sector and civil society in debate about the most significant and pressing developments in international affairs.

Today I want to talk about the importance of international law in cyber space and to emphasize that cyber space is an integral part of the rules based international order. That being so, it is the U.K.'s view that there are boundaries of acceptable state behavior in cyberspace, just as there are everywhere else.

One of the biggest challenges for international law is ensuring it keeps pace as the world changes. International law must remain relevant to the challenges of modern conflicts if it is to be respected, and as a result, play its critical role in ensuring certainty, peace and stability in the international order. If it is seen as irrelevant it will be ignored and that makes the world less safe.

Whilst the need to adapt to changing times is true of all law, international law is unusual – other types of law are found in statutes and in court judgments – but there are few of either in international law, instead there are treaties, and customary international law formed from the general and consistent practice of states acting out of a sense of obligation.

The necessity of international law keeping pace with the modern world underpinned my speech at the International Institute for Strategic Studies on the modern law of self- defense in January 2017. In that speech, I set out how the law of self-defense must adapt to meet the particular demands of a world in which an armed attack is as likely to be inspired by something on the internet as it is to be instructed by someone in direct contact with the perpetrator, and where we can't see such an attack coming in the way we once could.

I made that speech last year because I believe that a nation like ours should be open and clear in setting out the rules it feels bound by. In doing so, we demonstrate not just our commitment to the rules based international order, but also our leadership in its development.

I am here today in pursuit of the same goal.

There are few areas in which the world has moved faster than in the development of cyber technology. Cyber has become a noun and a prefix meaning anything including or relating to computers, especially the internet.

And cyber is everywhere – in the light transmitted along millions on miles of optical fiber cables crossing the deep ocean floor, from our homes to the battlefield and on the display screens of stock markets across the world. It is increasingly the means by which we communicate in every sphere of our lives, locally and globally.

Right now, the impact of the internet is near universal. Even those not online themselves are using public or private sector services whose operations depend on interconnectivity via cyberspace. We have moved from a country and a world operating in analogue, to one where almost every aspect of daily life is affected by cyber activity.

In addition to the enormous opportunities for further freedom, understanding, advancement, global connectivity and prosperity, the cyber domain is now one of the primary means through which states conduct their international relations, both in peacetime and in times of conflict. It features in the risk assessments of Ministers, diplomats, intelligence officials and military leaders. The growth of cyber technology has also meant that the threats we face as nations have never been as widespread or as complex. And this complexity is easily exploited.

Yet, despite this ubiquity, until a few years ago, the international community had yet to agree whether there were any applicable rules in cyber space at all. The academic community has been quick to fill the gap and academics have made valuable contributions to the debate, but states have remained relatively quiet.

This is in part due to the fact that cyber technologies develop at an unprecedented pace. It is also no doubt due to the fact that these technologies are uniquely accessible to a wide range of state and non- state actors, crossing a number of legal and practical boundaries and frameworks and resulting in unparalleled complexity. The development and use of these technologies can also stray into highly sensitive areas that governments have been traditionally unwilling to publicly comment on or to debate.

But the truth is, as authors and subjects of international law, states have a responsibility here. A responsibility to be clear about how our international law obligations bind us. A responsibility we fulfil through our treaty obligations, our actions and our practice, as well as through our public statements. And a responsibility I believe extends to cyberspace.

The very pervasiveness of cyber makes silence from states on the boundaries of acceptable behaviour in cyberspace unsustainable. If we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.

Those around the world whose behaviors international law seeks to constrain of course resent it, and they will seize on any excuse to say international law is outdated and irrelevant and can therefore be ignored. We must not give them that opportunity by conceding that applying international law principles to cyberspace is just too difficult.

And we need not, and should not, make that concession.

Cyber space is not – and must never be – a lawless world. It is the U.K.'s view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain. The U.K. has always been clear that we consider cyber space to be an integral part of the rules based international order that we are proud to promote. The question is not whether or not international law applies, but rather how it applies and whether our current understanding is sufficient.

What this means is that hostile actors cannot take action by cyber means without consequence, both in peacetime and in times of conflict. States that are targeted by hostile cyber operations have the right to respond to those operations in accordance with the options lawfully available to them and that in this as in all things, all states are equal before the law.

These are principles best developed with others.

U.K. has made great efforts across the last decade to develop shared understanding and agreement on how international law applies in cyberspace. We have engaged across U.K. government departments and agencies and worked closely with industry; we have consulted with academics, international organizations and the wider international law community. And we have engaged both bilaterally, regionally and multilaterally with our international counterparts in other states and those in international organizations - some of whom I am very pleased to see here today.

To build international consensus on the role of international law in this area, the U.K., together with other states, has engaged in negotiations under a mandate from the UN Secretary General to progress multilateral agreement on the parameters of responsible state behavior in cyberspace.

In 2013, the UN Group of Governmental Experts on the use of cyber technologies, affirmed the application of existing international law to states' cyber activities. On 26 June 2015, the UN Expert Group, including not just the U.K. and the US but also Russia and China recognized that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defense in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections of *international humanitarian law: necessity, proportionality, humanity and distinction, apply in cyberspace.*

Whilst these may seem to be cautious advances, it is no small achievement given negotiations involved states with vastly different resources, cyber capabilities, and approaches to international law. And in the current political climate, the fact that consensus was achieved at all among the nations I have mentioned is not to be underestimated.

So wherever possible we can and should work with others, but every state should be clear about the legal principles and thresholds it believes apply in cyberspace and I want to be as clear as I can be about the U.K.'s position.

Perhaps the most useful starting point is the UN Charter and three specific rules are particularly relevant.

First, there is the rule prohibiting interventions in the domestic affairs of states both under Article 2(7) of the Charter and in customary international law. This prohibition means that any activity in cyber space which reaches the level of such an intervention is unlawful. Any activity of this nature by a state could only become permissible in response to some prior illegality by another state.

The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defense or as a Chapter VII action authorized by the Security Council. In addition, the U.K. remains of the view that it is permitted under international law, in exceptional circumstances, to use force on the grounds of humanitarian intervention to avert an overwhelming humanitarian catastrophe.

Thirdly, the U.K. considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self- defense, as recognized in Article 51 of the UN Charter.

If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us.

If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.

And in addition to the provisions of the UN Charter, the application of international humanitarian law to cyber operations in armed conflicts provides both protection and clarity. When states are engaged in an armed conflict, this means that cyber operations can be used to hinder the ability of hostile groups such as Daesh to coordinate attacks, and in order to protect coalition forces on the battlefield. But like other responsible states, this also means that even on the new battlefields of cyber space, the U.K. considers that there is an existing body of principles and rules that seek to minimize the humanitarian consequences of conflict.

Of course there are also particular challenges posed by the international law that regulates cyber activities in peacetime. I have already touched on the prohibition against interventions in the internal affairs of states.

In certain circumstances, cyber operations which do not meet the threshold of the use of force but are undertaken by one state against the territory of another state without that state's consent will be considered a breach of international law.

The international law prohibition on intervention in the internal affairs of other states is of particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of this principle is to ensure *that all states remain free from external, coercive intervention in the matters of government which are at the heart of a state's sovereignty, such as the freedom to choose its own political, social, economic and cultural system.*

The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.

Furthermore, a breach of this principle of non-intervention provides victim states with the ability to take action in response that would otherwise be considered unlawful, but which is permissible if it is aimed at returning relations between the hostile state and the victim state to one of lawfulness, and bringing an end to the prior unlawful act. Such action is permissible under the international law doctrine of countermeasures. Put simply, if a hostile state breaches international law as a result of its coercive actions against the target state's sovereign freedoms, then the victim state can take action to compel that hostile state to stop.

Consistent with the de-escalatory nature of international law, there are clear restrictions on the actions that a victim state can take under the doctrine of countermeasures. A countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state. This means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response. In cyberspace of course, attribution presents particular challenges, to which I will come in a few moments. Countermeasures cannot involve the use of force, and they must be both necessary and proportionate to the purpose of inducing the hostile state to comply with its obligations under international law.

These restrictions under the doctrine of countermeasures are generally accepted across the international law community. The one area where the U.K. departs from the excellent work of the International Law Commission on this issue is where the U.K. is responding to covert cyber intrusion with countermeasures.

In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.

In addition, it is also worth stating that, as a matter of law, there is no requirement in the doctrine of countermeasures for a response to be symmetrical to the underlying unlawful act. What matters is necessity and proportionality, which means that the U.K. could respond to a cyber intrusion through non-cyber means, and vice versa.

Through the principle of non-intervention, it is clear that the international community has set a boundary at which interference in another state's sovereign freedoms is considered internationally wrongful and as such, in breach of international law, giving rise to the right to take action which may otherwise be unlawful in response. As I have already mentioned, the precise parameters of this principle remain the subject of ongoing debate in the international law community, but a further contested area amongst those engaged in the application of international law to cyber space is the regulation of activities that fall below the threshold of a prohibited intervention, but nonetheless may be perceived as affecting the territorial sovereignty of another state without that state's prior consent.

Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent.

Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that *of a prohibited intervention. The U.K. Government's position is therefore that there is no such rule as a matter of current international law.*

Online as well as everywhere else, the principle of sovereignty should not be used by states to undermine fundamental rights and freedoms and the right balance must be struck between national security and the protection of privacy and human rights.

I have talked about the behavior to be expected of states in cyberspace and their entitlement to defend themselves, but having a legal framework within which to act is not the same as having the practical capacity to act, and the U.K. needs that too.

One of the biggest challenges for a state that finds itself a victim of a hostile cyber operation is determination of who was behind it. Without clearly identifying who is responsible for hostile cyber activity, it is impossible to take responsible action in response.

There are obviously practical difficulties involved in making any attributions of responsibilities when the action concerned is capable of crossing traditional territorial boundaries and sophisticated techniques are used to hide the identity and source of the operation. Those difficulties are compounded by the ready accessibility of cyber technologies and the resultant blurring of lines between the actions of governments and those of individuals.

The international law rules on the attribution of conduct to a state are clear, set out in the International Law Commissions Articles on State Responsibility, and require a state to bear responsibility in international law for its internationally wrongful acts, and also for the acts of individuals acting under its instruction, direction or control.

These principles must be adapted and applied to a densely technical world of electronic signatures, hard to trace networks and the dark web. They must be applied to situations in which the actions of states are masked, often deliberately, by the involvement of non-state actors. And international law is clear - states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.

But the challenge, as ever, is not simply about the law. As with other forms of hostile activity, there are technical, political and diplomatic considerations in publicly attributing hostile cyber activity to a state, in addition to whether the legal test is met.

There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances.

However, the U.K. can and does attribute malicious cyber activity where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. Sometimes we do this publicly, and sometimes we do so only to the country concerned. We consider each case on its merits.

For example, the WannaCry ransomware attack affected 150 countries, including 48 National Health Service Trusts in the United Kingdom. It was one of the most significant attacks to hit the U.K. in terms of scale and disruption. In December 2017, together with partners from the US, Australia, Canada, New Zealand, Denmark and Japan, we attributed the attack to North Korean actors. Additionally, our attribution, together with eleven other countries, of the destructive NotPetya cyber-attack against Ukraine to the Russian government, specifically the Russian Military in February this year illustrated that we can do this successfully. If more states become involved in the work of attribution then we can be more certain of the assessment. We will continue to work closely with allies to deter, mitigate and attribute malicious cyber activity. It is important that our adversaries know their actions will be held up for scrutiny as an additional incentive to become more responsible members of the international community.

Addressing our capacity more broadly, in November 2016, the Government launched its new National Cyber Security Strategy, which included the establishment of the National Cyber Security Centre with a mandate to pursue the action required to better protect the U.K.'s interests in cyberspace.

As part of its strategy, the Government is investing 1.9 billion in cyber security. And the U.K.'s active cyber defense program has now been underway for over a year. In this time it has prevented on average 4.5 million malicious emails per *month and has carried out more than 1 million security scans and 7 million security tests on public sector websites.*

In tandem, our National Offensive Cyber Program is building a dedicated capability allowing the U.K. to act in cyberspace. We believe each state has the right to develop a sovereign offensive cyber capability. It does not destabilize nor weaponize cyber space to do so, as there is an obligation on each state to ensure use and development are carried out in accordance with international law. We have therefore been and will continue to be transparent about the existence of this program.

As I have outlined, the U.K. is a leading voice on cyber at an international level: in the United Nations and in regional organizations including the Organization for Security Co-operation in Europe.

In 2011 the U.K. Foreign Office initiated the London Process, a global conference on cyber space which has now become an established event. Subsequent conferences have taken place in Hungary, South Korea, the Netherlands and India and welcomed attendees from over 120 countries and from governments, academia and the private sector.

Cyber security is something which this Government has consistently taken very seriously. It remains a very significant threat to the U.K.'s economic and national security – we all need to play our part and take responsibility as individuals, organizations and businesses. Much of the work of the NCSC and other parts of Government in cyber defense is in this area – helping all of us to help ourselves and to keep the U.K. as the safest place to be online.

But for all the work I have described, both domestic and international, it remains the case that defining the appropriate principles of international law to apply to cyberspace is difficult. Around the world there are many who would not bother trying – some because they have scant regard for international law more generally and some because they see little advantage in being explicit about rules of acceptable behavior.

We do. The clearer we are about the boundaries of acceptable behavior, the lower the risk of miscalculation and the clearer the consequences can be for transgressing them. I have tried to offer some of that clarity this morning, to say in terms that, for example, the targeting of essential medical facilities, the downing of civilian aircraft, the sabotage of nuclear power stations, are no less unlawful and no less deserving of a robust and legitimate response when they are undertaken by cyber means than when they are done by any other means.

The United Kingdom has always taken its international law responsibilities seriously, despite the restrictions on our freedom of action those responsibilities entail. We do so because we believe that a rules-based international order makes the world a safer place and that no nation can make a strong case for such an order if it is unprepared to accept the rules itself. But it must also follow that a rules-based international order can only prevail when the rules can be clearly understood and that where they are unclear we seek to bring clarity. It must be for those of us who believe in the benefits of international law to ensure it remains effective, that it continues to constrain and deter, online as well as offline, the worst failings of human nature.

Cyberspace is getting larger, not smaller. Its influence on international relations is growing not shrinking. So it is ever more important, and part of the U.K.'s role in global leadership, to do what we can to ensure the law applies in cyberspace too.

The era of fake video begins

By Franklin Foer

Source: http://www.homelandsecuritynewswire.com/dr20180531-the-era-of-fake-video-begins

May 30 – The *Telegraph* reports that official monitors are warning that "deepfake" videos produced by Russian-linked trolls are the latest weapon in the ongoing fake news war.

Experts at the U.K.-led East Stratcom Task Force, an EU counter-disinformation unit that monitors, analyzes, and debunks disinformation operations, say that Kremlin-backed trolls are already experimenting with new video manipulation techniques which use artificial intelligence to create convincing doctored videos.

Franklin Foer writes in *The Atlantic* that

> In a dank corner of the internet, it is possible to find actresses from *Game of Thrones* or *Harry Potter* engaged in all manner of sex acts. Or at least to the world the carnal figures look like those actresses, and the faces in the videos are indeed their own. Everything south of the neck, however, belongs to different women. An artificial intelligence has almost seamlessly stitched the familiar visages into pornographic scenes, one face swapped for another. The genre is one of the cruelest, most invasive forms of identity theft invented in the internet era. At the core of the cruelty is the acuity of the technology: A casual observer can't easily detect the hoax. This development, which has been the subject of much hand-wringing in the tech press, is the work of a programmer who goes by the nom de hack "deepfakes." And it is merely a beta version of a much more ambitious project. One of deepfakes's compatriots told *Vice*'s Motherboard site in January that he intends to democratize this work. He wants to refine the process, further automating it, which would allow anyone to transpose the disembodied head of a crush or an ex or a co-worker into an extant pornographic clip with just a few simple steps. No technical knowledge would be required. And because academic and commercial labs are developing even more-sophisticated tools for non-pornographic purposes—algorithms that map facial expressions and mimic voices with precision—the sordid fakes will soon acquire even greater verisimilitude.

Foer continues:

> The internet has always contained the seeds of postmodern hell. Mass manipulation, from clickbait to Russian bots to the addictive trickery that governs Facebook's News Feed, is the currency of the medium. It has always been a place where identity is terrifyingly slippery, where anonymity breeds coarseness and confusion, where crooks can filch the very contours of selfhood. In this respect, the rise of deepfakes is the culmination of the internet's history to date—and probably only a low-grade version of what's to come. Vladimir Nabokov once wrote that *reality* is one of the few words that means nothing without quotation marks. He was sardonically making a basic point about relative perceptions: When you and I look at the same object, how do you *really know* that we see the same thing? Still, institutions (media, government, academia) have helped people coalesce around a consensus—rooted in a faith in reason and empiricism—about how to describe the world, albeit a fragile consensus that has been unraveling in recent years. Social media have helped bring on a new era, enabling individuated encounters with the news that confirm biases and sieve out contravening facts. The current president has further hastened the arrival of a world beyond truth, providing the imprimatur of the highest office to falsehood and conspiracy. But soon this may seem an age of innocence. We'll shortly live in a world where our eyes routinely deceive us. Put differently, we're not so far from the collapse of reality.

Foer notes that we cling to reality today, and that

> We still very much live in Abraham Zapruder's world. That is, we venerate the sort of raw footage exemplified by the 8 mm home movie of John F. Kennedy's assassination that the Dallas clothier captured by happenstance. Unedited video has acquired an outsize authority in our culture. That's because the public has developed a blinding, irrational cynicism toward reporting and other material that the media have handled and processed—an overreaction to a century of advertising, propaganda, and hyperbolic TV news. The essayist David Shields calls our voraciousness for the unvarnished "reality hunger." Scandalous behavior stirs mass outrage most reliably when it is "caught on tape." Such video has played a decisive role in shaping the past two U.S. presidential elections. In 2012, a bartender at a Florida fund-raiser for Mitt Romney surreptitiously hit record on his camera while the candidate denounced "47 percent" of Americans—Obama supporters all—as enfeebled dependents of the federal government. A strong case can be made that this furtively captured clip doomed his chance of becoming president. The remarks almost certainly would not have registered with such force if they'd merely been scribbled down and written up by a reporter. The video—with its indirect camera angle and clink of ambient cutlery and waiters passing by with folded napkins—was far more potent. All of its trappings estified to its unassailable origins.Donald Trump, improbably, recovered from the *Access Hollywood* tape, in which he bragged about sexually assaulting women, but that tape aroused the public's passions and conscience like nothing else in the 2016

> presidential race. Video has likewise provided the proximate trigger for many other recent social conflagrations. It took extended surveillance footage of the NFL running back Ray Rice dragging his unconscious wife from a hotel elevator to elicit a meaningful response to domestic violence from the league, despite a long history of abuse by players. Then there was the 2016 killing of Philando Castile by a Minnesota police officer, streamed to Facebook by his girlfriend. All the reports in the world, no matter the overwhelming statistics and shattering anecdotes, had failed to provoke outrage over police brutality. But the terrifying broadcast of his animalistic demise in his Oldsmobile rumbled the public and led politicians, and even a few hard-line conservative commentators, to finally acknowledge the sort of abuse they had long neglected.

Foer writes this takes us to the heart of the problem, because it is natural to trust one's own senses, to believe what one sees—a hardwired tendency that the coming age of manipulated video will exploit.

> Consider recent flash points in what the University of Michigan's Aviv Ovadya calls the "infopocalypse"—and imagine just how much worse they would have been with manipulated video. Take Pizzagate, and then add concocted footage of John Podesta leering at a child, or worse. Falsehoods will suddenly acquire a whole new, explosive emotional intensity. But the problem isn't just the proliferation of falsehoods. Fabricated videos will create new and understandable suspicions about everything we watch. Politicians and publicists will exploit those doubts. When captured in a moment of wrongdoing, a culprit will simply declare the visual evidence a malicious concoction. The president, reportedly, has already pioneered this tactic: Even though he initially conceded the authenticity of the *Access Hollywood* video, he now privately casts doubt on whether the voice on the tape is his own. In other words, manipulated video will ultimately destroy faith in our strongest remaining tether to the idea of common reality. As Ian Goodfellow, a scientist at Google, told *MIT Technology Review*, "It's been a little bit of a fluke, historically, that we're able to rely on videos as evidence that something really happened." The collapse of reality isn't an unintended consequence of artificial intelligence. It's long been an objective—or at least a dalliance—of some of technology's most storied architects.
>
> ….
>
> Fake-but-realistic video clips are not the end point of the flight from reality that technologists would have us take. The apotheosis of this vision is virtual reality. VR's fundamental purpose is to create a comprehensive illusion of being in another place. With its goggles and gloves, it sets out to trick our senses and subvert our perceptions. Video games began the process of transporting players into an alternate world, injecting them into another narrative. But while games can be quite addictive, they aren't yet fully immersive. VR has the potential to more completely transport—we will see what our avatars see and feel what they feel. Several decades ago, after giving the nascent technology a try, the psychedelic pamphleteer Timothy Leary reportedly called it "the new LSD."
>
> ….
>
> The ability to manipulate consumers will grow because VR definitionally creates confusion about what is real. Designers of VR have described some consumers as having such strong emotional responses to a terrifying experience that they rip off those chunky goggles to escape. Studies have already shown how VR can be used to influence the behavior of users after they return to the physical world, making them either more or less inclined to altruistic behaviors. Researchers in Germany who have attempted to codify ethics for VR have warned that its "comprehensive character" introduces "opportunities for new and especially powerful forms of both mental and behavioral manipulation, especially when commercial, political, religious, or governmental interests are behind the creation and maintenance of the virtual worlds." As the VR pioneer Jaron Lanier writes in his recently published memoir, "Never has a medium been so potent for beauty and so vulnerable to creepiness. Virtual reality will test us. It will amplify our character more than other media ever have." Perhaps society will find ways to cope with these changes. Maybe we'll learn the skepticism required to navigate them. Thus far, however, human beings have displayed a near-infinite susceptibility to getting duped and conned—falling easily into worlds congenial to their own beliefs or self-image, regardless of how eccentric or flat-out wrong those beliefs may be. Governments have been slow to respond to the social challenges that new technologies create, and might rather avoid this one. The question of deciding what constitutes reality isn't just epistemological;

> it is political and would involve declaring certain deeply held beliefs specious. Few individuals will have the time or perhaps the capacity to sort elaborate fabulation from truth. Our best hope may be outsourcing the problem, restoring cultural authority to trusted validators with training and knowledge: newspapers, universities. Perhaps big technology companies will understand this crisis and assume this role, too. Since they control the most-important access points to news and information, they could most easily squash manipulated videos, for instance. But to play this role, they would have to accept certain responsibilities that they have so far largely resisted.

Foer concludes:

> In 2016, as Russia used Facebook to influence the American presidential election, Elon Musk confessed his understanding of human life. He talked about a theory, derived from an Oxford philosopher, that is fashionable in his milieu. The idea holds that we're actually living in a computer simulation, as if we're already characters in a science-fiction movie or a video game. He told a conference, "The odds that we're in 'base reality' is one in billions." If the leaders of the industry that presides over our information and hopes to shape our future can't even concede the existence of reality, then we have little hope of salvaging it.

▶▶ *Read more in Franklin Foer, "The era of fake video begins," The Atlantic (May 2018).*

Increased IT security at hospitals does not equal fewer cyberattacks, breaches

Source: http://www.homelandsecuritynewswire.com/dr20180606-increased-it-security-at-hospitals-does-not-equal-fewer-cyberattacks-breaches

June 06 – The Verizon Data Breach report indicates the health care sector is the top target for cyberattacks. And, as hospitals do more to guard against attacks, it's not necessarily translating into fewer data breaches, according to research from the University of Notre Dame.

A study titled "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," published in *MIS Quarterly*, found that the increased use of information technology security systems by hospitals did not equal fewer breaches, contrary to predictions.

Lead author Corey Angst, professor of IT, Analytics, and Operations in Notre Dame's Mendoza College of Business, says, "It even seems that only certain types of hospitals are able to reap the benefits of having a greater number of IT security systems. Those hospitals that symbolically, as opposed to substantively, adopt practices are not effective in using IT security to thwart breaches. We also found that it takes time for hospitals to realize the benefits of substantive adoption."

Notre Dame says that the team studied data breaches in U.S. hospitals from 2005-2013. Depending on the year, the number of hospitals varied from 4,000 to almost 6,000 — nearly every hospital in the U.S. The researchers continued to collect data on hospital breaches through May 2018.

A February phishing attack on Ohio-based Aultman Health Foundation potentially breached the data of 42,600 patients. The California-based Center for Orthopedic Specialists notified 85,000 patients that a February ransomware attack on its IT vendor may have breached their data. And a March breach within Maryland-based LifeBridge Health and LifeBridge Potomac Professionals potentially exposed some 500,000 patients.

"While our report suggests there was a spike in breaches in the first quarter of 2018, our assessment is that these things tend to fluctuate quite a bit over the years," Angst says. "But to be clear, the threat to hospitals is significant and not decreasing in any meaningful way at least going back to 2006."

The Verizon report suggests hospitals are inviting more threats because they are adopting new technologies at a rapid pace. Although Angst agrees with the observation, the study's results indicate that hospitals that are early adopters of innovative IT solutions have a lower likelihood of suffering a breach. Angst emphasizes that simply purchasing IT security systems is not an adequate response.

"New processes, including training, changes in mindsets and procedures, need to accompany any technology," Angst says. "In addition, it appears there is a learning curve associated with gaining value from IT security. It takes time for the benefits to accrue."

The military wants to know what technology can do to improve information warfare.

Source: https://www.nextgov.com/emerging-tech/2018/06/military-seeks-new-tech-weaponize-information/148808/

graphicwithart/Shutterstock.com

June 07 – Knowledge is power, and the Defense Department wants to ensure it can outpower any enemy in any domain. But first, it needs to know what is technically possible and how industry can support those efforts.

Information warfare—controlling the flow of information in and out of a battlespace to gain a tactical edge—is one of the oldest military tactics in existence. But with the rise of the internet and other advanced communications technologies, it is fast becoming a core tool in every military's playbook.

In February 2017, Russian military leaders announced the existence of an information warfare branch, replete with troops trained in propaganda and other information operations. In the U.S., these duties are performed by troops in the Joint Information Operations Warfare Center.

The U.S. Army and JIOWC are hosting an industry event on June 26-28 in McLean, Virginia, to identify potential industry and academic partners, find out what new technologies are available to support information operations and determine what kind of products and services the military might want to contract for in the future. While the Army is hosting the event, representatives from the entire Defense Department have been invited to attend.

The information gathered during the event will help JIOWC develop requirements for future procurements to "support the emerging domain of operations in the information environment," according to a notice on FedBizOpps.

Those requirements will likely fall under one of four capability areas:

Characterize and assess the informational, physical and human aspects of the security environment. This includes determining the relevance of information; situational awareness of the region in which operations are being conducted, including perceptions and attitudes; and analysis of other ongoing information operations conducted by other actors.

Integration of physical and informational power. This includes assessing the relative effectiveness of physical and information operations toward a specific goal; conducting operations that influence other actors' ability and willingness to conduct physical and information operations; and assess those actors' ability to respond to U.S. physical and information operations.

Ability to execute and modify options. This includes the ability to integrate "physical and informational activities designed to achieve psychological effects" and adjust information operations with the "same level of competency as physical power."

Institutionalize the integration of physical and informational power. This includes changing the way the military views information operations; organizing, training and equipping military units to properly integrate the two; and leveraging both powers to achieve objectives.

Military leaders will kick off the event with a talk on the importance of information operations, then split the attendees into the four capability areas for in-depth discussions. Time will also be set aside for attendees to conduct demos showcasing their technologies.

Facial ID Technology Used in 2020 Tokyo Olympics

Source: https://www.tolonews.com/science-technology/facial-id-technology-used-2020-tokyo-olympics

Jan 2018 – **Facial recognition technology will be used at the Tokyo 2020 Olympics and Paralympics to control the entry of athletes, officials and journalists at the games' venues, according to Japan Times.**

The decision to implement high-tech identification follows concerns about terrorism. The games' organizers aim to bolster security and prevent those involved in the 2020 Games from borrowing official ID cards to access venues. Digital verification will make it difficult to use stolen or forged cards and likely reduce waiting times.

The technology won't be used for spectators, who will be asked to show their tickets and submit to luggage checks just as in the previous Olympics, the sources, who declined to be named, said Saturday.

The organizing committee will distribute ID cards bearing facial photos for those involved in the games. The total is expected to reach around 300,000 to 400,000 and includes athletes and media representatives.

When they enter the venues via the competition entrances or media facilities, their faces will automatically be checked against registered photos for discrepancies.

Japan's Justice Ministry deployed gates using facial recognition technology to screen passengers at Tokyo's Haneda airport in October.

The Tokyo Olympics are scheduled to be held from July 24 to Aug. 9, followed by the Paralympics from Aug. 25 to Sept. 6. Given Japan's hot and humid summers, organizers are also studying how to get people into the venues quickly.

The internet of things is built to leak

By Gilad Rosner (*The Hill*)

For all the cases of hackers illegally accessing data from IoT products, few consumers are aware that many IoT devices are designed to collect and share potentially private data as part of their normal operation. The stakes are enormous: as more products come equipped with cameras and microphones — not to mention thermal sensors, accelerometers, facial and biometric analysis, and GPS — we are quietly building a sensor fabric that may soon be inescapable, even inside private spaces like the home.

Novel transmitter protects wireless data from hackers

By Rob Matheson

Source: http://www.homelandsecuritynewswire.com/dr20180613-novel-transmitter-protects-wireless-data-from-hackers

June 13 – Today, more than eight billion devices are connected around the world, forming an "internet of things" that includes medical devices, wearables, vehicles, and smart household and city technologies. By 2020, experts estimate that number will rise to more than twenty billion devices, all uploading and sharing data online.

But those devices are vulnerable to hacker attacks that locate, intercept, and overwrite the data, jamming signals and generally wreaking havoc. One method to protect the data is called "frequency hopping," which sends each data packet, containing thousands of individual bits, on a random, unique radio frequency (RF) channel, so hackers can't pin down any given packet. Hopping large packets, however, is just slow enough that hackers can still pull off an attack.

Now MIT researchers have developed a novel transmitter that frequency hops each individual 1 or 0 bit of a data packet, every microsecond, which is fast enough to thwart even the quickest hackers.

The transmitter leverages frequency-agile devices called bulk acoustic wave (BAW) resonators and rapidly switches between a wide range of RF channels, sending information for a data bit with each hop. In addition, the researchers incorporated a channel generator that, each microsecond, selects the random channel to send each bit. On top of that, the researchers developed a wireless protocol — different from the protocol used today — to support the ultrafast frequency hopping.

"With the current existing [transmitter] architecture, you wouldn't be able to hop data bits at that speed with low power," says Rabia Tugce Yazicigil, a postdoc in the Department of Electrical Engineering and Computer Science and first author on a paper describing the transmitter, which is being presented at the IEEE Radio Frequency Integrated Circuits Symposium. "By developing this protocol and radio frequency architecture together, we offer physical-layer security for connectivity of everything." Initially, this could mean securing smart meters that read home utilities, control heating, or monitor the grid.

"More seriously, perhaps, the transmitter could help secure medical devices, such as insulin pumps and pacemakers, that could be attacked if a hacker wants to harm someone," Yazicigil says. "When people start corrupting the messages [of these devices] it starts affecting people's lives."

Co-authors on the paper are Anantha P. Chandrakasan, dean of MIT's School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science (EECS); former MIT postdoc Phillip Nadeau; former MIT undergraduate student Daniel Richman; EECS graduate student Chiraag Juvekar; and visiting research student Kapil Vaidya.

Ultrafast frequency hopping

One particularly sneaky attack on wireless devices is called selective jamming, where a hacker intercepts and corrupts data packets transmitting from a single device but leaves all other nearby devices unscathed. Such targeted attacks are difficult to identify, as they're often mistaken for poor a wireless link and are difficult to combat with current packet-level frequency-hopping transmitters.

With frequency hopping, a transmitter sends data on various channels, based on a predetermined sequence shared with the receiver. Packet-level frequency hopping sends one data packet at a time, on a single 1-megahertz channel, across a range of 80 channels. A packet takes around 612 microseconds for BLE-type transmitters to send on that channel. But attackers can locate the channel during the first 1 microsecond and then jam the packet.

"Because the packet stays in the channel for long time, and the attacker only needs a microsecond to identify the frequency, the attacker has enough time to overwrite the data in the remainder of packet," Yazicigil says.

To build their ultrafast frequency-hopping method, the researchers first replaced a crystal oscillator — which vibrates to create an electrical signal — with an oscillator based on a BAW resonator. However, the BAW resonators only cover about 4 to 5 megahertz of frequency channels, falling far short of the 80-megahertz range available in the 2.4-gigahertz band designated for wireless communication. Continuing recent work on BAW resonators — in a 2017 paper co-authored by Chandrakasan, Nadeau, and Yazicigil — the researchers incorporated components that divide an input frequency into multiple frequencies. An additional mixer component combines the divided frequencies with the BAW's radio frequencies to create a host of new radio frequencies that can span about 80 channels.

Randomizing everything

The next step was randomizing how the data is sent. In traditional modulation schemes, when a transmitter sends data on a channel, that channel will display an offset — a slight deviation in frequency. With BLE modulations, that offset is always a fixed 250 kilohertz for a 1 bit and a fixed -250 kilohertz for a 0 bit. A receiver simply notes the channel's 250-kilohertz or -250-kilohertz offset as each bit is sent and decodes the corresponding bits.

But that means, if hackers can pinpoint the carrier frequency, they too have access to that information. If hackers can see a 250-kilohertz offset on, say, channel 14, they'll know that's an incoming 1 and begin messing with the rest of the data packet.

To combat that, the researchers employed a system that each microsecond generates a pair of separate channels across the 80-channel spectrum. Based on a preshared secret key with the transmitter, the receiver does some calculations to designate one channel to carry a 1 bit and the other to carry a 0 bit. But the channel carrying the desired bit will always display more energy. The receiver then compares the energy in those two channels, notes which one has a higher energy, and decodes for the bit sent on that channel.

For example, by using the preshared key, the receiver will calculate that 1 will be sent on channel 14 and a 0 will be sent on channel 31 for one hop. But the transmitter only wants the receiver to decode a 1. The transmitter will send a 1 on channel 14, and send nothing on channel 31. The receiver sees channel 14 has a higher energy and, knowing that's a 1-bit channel, decodes a 1. In the next microsecond, the transmitter selects two more random channels for the next bit and repeats the process.

Because the channel selection is quick and random, and there is no fixed frequency offset, a hacker can never tell which bit is going to which channel. "For an attacker, that means they can't do any better than random guessing, making selective jamming infeasible," Yazicigil says.

As a final innovation, the researchers integrated two transmitter paths into a time-interleaved architecture. This allows the inactive transmitter to receive the selected next channel, while the active transmitter sends data on the current channel. Then, the workload alternates. Doing so ensures a 1-microsecond frequency-hop rate and, in turn, preserves the 1-megabyte-per-second data rate similar to BLE-type transmitters.

"Most of the current vulnerability [to signal jamming] stems from the fact that transmitters hop slowly and dwell on a channel for several consecutive bits. Bit-level frequency hopping makes it very hard to detect and selectively jam the wireless link," says Peter Kinget, a professor of electrical engineering and chair of the department at Columbia University. "This innovation was only possible by working across the various layers in the communication stack requiring new circuits, architectures, and protocols. It has the potential to address key security challenges in IoT devices across industries."

The work was supported by Hong Kong Innovation and Technology Fund, the National Science Foundation, and Texas Instruments. The chip fabrication was supported by TSMC University Shuttle Program.

The partisan brain: Why people are attracted to fake news and what to do about it

By Andrea Pereira and Jay J. Van Bavel

Source: http://www.homelandsecuritynewswire.com/dr20180614-the-partisan-brain-why-people-are-attracted-to-fake-news-and-what-to-do-about-it

June 14 – Orwell's famous novel, *1984*, describes a totalitarian government in which the party in power manipulatese the minds of its citizens through perpetual war, government surveillance, propaganda, and aggressive police, and demands that they abandon their own perceptions, memories, and beliefs in favor of party propaganda.

In this dystopian nightmare, people are forced against their will to adopt the beliefs of the ruling party. However, modern research in political science, psychology, and neuroscience suggests that people are often quite willing to adopt the (mis)beliefs of political parties and spread misinformation when it aligns with their political affiliations.

While it is widely accepted that identification with a political party – or partisanship – shapes political judgments such as voting preferences or support for specific policies, there is now evidence that it may shape belief in more elemental information. For example, US Democrats and Republicans disagree on scientific findings, such as climate change, economic issues, and even facts that have little to do with political policy, such as crowd sizes. These examples make it clear that people can ignore their own eyes and ears even in the absence of a totalitarian regime.

The influence of partisanship on cognition is a serious threat to democracies, because they assume that citizens have access to factual knowledge in order to participate in public debates and make informed decisions in elections and referenda. If that knowledge is biased, then the resulting decisions made by citizens are likely to be biased as well. Worse, there are reasons to believe that this knowledge can be actively and voluntarily distorted in order to shape the outcome of certain democratic processes.

For example, the UK Prime Minister, Theresa May, has publicly accused Russia of ‘planting fake stories’ to ‘sow discord in the West’, and suggested that fake news (spread by Russia) has influenced several national elections in Ukraine, Bulgaria, France and the US, as well as the Brexit campaign. Likewise, roughly 126 million Americans may have been exposed to Russian trolls’ fake news on Facebook during the 2016 US Presidential election. This stresses the scope and consequences of political misinformation.

An identity-based model of political belief

We recently developed a model to understand how partisanship can lead people to value party dogma over truth. Because identification with a political party is a voluntary and self-selected process, people are usually attracted to parties that align with their personal ideology. Political parties are also social groups that generate a feeling of belonging and identity – similar to fans of a sports club. Indeed, neuroimaging research has found that the human brain represents political affiliations similarly to other forms of group identities that have nothing to do with politics. As such, identification with a political party is likely to activate mental processes related to group identities in general.

Social groups fulfil numerous basic social needs such as belonging, distinctiveness, epistemic closure, access to power and resources, and they provide a framework for the endorsement of (moral) values (cf. Fig. 1). Political parties fulfil these needs through different means. For example, political rallies and events satisfy belonging needs; party elites and think tanks provide policy information; party members model norms for action; electoral success confers status and power; and party policy provides guidance on values.

Because partisan identities can fulfil these goals, they generate a powerful incentive to distort beliefs in a manner that contradicts the truth. Similar to a tug of war, when these identity goals are stronger than our accuracy goals they lead us to believe in fake news, propaganda, and other misinformation. In turn, these beliefs shape political attitudes, judgements, and behaviours.

The importance of each goal varies across individuals and contexts. When our accuracy goals are more important than the other goals, we will be more likely to arrive at accurate conclusions (insofar as we have access to factual information). Conversely, when one or more identity goals outweigh our accuracy goal, we will be more likely to distort our beliefs to align with the beliefs of our favourite political party or leader. When party beliefs are factually correct, our identity goals will generate accurate beliefs; but when party beliefs are incorrect, our identity goals will lead us to false beliefs.

This process is likely intensified when competing political parties threaten moral values and access to resources, since these factors increase group conflict. Political systems dominated by two competing groups, like the Labour and Conservative parties in the UK, may heighten partisan motives because they are particularly effective at creating a sense of ‘us’ vs. ‘them’.

How can we reduce biases related to partisanship?

To reduce partisan bias, our model suggests that interventions should either fulfil social needs that drive partisanship or increase the strength of accuracy goals. To make this effective in a political context, policy makers need to first determine which goals are valued by an individual and then aim to fulfil those goals. For example, when people are hungry for belonging, interventions should either affirm a feeling of belonging or make other social groups available or salient to each individual.

When trying to correct a false belief, one risks threatening the target’s identity or revealing a gap in their knowledge, creating a feeling of uncertainty that is highly aversive. For instance, one study found that simply denying a false accusation did not change beliefs. However, denying the accusation while also providing an alternative explanation for the event did. Thus, an effective way of correcting people’s beliefs about false news might be to enrich the corrective information in order to provide a broader account of the news.

Another strategy is to enhance accuracy goals. This can be done by activating identities associated with this goal, such as scientists, investigative journalists, or simply the identity of someone who cares about the truth. Another possibility is to incentivise accuracy or accountability. For instance, incentives and education that foster curiosity towards science, accuracy and accountability, can reduce partisan bias. Interacting with counter-partisan sources or being made aware of one's ignorance about policy details also reduces political polarisation.

Another factor to keep in mind while building interventions is the importance of the source of the message. We know that people resist influence from out-groups. Therefore, interventions should aim at appealing to a superordinate identity that includes all targets of the message – like all British people – or use a trusted source within the targets' political party to deliver the message.

Conclusion

Partisanship represents a threat to democracy. For example, there is evidence that foreign propaganda leverages existing social and moral divisions to drive a wedge between citizens. Social media might exacerbate expressions of moral outrage. Indeed, our research has found that moral emotional language is more likely to be shared on social media, but only within one's political group –which can lead to disconnected political echo chambers and political polarisation. It is crucial to tackle these issues to ensure a healthy and robust democracy.

***Andrea Pereira** is a post-doctoral researcher at New York and Leiden Universities.*
***Jay J. Van Bavel** is Professor of Psychology and Neural Science at New York University.*

Why 50,000 ships are so vulnerable to cyberattacks

Source: http://www.homelandsecuritynewswire.com/dr20180614-why-50-000-ships-are-so-vulnerable-to-cyberattacks

June 14 – The 50,000 ships sailing the sea at any one time have joined an ever-expanding list of objects that can be hacked. Cybersecurity experts recently displayed how easy it was to break into a ship's navigational equipment. This comes only a few years after researchers showed that they could fool the GPS of a superyacht into altering course. Once upon a time objects such as cars, toasters and tugboats only did what they were originally designed to do. Today the problem is that they all also talk to the internet.

The story so far

Stories about maritime cybersecurity are only going to proliferate. The maritime industry has been slow to realize that ships, just like everything else, are now part of cyberspace. The International Maritime Organization (IMO), the UN body charged with regulating maritime space, has been late and somewhat slow in considering appropriate regulation when it comes to cybersecurity.

In 2014, the IMO consulted their membership on what maritime cybersecurity guidelines should look like. Two years later they issued their interim cybersecurity risk management guidelines, which are broad and not particularly maritime specific. And now, unsurprisingly, ships are being hacked.

Complexity of the maritime industry

There are several core issues that make cybersecurity for the maritime industry particularly challenging to address.

First, there are many different classes of vessel, all of which operate in very different environments. These vessels tend to have different computer systems built into them. Significantly, many of these systems are built to last over 30 years. In other words, many ships run outdated and unsupported operating systems, which are often the ones most prone to cyber-attacks.

Second, the users of these maritime computer systems are constantly in flux. Ship crews are highly dynamic, often changing at short notice. As a result, crew members are often using systems they are unfamiliar with, increasing the potential for cybersecurity incidents relating to human error. Further, the maintenance of onboard systems, including navigational ones, is often contracted to a variety of third parties. It is perfectly possible that a ship's crew have little understanding of how onboard systems interact with each other.

A third complexity is the linkage between onboard and terrestrial systems. Many maritime companies stay in constant communication with their vessels. The cybersecurity of the ship is also dependent, then, on the cybersecurity of the land-based infrastructure that makes this possible. The implications of such dependencies was made clear in 2017 when a cyber-attack on the systems of A.P. Moller-Maersk resulted in cargo delays across their entire fleet. This is particularly challenging for the IMO who can govern the likes of port regulations, but have very little control over the wider systems and processes of maritime operators.

Steps in the right direction

In 2017, the IMO amended two of their general security management codes to explicitly include cybersecurity. The International Ship and Port Facility Security Code (ISPS) and International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. Making cybersecurity an integral part of these processes should ensure that operators are at least conscious of cyber-risks.

Hopefully, this is the start of a more holistic approach to maritime cybersecurity regulation. The knowledge gained from these new cyber-risk assessments may enable the IMO to develop a broader set of cybersecurity regulations. There is a lot of low-hanging fruit to be picked, for example by harmonizing some equipment requirements with existing cybersecurity standards adopted by other sectors.

Turning the ship around

The maritime industry is undoubtedly behind other transportation sectors, such as aerospace, in cybersecurity terms. There also seems to be a lack of urgency to get the house in order. After all, the cyber-specific amendments to the ISM and ISPS don't come into force until 1 January 2021, and they only represent the beginning of a journey. So the maritime industry seems particularly ill-equipped to deal with future challenges, such as the cybersecurity of fully autonomous vessels.

On the positive side, the slow and steady approach to development of cybersecurity regulations at least provides the opportunity to learn from other sectors and fully understand maritime cybersecurity risks, rather than make hasty ill-informed decisions.

Development of robust maritime cybersecurity regulations is going to be a very slow, and possibly painful, process. But, the ship has started turning

__Keith Martin__ is Professor, Information Security Group, Royal Holloway.
__Rory Hopcraft__ is PhD Researcher, Royal Holloway.

EDITOR'S COMMENT: The guided-missile destroyers *USS Fitzgerald* and *USS John S. McCain* collided with commercial ships in June and August, 2017 respectively. Could these be due to cyber attacks? I also "dare" to recall two cases in the Hellenic Navy where vessels (one frigate and one supporting torppidos' fishing ship) moored on underwater structures. In both cases, captains where hghly experienced Navy officers and incidents happened during day time with nice weather. **What if?**

This is not a drill: A cyberthreat reality check

By Ali Moore

Source: https://pursuit.unimelb.edu.au/articles/this-is-not-a-drill-a-cyberthreat-reality-check

It's difficult, if not impossible, to find a security expert who doesn't think a major cyberattack with potentially devastating consequences is a case of when, not if.

There were 47,000 cyber incidents in Australia alone last year. An 'incident' is defined as one or more unexpected events that are likely to compromise an organisation's operations. That's 128 a day. Five every hour.

Many of them are online scams or frauds.

But the rest are more serious, often aimed at disrupting businesses, sometimes destroying them; stealing secrets and compromising operations; making money and costing companies both cash and reputation.

Lloyds of London rates cyberthreats in Australasia as the second highest risk to our Gross Domestic Profit after a market crash.

Meanwhile, all those hackers are hard at work, and here's five reasons why they often succeed.

1. PEOPLE

We are the biggest problem - opening that email, clicking on that attachment. You might think when you read the headlines that "I would never do that" but you'd be surprised who would. Phishing emails are still one of the most popular (and successful) tools of the cybercriminal.

And hackers are using increasingly sophisticated techniques to get you to help them access the systems you're connected to. It's not always obvious you're being had.

Last year, reports to the government's Cybercrime Online Reporting Network indicated losses of over A$20 million as a result of compromised emails. That's up from A$8.6 million the previous year - a jump of 130 per cent.

But as the government notes, it's probably a fraction of the real number because it's a crime that is commonly underreported.

There were 47,000 cyber incidents in Australia alone last year. Picture: Getty Images

2. OBSOLETE TECHNOLOGY

It may seem extraordinary that in the 21st century as we move closer to the reality of driverless cars, some of our critical infrastructure still operates on systems so old they can no longer be patched; this basically means the technology can no longer be updated to address any vulnerabilities.

Last November, Victoria's Auditor General looked at four government departments as well as the Victoria Police, and found 41 per cent of the systems that support their critical business functions were obsolete. At Victoria Police, that figure sat at 79 per cent, while a number of public hospitals were also found to have unsupported or outdated technology.

Victoria is not alone, every state has its version of the issue. Old systems are hard to replace – it's time consuming, complicated and expensive.

3. BETTER HACKERS

Whether they're motivated by money (the criminal) or to push a political or social cause (the hacktivist) or to steal secrets (the nation state) or an employee who acts consciously or unwittingly (the insider) - hackers are agile, adaptable, and innovative.

As quickly as one bit of malware is detected, another pops up. Speak up as a target and you risk losing visibility and it is virtually impossible to stay ahead of the game. It may not even be an attack on your own systems – think of your supply chain. Brand new software can come with its very own pre-loaded infections and the more connected we are, the higher the risk.

Officially, nation states have the greatest capability to compromise Australian networks, with the resources of an entire country behind them. The government says it's detected extensive state-sponsored activity against itself and the private sector.

Just in the last three years, we've seen the Russians deny they brought down Ukraine's power grid; the North Koreans deny they were behind the global chaos of the *Wannacry* ransomware attack; and the Chinese deny they installed malware on computers at Australia's Bureau of Meteorology.

The Australian Prime Minister Malcolm Turnbull calls cybersecurity the new "frontier of warfare".

Australia now has a very publicly declared offensive cyber capability, with the government officially directing the Australian Signals Directorate to use that capability to "disrupt, degrade, deny and deter" organised offshore cyber criminals.

But what's not clear is when and how we're using it. Indeed, just what is acceptable under international law when it comes to offensive cyber operations is the subject of significant debate.

Last year, the UN Group of Governmental Experts on Information Security, which had been negotiating norms of state behaviour in cyber space, collapsed. The sticking point was the application of international law. As a result, the "Wild West" of cyberspace remains with no established legal framework to address cyberattacks internationally.

4. CORPORATE PRIORITIES

Cybersecurity is now on the priority list for most corporate boards in Australia, but what exactly does that mean? Two years ago, the American research and advisory firm Gartner said organisations spent an average of just 5.6 percent of their entire IT budget on security and risk management.

Technology systems, rather than security and risk, have traditionally been where the money's gone. But the good news is, that's changing.

This month, Australia's Cyber Emergency Response Team (AusCERT) found that 58 per cent of organisations in Australia increased their security spend in 2017.

A change in the legislative landscape is also helping to focus minds, with a number of new regulatory requirements aimed at greater accountability.

A key change is the new mandatory breach reporting laws. Since February of this year, businesses have been required to report data breaches involving personal information that is likely to result in "serious harm" to the individual affected. In the first 6 weeks of the new regime there were 63 breaches. The next quarterly report will be interesting reading to see if this trend continues.

But there is still a fair way to go when it comes to how business manages its data use.

For its latest State of Information Security survey, PriceWaterhouseCoopers interviewed more than 9,500 senior executives across the globe. It found that just over half have an overall information security strategy. Which means around half don't. And this could prove disastrous if current threats continue to rise.

5. HUMAN NATURE

How many times have you been working on your laptop when the 'updates available' box has popped up, and you've clicked 'tonight', 'tonight', 'tonight' repeatedly – and when tonight comes you're away from your computer and you never install it.

You should.

And it's the same for business.

The sheer number of businesses that are not adequately protected, and don't have backups, is astounding. If they did approach their cybersecurity properly, hackers would find their jobs a lot harder.

The Australian Cyber Security Agency makes the point that "too many"of the incidents they deal with "could have been prevented had organisations employed established and relatively straightforward cybersecurity measures".

The problem is, human nature often gets in the way. Whether it's making the decision to install the measures in the first place, following the rules and keeping them up to date, or finding a way to hack around them... humans are the biggest vulnerability.

Australia's cybersecurity is an issue tackled by Ali Moore's This is Not A Drill series in partnership with the University of Melbourne, Asialink, the Wheeler Centre and the ABC. This episode will air on the ABC News Channel at 10pm on Sunday 24 June.

***Ms Ali Moore** is Vice-Chancellor's Fellow @ University of Melbourne*

Why some claim credit for cyberattacks – and some don't

Source: http://www.homelandsecuritynewswire.com/dr20180615-why-some-claim-credit-for-cyberattacks-and-some-don-t

June 15 – The decision to claim credit for a cyberattack on a government or institution depends on both the goals of the attack and the characteristics of the attacker, according to a study co-authored by a UConn political scientist that is one of the first to look into the voluntary claiming of cybersecurity operations.

The type of attacker – whether a state or a non-state actor such as a terrorist group – determines whether credit is claimed for a cyberattack and how it is communicated, according to the study, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," forthcoming in the Journal of Global Security Studies. Co-authors of the study are Evan Perkoski, assistant professor of political science at UConn, and Michael Poznansky, assistant professor of political science at the University of Pittsburgh's Graduate School of Public Affairs.

UConn says that among the findings of the study:

- Both states and non-state actors face similar decisions in the lifecycle of a cyberattack, yet the characteristics of each can cause their strategies to diverge, "particularly with the optics of credit claiming."
- While most research treats cyber operations as distinct from more traditional elements of state power, states "may be able to leverage their cyber assets to achieve many of the same goals most frequently pursued with conventional forces."
- The decision to privately or publicly acknowledge sponsorship of an attack may provide "crucial information about both their motives and identity."

Perkoski says that in developing the study, a distinction was drawn between cybercrime and cyberblackmail because "they are inherently different forms of cyber operations with different goals in mind."

He notes that typically the goal of cybercrime is personal or financial gain, which does not follow the same logic as states operating against other states in cyberspace. In the case of cyberblackmail, the attacker wants the victim to know something was stolen, such as when North Korea hacked into the servers at Sony following the release of "The Interview," a film about assassinating its leader, Kim Jong-un.

"They hacked into Sony servers, stole certain information, and said we want you to do X or we'll release this information," Perkoski says. "It was a form of pretty basic blackmail. It's not operating on the same kind of pattern of state-on-state or non-state-on-state intervention in cyberspace. In that case, you only want to communicate with the person you've hacked and let them know you have this material. It's a different dynamic than a state trying to coerce an opponent to give up their nuclear arms program."

The researchers began their collaboration studying cybersecurity several years ago while they were both fellows at the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government. Perkoski is a specialist in political violence and terrorism, while Poznansky studies clandestine and covert interventions.

Perkoski says the alleged Russian meddling in the 2016 U.S. Presidential election fits into the study's findings. Russian operatives reportedly hacked into the Democratic National Committee computers to obtain emails from the Hillary Clinton campaign, and then used social media trolls to sway public opinion toward Donald J. Trump's campaign.

"Russia wouldn't get as many benefits from claiming their operation," he says. "They're not looking to get attention for their message or cause. They're really looking to influence the way events might unfold. Because it's unclear, it makes it hard for the U.S. to take a hard stance against them. You can always play devil's advocate and say maybe it wasn't Russia, as President Trump has said. Maybe it was some guy in his basement hacking on his own. In that case, it makes sense that Russia doesn't want to claim credit, to limit possible escalatory dynamics."

One of the challenges in confirming clandestine state-sponsored activities is that it may only be possible from classified documents. Perkoski says scholars are still learning important details about historic events with the release of classified documents decades after the events occurred, such as the recent release of documents concerning the controversial 1961 U.S. invasion of Cuba at the Bay of Pigs.

"When we think about what's happening with the U.S. and Russia, Iran, and North Korea and their cyber operations, it may be another 30 or 40 years until we know what's really going on," he says.

Perkoski says the study helps to clarify the fact that not all cyber operations are inherently anonymous, and that actors may claim credit for them, which then opens the door to using cyber tools as almost traditional instruments of state power. At the same time, there is no firm understanding of how non-state actor groups operate in cyberspace.

"We know a lot about how terrorists and insurgent groups come together, and what sustains them, but we don't have a theory of any of this stuff for a hacking organization and whether they follow the same paradigms or not," Perkoski says. "How do you defeat a militant organization or a hacking collective like Anonymous when they're all spread out around the world, they operate in states that don't have extradition treaties with the United States, and they might even operate in some states that give them de facto immunity? We know, for instance, that some Russian hackers don't get support from the government, but they allow them to operate freely because they're operating in Russia's own interest. That raises a lot of questions about understanding these groups."

At the same time, Perkoski says, as advances in cybersecurity improve the ability of government and law enforcement agencies to track hackers, terror groups and militant organizations are moving away from technology.

"There was a period when government agencies were quite effective at using these tools to their advantage and gaining information. Now I think you're seeing militant groups respond to that and go more low-tech, to avoid some of those weaknesses," he says. "Look at how the U.S. found Osama bin Laden in Pakistan. It wasn't through hacking or satellite imagery. It was by tracking a courier going to his house and meeting with other guys who would go back to Afghanistan. It was very much traditional signals intelligence that the CIA has been using for 50 to 60 years."

Drexel University (online)

Source: https://duo.online.drexel.edu/are-you-ready/

Drexel UNIVERSITY | ONLINE

GRADUATE CERTIFICATE
IN CYBERSECURITY AND INFORMATION PRIVACY COMPLIANCE

- ◈ Curriculum covers topics such as third party compliance, international regulations, and information breach management, along with the best strategies to navigate associated issues
- ◈ Designed for both technical and non-technical professions
- ◈ Taught by Kline School of Law faculty, a nationally-recognized group of scholars and practitioners with tremendous expertise in their field
- ◈ Available in a 100% online format
- ◈ Special tuition plans for employees and members of partner organizations
- ◈ No GMAT, GRE or LSAT scores required

From Nord Stream to Novichok: Kremlin propaganda on Google's front page

Source: http://www.homelandsecuritynewswire.com/dr20180615-from-nord-stream-to-novichok-kremlin-propaganda-on-google-s-front-page

June 15 – On 24 May, an international team of investigators from the Netherlands, Australia, Malaysia, and Ukraine announced that a Russian anti-aircraft missile was directly responsible for the downing of Malaysian Airlines Flight 17 (MH17). The following day, Australia and the Netherlands officially declared that they held the Russian government responsible for the downing. Concurrently, Bellingcat, McClatchy DC Bureau, and the *Insider* released a joint report revealing a Russian military intelligence commander as a key person of interest in the investigation.

Initial analysis of social media reactions to these announcements indicated that Kremlin outlets were struggling to effectively counter the new evidence implicating Moscow in the downing of MG17. However, over the next week, conspiracy theories and disinformation narratives from Russian propaganda outlets found a foothold on an impactful and unlikely medium: Google's front page.

In the weeks following the new announcements surrounding the MH17 investigation, articles from Russian state-controlled news outlets RT, TASS, and Sputnik regularly appeared on the front page of English-language Google searches for "MH17" through the site's Top Stories function.

Searches run through various VPNs and Google's incognito mode reveal that the pattern is not limited to a particular English-speaking community or locale. Additionally, searches for "MH17" through a Berlin-based VPN exposed similar results from RT and Sputnik's German-language affiliates.

The articles published by these sites present an alternative reality to the downing of MH17, often discrediting existing evidence, pushing false narratives, and creating conspiracy theories to undermine readers' understanding of events.

Unfortunately, the prevalence of Kremlin propaganda in Google's Top Stories is a relatively consistent pattern. In the days and weeks following several other international events, including the poisoning of Sergei and Yuliya Skripal, Russian propaganda similarly haunted Google's front page.

***Bradley Hanlon** is Research Assistant at the Alliance for Securing Democracy.*

CyberSecurity: Now in Medical Equipment as Well

Source: https://i-hls.com/archives/72314

Oct 2016 – In a letter to diabetes patients, **Johnson & Johnson** said that **OneTouch Ping** insulin pump owners who are anxious about a potential hack can stop using the remote, or program the pump to limit the maximum dose of insulin. **A security vulnerability was found in the insulin pump that a hacker could exploit to overdose diabetic patients with insulin,** though the company describes the risk as low.

Following the vulnerabilities revealed in 2011 and the 2012 demonstration of a hack at a security conference in Melbourne, Australia, the US Food and Drug Administration began in 2013 formulating cybersecurity guidance for medical device makers.

Since these attacks require technical expertise and sophisticated equipment, "the probability of unauthorized access to the OneTouch Ping system is extremely low", the company said in a warning letter to physicians and patients. In case of piracy, the pumps could see their programming changed to provide a higher than expected dose of insulin.

According to a 2011 Bloomberg News report , a cybersecurity flaw in the device could allow hackers to infuse potentially life-threatening additional doses of insulin without a patient's knowledge. In 2011, however, well-known hacker Jay Radcliffe stunned a Las Vegas tech show audience by gaining access to his own Medtronic insulin pump. They are sold by Animas Corporation, a subsidiary of Johnson & Johnson.

According to crcconnection.com, nearly 114,000 patients use the device in the United States and Canada.

At issue is the so-called "Internet of things", according to BlackBerry Chief Security Officer David Kleidermacher and Security Expert Graham Murphy.

It is believed attacks against the medical device could take place from up to 10 meters away, but this could be extended to one or two kilometers with off-the-shelf radio kit. This research highlights why it is so important to wait for vendors, regulators and researchers to fully work on these highly complex devices.

Three Emerging Technologies with Life-Saving Potential

Source: http://www.govtech.com/public-safety/Three-Emerging-Technologies-with-Life-Saving-Potential.html

June 14 – The National Oceanic and Atmospheric Administration reported that 2017 was the most expensive year on record for disasters in the U.S., estimating $306 billion in total damage. The FBI also reported 2017 as having the most incidents and the most people killed in any one year by active shooters. With this rise in crises across the United States, data and technology have an increasingly important role in improving emergency management departments across the country. Approximately 240 million calls are made to 911 in the United States each year, with at least 80 percent coming from wireless devices, yet many emergency management systems still operate on legacy systems made for wireline phones. As a result, people in need are unable to easily share precise locations or send media messages to responders, making emergency communication and resource coordination more costly and difficult.

City and national government entities are already making strides in using analytics to improve emergency response operations, from Google's 911 study in San Francisco to the Office of Management and Budget's (OMB) work with FEMA to crowdsource real-time information during emergencies. Yet, emerging technologies present even greater opportunities to make our emergency management systems more intelligent, secure, and effective. While cities have long sought to integrate tech into disaster response, the available technologies and opportunities are constantly evolving. Today, artificial intelligence (AI), the Internet of Things (IoT), and blockchain offer the potential to generate, transmit and read emergency-related data for better decision-making in crises.

ARTIFICIAL INTELLIGENCE

Industry and government leaders today are discussing—and seeing firsthand—how AI can change the way we work, get around, serve residents, and much more. **In emergency management, AI can help predict, evaluate, and simulate incidents to improve response times and streamline resource dispatch processes.**

The city of Los Angeles, city of San Francisco, and multiple San Mateo County cities are now using the One Concern platform, which employs artificial intelligence through analytical disaster assessment and calculated damage estimates. Specifically, One Concern assigns a "unique, verified 'digital fingerprint'" to every element in a city, modeling the entire system, and monitoring the impact of each disaster and climate change on a location. The team leverages data on city infrastructure and former disasters to predict the damage when different disasters hit, accomplishing 85 percent accuracy within 15 minutes on a city block-level basis. In Santa Clara County, One Concern worked with Woodside Fire Protection District, Portola Valley, and Woodside to gather jurisdiction-specific critical infrastructure data and model their Seismic Concern product, providing a bigger picture of risks in the area.

For 911 call evaluation, the Association of Public-Safety Communications Officials (APCO) and IBM Watson recently partnered to use speech-to-text analytics software to help agency directors better analyze conversations and compare them to pre-scripted content in real time. As a result, directors can learn from real-time conversations between callers and dispatchers, and iterate training materials to help improve the performance of 911 staff. The city of Memphis also used Watson Analytics to reveal trends in emergency medical services. The IBM team conducted 80 stakeholder interviews and gathered relevant data from various city departments on the 911 process, including 911 call volume and use of emergency services. IBM helped the different city agencies pool and analyze information to identify challenges and improve joint decision-making and enlisted the help of third parties—such as health insurance companies and health care clinics—for non-emergency calls. Based on the analysis, the city determined that about 64 percent of ambulance callers would be better served by long-term care for chronic conditions rather than emergency room visits, and was thereby able to reduce emergency service costs by $20 million.

The Cincinnati Fire Department has started using a new predictive analytics system to surface recommendations to dispatchers on appropriate responses to emergency calls based on a number of different variables including location, weather, and inputs from similar types of calls. The AI software helps the department prioritize and respond more effectively to the 80,000 requests they receive annually, reportedly improving emergency response times for the department.

INTERNET OF THINGS (IoT)

IoT refers to a network of physical objects embedded with sensors and software that collect data and communicate with one another. As it relates to emergency management, **IoT can be used to enhance d ata collection from the physical environment and quickly communicate this data to different city departments.**

Weather-related disasters such as hurricanes or floods sometimes prevent emergency response teams from reaching certain locations. This obstruction reduces teams' ability to track damage, notify the public with up-to-date information, and respond in a timely manner. However, if IoT devices were present in these areas, they would be able to more easily broadcast signals and communicate critical data such as temperature, water quality, or smoke. With this data, government can make more informed decision on how to deploy resources during a disaster situation. Today, the Rio de Janeiro City Hall Operations Center uses sensors to collect real-time data about weather, traffic, police, and medical services in the city. In the United States, the city of Houston worked with AT&T after Hurricane Harvey to deploy IoT technology for identifying damage and communicating information.

From a more proactive standpoint, cities can place IoT on city infrastructure to monitor risk factors and surface data about potential emergencies. For example, The Lower Colorado River Authority (LCRA) uses 270 sensors to measure how fast water is moving across a stream and models what water may do at different touch points. From this, LCRA can proactively manage floods and easily get ahead of water-related disasters in the area.

Cost, security, and interoperability challenges are still barriers to scaling IoT solutions across a city for emergency management. However, the power to share data during emergency situations—as well as a number of other use cases, from monitoring air quality to locating parking spots—make these challenges worth overcoming.

BLOCKCHAIN

Of these three technologies, blockchain is in the earliest stages of development, but is a tool that some claim will be transformational for how we transact data. Blockchain is a distributed and immutable digital ledger, secured by cryptography, which can be programmed to record a series of transactions. Its most scalable application today is bitcoin, a cryptocurrency and payment system still growing in its use around the world.

The benefit of blockchain in emergency management is that it provides interoperability and transparency. In terms of interoperability, blockchain can be adopted as a universal system across organizations—similar to the internet—and allow multiple parties across that system to coordinate resources in an emergency. In a disaster relief scenario, multiple parties are often contributing resources to aid an affected area. If all parties involved in this scenario were to adopt a blockchain-based shared system of record, they could coordinate more efficient disaster responses, ensuring resources were allocated to the areas where they are needed most. The Centers for Disease Control and Prevention (CDC) is now looking to pilot blockchain for the use case of public health data surveillance, where it will collect and communicate data to entities who treat patients in disaster relief scenarios, including local public health agencies, hospitals, and pharmacies.

Regarding transparency in the disaster relief scenario, blockchain could provide an immutable record, accessible by everyone, to illustrate what resources have been dedicated to an area and by whom.

This transparent record—to which anyone could submit an entry—would reduce the possibility of resource diversion and corruption in these types of scenarios.

UNICEF is testing blockchain technology to track the status of international grants in a secure way that is accessible by the public. Along these same lines, FEMA's Public Assistance program could be another great use case for blockchain, tracking where resources are going after a disaster. Seeing the potential of blockchain, the Department of Homeland Security's Science and Technology Directorate awarded $1.3 million in grants to explore blockchain technology through their Small Business Innovation Research program. Several technical limitations prevent blockchain from scaling across any industry today, but emergency management departments across cities should take the opportunity to learn about the technology and its various applications to plan for future IT systems.

Above all, a city's ability to collect, analyze and communicate data is critical to effective and efficient emergency management. AI, IoT and blockchain are all technologies that enable more sophisticated data processes and can improve the capacity and efficiency of emergency staff.

Red-teaming by DHS 'quietly and slowly' uncovers agency vulnerabilities

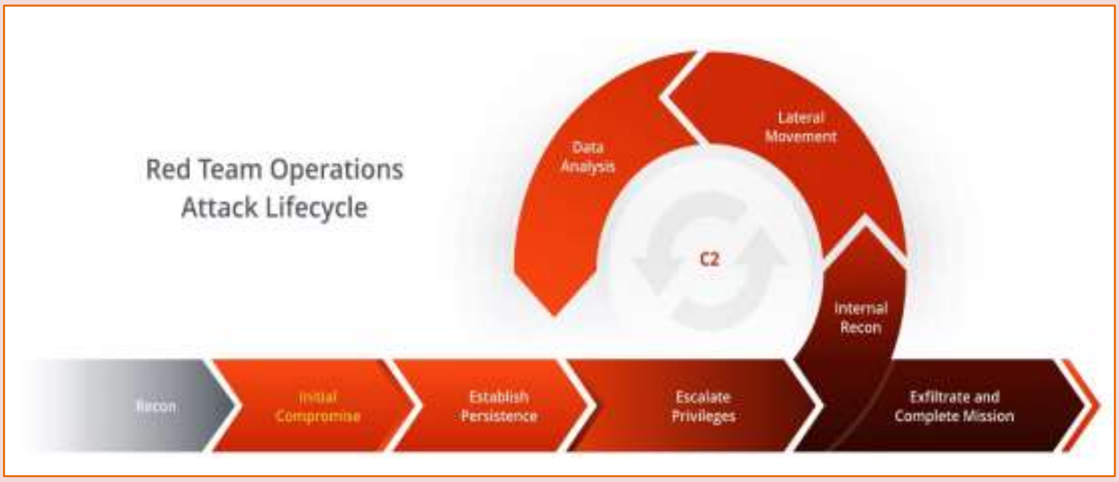
Source: https://www.cyberscoop.com/red-teaming-dhs-quietly-slowly-uncovers-agency-vulnerabilities/

June 13 – The Department of Homeland Security has carried out quiet "red-teaming" exercises at three federal agencies, breaking into networks and telling agency officials how it was done. The goal is for officials to more quickly realize when a hacker has a foothold in their systems to keep them from exfiltrating data.

"We go really quietly and slowly, just like an adversary would," Rob Karas, the DHS official leading the red-team exercises, said Wednesday at the Cybersecurity Leadership Forum presented by Forcepoint and produced by CyberScoop and FedScoop.

Karas said his team has carried out five such red-team drills at three agencies, declining to name them.

The 90-day assessments begin with about two weeks of reconnaissance that might culminate in a carefully crafted spearphishing email.



"We send a phishing email and it beacons back to our host in Arlington, and then we have a foothold" into the organization, said Karas, DHS's director of national cybersecurity assessments and technical services. "From there, we pivot to other computers, to domain controllers, to enterprise computers."

His team of security testers litters the target network with signatures representing ransomware or other malware — no actual malicious code is used. They check to see if the agency's security operations center (SOC) detects malicious scans of the network and how it responds. The ethical hackers also attempt to exfiltrate large volumes of data over various channels.

Cybersecurity experts say rigorous red-team exercises are key to giving an organization a clear understanding of its vulnerabilities. A recent Office of Management and Budget report suggests many agencies still lack that clear understanding. Just 27 percent of agencies say they can detect and investigate "attempts to access large volumes of data," and even fewer agencies test that capability annually, according to the report.

One of the more infamous cases of an undetected data heist at an agency was the 2015 hack of the Office of Personnel Management. Hackers sat unnoticed on the agency's network for months and made off with the personal data of 22 million current and former federal workers.

Karas is trying to keep that from happening again.

At the end of a red-team assessment, Karas's team sits down with officials from the target agency to deliver their security verdict. It might take three or four days for an agency to notice Karas's testers had created or deleted accounts on the network, he said. "Other things might take them weeks — or they might not notice at all."

After the initial assessment, the plan is to do another test in six months or a year's time, he said.

Security Vulnerabilities Expose BMW Cars to Hackers

Source: https://i-hls.com/archives/83673

June 23 – A new research discovered critical vulnerabilities in several BMW car models. Researchers from Keen Security Lab, a cybersecurity research unit of Chinese company Tencent, have conducted an in-depth analysis of various systems present in BMW cars and discovered 14 locally and remotely exploitable vulnerabilities. Keen Security Lab focused on the head unit, the telematics control unit (TCU or T-Box), and the central gateway module in several BMW models. The experts tested various systems that critically influence the vehicle functioning and security, supplying just another proof of the importance of autonomous cars security.

The research raises high interest in the car industry, as much of the information in it has not been published yet in order to avoid malicious use of the vulnerabilities before they are patched. The full results will be published only in the beginning of 2019, according to securityweek.com.

Karmaba Security specializes in car cybersecurity and prevention of malicious access to these vehicles' smart systems. According to Assaf Harel, the company's Chief Scientist and Co-Founder, "The vulnerabilities identified enable the assailant a remote control over the operating system of the vehicle, the electronic control unit (ECU), and from that stage, he is able to do gain control over a whole vehicle fleet.

"The defense and information security approach that applies solutions incorporating updates for identifying attacks is obsolete and not efficient regarding the security of the vehicle's activities during the ride.

"In real time, these systems will not be reliable, as securing one part of the smart vehicle system will not guarantee the same level of security for another part. This is the reason why our security focuses on the manufacturer's specific definitions regarding each model of the car, so we are able to supply a complete peripheral defense that sees the vehicle as a whole and not just a system in it.

"Another clear conclusion drawn from the research, so far, emphasizes our claim that in fact, there is no efficient way to secure the gateway because the information has to stream among the vehicle's systems. Using 'intermediary'/third-party solutions will only expose the systems to more vulnerabilities.

"The vehicle systems' interfaces vis a vis external interfaces, such as battery charging, diagnosis and testing services, autonomous parking etc. require a wide array of communication channels. Securing each and every one of the will harm the vehicle's performances.

He concluded that with the company's innovative technology, "the autonomous security adjusts itself to the clear definitions of the car and its technological interfaces without harming performances. This is achieved by controlling one main channel, that includes all the basic definitions so that the vehicle remains secure and free from any external hostile influence."

Innovative OSINT Solution to Expose Important Web Information

Source: https://i-hls.com/archives/83670

June 22 – Currently, one of the biggest challenges that intelligence officers around the world face on a daily basis is the information overload in open channels, how to monitor it and distill from it real intelligence to identify illegal activity. A new OSINT (Open Source Intelligence) solution has been recently exposed by an Israeli firm. BLER Systems, specializing in security and cyber intelligence solutions, developed the Target Profiler System – an integrated, enterprise-grade intelligence and investigation-support solution, used to conduct business intelligence, and criminal and terror investigations for enterprise organizations, financial institutions and government agencies.

According to the company announcement, their solution, which is already being used by intelligence organizations and other customers around the world, is able to automatically and quickly examine huge amounts of information from the Internet, social networks and web applications, and Dark Web channels and to extract from it actionable intelligence.

The system is modular, open architecture and scalable and can be very simply adapted by clients to deal with the tasks they require.

The system has various configurable capabilities:

- Link analysis – identifying social connections, similar preferences and common groups between suspects at multiple levels.
- Sentiment analysis capabilities – analyzing the target's posts and identifying feelings and word anomalies.
- Face analytics – identifying the target in multiple pictures captured by a profiling process, including characteristics such as age, race, emotion, whether the suspect is wearing lenses or glasses, and many other unique features.
- Identifying whether the suspect is already in the system, based on their picture, and indicating a confidence level.
- Identifying potential activity in Dark Web marketplaces.
- Indicating on a map the last location of a target, using data collected from social networks and websites.
- TimeLine – viewing and analyzing all target posts and social network activities, easily finding the most-liked post and all relations between targets according to likes, tagging and comments activity.

BLER Systems is a part of the Avnon Group – a leading supplier of HLS & cyber technologies and equipment.

What War Games Tell Us About the Use of Cyber Weapons in a Crisis

By Jacquelyn G. Schneider

Source: https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis

The second battle of Libya during World War II. A British brigadier commanding tank units in Tobruk instructs officers on an operation, using a sand table for demonstration purposes. British Army/Wikimedia

June 21 – Last week, Jason Healey argued that “there is now a well-documented instance of cyber deterrence,” pointing to a report of conversations within the Obama administration. Some White House officials argued against a cyberattack, citing asymmetric vulnerabilities in tit for tat engagements within the cyber domain. Healey highlights a powerful example of cyber restraint within the Obama administration, but is it deterrence? The United States has also exercised restraint in the nuclear domain, but it is unclear even now whether that restraint is a result of adversary deterrence efforts or a normative nuclear taboo. So what is driving the cyber restraint Healey identified?

In order to understand the motivations behind cyber behaviors, I performed a longitudinal analysis of strategic war games conducted at the Naval War College from 2011-2016. These free-play games, which feature 150-200 U.S. government experts and senior leader players, situate players within crisis scenarios and then allow them to play all instruments of national power to resolve the crisis. Over the years that I analyzed, these war games varied the adversary, the intensity of the crisis, and the players. Like the evolution of cyber operations in real life, the way cyber capabilities were designed in the games evolved in complexity, representing the institutions and capabilities that developed from 2011 to 2016. Bottom line: a lot of things changed between the games.

However, what remained remarkably consistent across the games was how players utilized cyber operations. In five of the six games, players launched offensive cyber operations only after conventional weapons conducted destructive attacks. Additionally, players were more willing to place systems on nuclear alert than to launch cyberattacks or even cyber-enabled information operations. Over and over players cited concerns about escalation in their cyber restraint, articulating fears that cyberattacks could “lead to nuclear war.” Further, in all of the six games, despite large scale adversary cyberattacks (up to nuclear effects in allied countries), none of the “blue” teams chose to respond to cyberattacks. In one game, a player explained, “this is cyber—it’s different psychologically.” In all of these games, players were told who had attacked them in cyberspace, essentially priming them for retaliation. The lack of support for retaliation in these games is, therefore, especially compelling.

This research suggests two types of restraint: restraint in using cyber operations and an overall restraint in responding to cyber operations. What causes this restraint? Is it deterrence or is it a cyber taboo? These games couldn't definitively answer this puzzle, but they do suggest a series of potential hypotheses about cyber restraint. First, restraint in utilizing cyber operations could be a uniquely U.S. phenomenon tied to a perception of asymmetric cyber vulnerabilities combined with overwhelming conventional superiority (what Healey's article alludes to). In other words, why open the Pandora box of cyber operations when the United States has the option to respond to any significant problems with economic punishment or military might? A secondary hypothesis suggests that cyber restraint derives from a false cyber-nuclear equivalency in which the institutional legacy of Strategic Command and the narrative of "strategic" cyber weapons has led to an extension of the nuclear taboo to the cyber domain. These hypotheses are largely agnostic to the adversary—mainly because the games I analyzed featured different adversaries with different cyber, conventional, and nuclear capabilities. Restraint was consistent despite these threat differences, suggesting that cyber restraint was not a product of adversary-tailored deterrence but instead internally derived incentives.

Perhaps more puzzling is why these games also show restraint when responding to cyber operations—a phenomenon not found in the nuclear domain. Once again, this could be a strictly U.S. form of restraint, in which the United States—as the largest economic and military power—can withstand significant cyberattacks without retaliation because it relies on a greater conventional and nuclear superiority. However, there could be a more generalizable explanation which links cyber restraint to emotions and argues that the virtual and novel threat of cyber operations fail to generate the kind of fight or flight gut reaction created by more evolutionarily-primed threats. If this final hypothesis is true, then the restraint in cyber response may permeate beyond U.S. borders and suggest that cyber operations are highly unlikely to lead to escalation in other domains.

Finally, the one war game which did not display cyber use restraint has important implications for foreshadowing the long-term strength of the cyber taboo. In that game, the player leading the blue team executed an extraordinarily risk-acceptant "escalate to dominate" strategy that featured early first use of cyberattacks against a series of domestic and military targets followed by a large-scale conventional offensive. This game highlighted how important the risk proclivity and personality of leaders are to when and how cyber operations are used. Previous research highlighted the large role that risk aversion played in the Obama administration and restraint across a series of domains. The Trump administration is much more risk acceptant, which may lead to less incentives for self-restraint in cyberspace.

***Dr. Jacquelyn G. Schneider** is an assistant professor and affiliate faculty at the Center for Cyber Conflict Studies at the U.S. Naval War College. This article represents her views alone and do not represent those of the U.S. Naval War College, the U.S. Navy, or the Department of Defense.*

HENG
LIANHE ZAOBAO
Singapore
SINGAPORE
Heng
BANK
BELIEVE ME, IT'S SO MUCH EASIER TO DO IT ONLINE!
CartoonArts International: www.nytsyn.com/cartoons

EMERGENCY RESPONSE

Terror attacks: how psychological research can help improve the emergency response

By Nicola Power, Laura Boulton, and Olivia Brown

Source: http://www.homelandsecuritynewswire.com/dr20180522-terror-attacks-how-psychological-research-can-help-improve-the-emergency-response

May 22 – Western society is engaged in what has been referred to as an "arms race" against terrorism. Atrocities are increasingly characterized by novel and low-cost methods with the sole aim of causing as much death and destruction as possible. "The terrorist" is no longer a distinct enemy from a defined terrorist organization, but is increasingly associated with diverse and wide-ranging beliefs.

So in this age of unpredictability, how can the emergency services prepare themselves to respond to a terror attack, like the one at the Ariana Grande concert in Manchester in 2017? We've looked into the psychology of decision making and how the key lessons from The Kerslake Report – which evaluated the emergency response during the Manchester attack – could be applied on the ground.

Design for the unpredictable

Operational plans must be designed to reflect the unpredictable nature of terror attacks. One of the key lessons from the Kerslake Report related to the mismatch between current operational procedures and the nature of real-world attacks. It was noted that the agreed joint operational response to terror attacks – so-called Operation PLATO – did not fit Manchester.

Operation PLATO is based on an assumption of firearms being present, meaning that only specialist trained and protected responders can operate in the affected areas. However, the Manchester attack was the result of a bomb and no firearms were present. In fact, none of the most recent attacks in the U.K., such as Finsbury Park, London Bridge or Westminster involved firearms. This begs the question of how the emergency services can best prepare for terror attacks when modern day terrorism is becoming less and less predictable?

One way to cope with unpredictability during operational planning could be to shift focus away from the "type" of incident (for example, firearms) and focus on the dynamic risk currently faced at scene (threat to lives of responders).

Our research found an inherent conflict for incident commanders is the trade-off between saving public life while ensuring that this does not disregard the safety of responders. Operation PLATO did not fit the Manchester attack because the response was based on the assumption that a terror attack involved an active threat to responder life. As a result, fire crews played "no meaningful role". However, there was no active threat. Developing operational procedures that focus on the actual risk to responders, rather than hypothetical assumptions about the type of risk involved during a terror attack, may make future operational planning more effective.

Training and decision making

There needs to be more training to develop skills in dynamic decision making. The Kerslake Report praised the work of Greater Manchester Police's Force Duty Officer. They recognized that standard protocols did not fit the situation and allowed responders to operate in an area from which they should (according to PLATO) have been withdrawn. This decision to deviate from procedure was hailed as "one of the most crucial decisions taken" and the Force Duty Officer was congratulated for their dynamic "life or death" decision making.

But if this decision had gone wrong – for example a second explosive device was in the area – things would have turned out very differently. It is important therefore to consider how to best support commanders to know when and when not to break procedures, without putting the public at risk.

Psychology teaches us that experienced people can make very fast and accurate decisions in their workplace. This is largely due to what has been termed "recognition primed" decision making, which enables them to quickly recognize subtle cues in the environment that trigger learned responses. Experts can also quickly identify when standard rules no longer fit and they need to develop innovative ways to solve the problem instead.

Our research with firearms police officers shows that more experienced officers use flexible thought processes allowing them to adapt their decisions to changing situations. Whereas less experienced officers used more rigid processing. Such adaptability is thought to be crucial under the uncertain and pressurized conditions of a critical incident.

The importance of flexibility

While emergency services train their staff in technical skills, the development of flexible decision making is often not a specified learning objective. It may occur as a by-product of training or "on the job" experience but it is rarely a core focus.

One way to expedite the development of flexible thinking is through systematically exposing emergency responders to a variety of simulated scenarios where, through guided practice and feedback, they can develop adaptive decision making. By focusing on adaptive expertise specifically in training, (such as "worst case" scenarios that cannot be solved through standard operating procedures), the type of dynamic decision making that was so highly praised in Manchester may be more quickly developed in trainees.

One thing that shines through from our research is the importance of flexibility. Terrorist attacks are increasingly unpredictable, which can render previous response plans obsolete. Manchester provides a key lesson in identifying how the gap between hypothetical plans and the reality of incidents is widening. Taken together, it is hoped that the future of emergency training embeds these lessons, providing a greater focus on the need for flexible planning and dynamic decision making.

__Nicola Power__ is Lecturer in Psychology, Lancaster University.
__Laura Boulton__ is Lecturer in Policing, University of Central Lancashire.
__Olivia Brown__ is Ph.D. Researcher, Lancaster University.

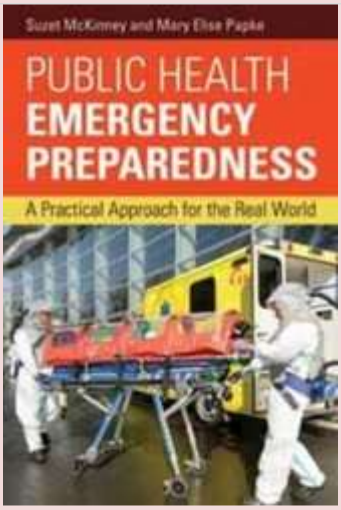
Free login at: https://subscriber.pagesuite-professional.co.uk/subscribe.aspx?source=4&eid=ff46d4e1-5bdd-46b2-b146-36c7511115de

Public Health Emergency Preparedness: Practical Applications for the Real World

By Suzet McKinney and Mary Elise Papke (authors)
Source: http://www.jblearning.com/catalog/9781284069259/

Public Health Emergency Preparedness: Practical Applications for the Real World is a comprehensive examination of the critical competencies necessary to prepare for and respond to Public Health emergencies.

Starting with a historical context of the early preparedness need, the book defines emergency preparedness and the legal framework for the field. The book goes on to cover the full range of the field from hazards and threats to considerations for leadership development in the field. It includes information on roles and responsibilities of local, state, and national organizations, the cycle of practice for preparedness officials, as well as principles of incident management and response; and finally, considerations for leadership development in the field.


Suzet McKinney and Mary Elise Papke
PUBLIC HEALTH EMERGENCY PREPAREDNESS
A Practical Approach for the Real World

With real-world stories and anecdotes throughout, the authors synthesize a wealth of material in an easy-to-read format that stimulates learning and provokes reflection about emergency preparedness.

Key Features:

- Offers a full chapter on medical countermeasures including distribution operations and logistics
- Defines multi-agency coordination systems (MACS) and how they are used in response to disaster events
- Provides thorough coverage of medical surge including the key strategies and tactics needed for aligning public health and healthcare system responses during disaster events
- Explores key ethical considerations during emergency response and details Crisis Standards of Care strategies
- Examines key strategies to ensure the health and safety of first responders and volunteers

Suzet McKinney, DrPH, MPH*-CEO/Executive Director, Illinois Medical District. Dr. Suzet M. McKinney currently serves as CEO/Executive Director of the Illinois Medical District. The Illinois Medical District (IMD), a 24/7/365 environment that includes 560 acres of medical research facilities, labs, a biotech business incubator, universities, raw land development areas and more than 40 healthcare related facilities, is one of the largest urban medical districts in the United States. Dr. McKinney is the former Deputy Commissioner of the Bureau of Public Health Preparedness and Emergency Response at the Chicago Department of Public Health (CDPH), where she oversaw the emergency preparedness efforts for the Department and coordinated those efforts within the larger spectrum of the City of Chicago's Public Safety activities, in addition to overseeing the Department's Division of Women and Children's Health. During her time at CDPH, Dr. McKinney also spearheaded Chicago's efforts as the field test site for the U.S. Department of Homeland Security's (DHS) Generation-3 autonomous biological detection system technology. Dr. McKinney previously served as the Sr. Advisor for Public Health and Preparedness at the Tauri Group, where she provided strategic and analytical consulting services to the U.S. Department of Homeland Security's (DHS), BioWatch Program. Her work at DHS included providing creative, responsive and operationally-based problem-solving for public health, emergency management and homeland security issues, specifically chemical and biological early detection systems and the implementation of those systems at the state and local levels. Dr. McKinney serves on numerous boards, committees and advisory boards. Most recently, she was appointed to the Board of Directors for Thresholds, Susan G. Komen Chicago, Good City Chicago and the African-American Legacy of the Chicago Community Trust. Dr. McKinney is Co-Chair of the National Academies of Science, Engineering and Medicine, Institute of Medicine's (IOM) Forum on Medical and Public Health Preparedness for Disasters and Emergencies and is a member of the IOM's Standing Committee on Health Threats Resilience. She also serves on the Science and Security Board for the Bulletin of the Atomic Scientists, the Board of Scientific Counselors for the U.S. Centers for Disease Control, Office of Public Health Preparedness and Response, as well as the Federal Emergency Management Agency's (FEMA) National Advisory Council (NAC). She has served as an Incident Commander for CDPH and was a member of Chicago's Incident Management Team. She has been responsible for leading multiple emergency response efforts, including Chicago's 2014- 2015 Ebola response; the operational response to the 2009 H1N1 outbreak, which was successful in vaccinating nearly 100,000 residents over a six week timeframe; as well as CDPH's participation in the 2012 NATO Summit response and the 2010 Haiti Earthquake response. Dr. McKinney has earned a reputation as an experienced, knowledgeable public health official with exceptional communication skills. She has served as an on-camera media expert on emergency issues including biological and chemical threats, natural disasters, pandemic influenza, and climate-related emergencies. A sought after expert in her field, she has also provided support to the U.S. Department of Defense's, Defense Threat Reduction Agency, providing subject matter expertise in biological terrorism preparedness to the country of Poland. In academia, Dr. McKinney serves as an Instructor in the Division of Translational Policy and Leadership Development at Harvard University's T.H. Chan School of Public Health and as Adjunct Assistant Professor of Environmental and Occupational Health Sciences at the University of Illinois at Chicago School of Public Health. She also serves as a mentor for the Biomedical Sciences Careers Project, also at Harvard University. Dr. McKinney holds her Doctorate degree from the University of Illinois at Chicago School of Public Health,* *with a focus on preparedness planning, leadership and workforce development. She received her Bachelor of Arts in Biology from Brandeis University (Waltham, MA) where she was also a Howard Hughes Medical Institute Fellow. She received her Master of Public Health degree (Health Care Administration) and certificates in Managed Care and Health Care Administration from Benedictine University in Lisle, IL.*

***Mary Elise Papke, DrPH, MPH**-Senior Public Health Specialist, UWM Joseph J. Zilber School of Public Health*

Firefighters Can Teach Us How To Make Good Decisions Under Pressure

By Tali Sharot

Source: https://www.govexec.com/excellence/promising-practices/2018/06/firefighters-can-teach-us-how-make-good-decisions-under-pressure/148798/

June 07 – Some of the most important decisions you will make in your lifetime will occur while you feel stressed and anxious. From medical decisions to financial and professional ones, we are often required to weigh up information under stressful conditions.

Take for example expectant parents who need to make a series of important choices during pregnancy and labor, when many feel stressed. Do we become better or worse at processing and using information under such circumstances?

My colleague Neil Garrett, now at the Princeton Neuroscience Institute in New Jersey, and I ventured from the safety of our lab to fire stations in the state of Colorado to investigate how the mind operates under high stress. Firefighters' workdays vary quite a bit. Some days are pretty relaxed: They'll spend part of their time washing the truck, cleaning equipment, cooking meals and reading. Other days can be hectic, with numerous life-threatening incidents to attend to: They'll enter burning homes to rescue trapped residents, and assist with medical emergencies. These ups and downs presented the perfect setting for an experiment on how people's ability to use information changes when they feel under pressure.

We found that perceived threat triggered a stress reaction that made the firefighters better at processing information—but only as long as it conveyed bad news.

This is how we arrived at these results. We asked the firefighters to estimate their likelihood of experiencing 40 different aversive events in their life, such as being involved in a car accident or becoming a victim of card fraud. We then gave them either good news (we told them that their likelihood of experiencing these events was lower than they'd thought) or bad news (that it was higher) and asked them to provide new estimates.

Research **has shown that people are normally quite optimistic—they will ignore the bad news and embrace the good.** This is what happened when the firefighters were relaxed. But when they were under stress, a different pattern emerged. Under these conditions, they became hyper-vigilant to any bad news we gave them, even when it had nothing to do with their job (such as learning that the likelihood of card fraud was higher than they'd thought), and altered their beliefs in response. In contrast, stress didn't change how they responded to good news (such as learning that the likelihood of card fraud was lower than they'd thought).

Back in our lab, we observed the same pattern in undergraduates who were told they had to give a surprise public speech, which would be judged by a panel, recorded, and posted online. Sure enough, their cortisol levels spiked, their heart rates went up and, lo and behold, they suddenly became better at processing unrelated, yet alarming, information about rates of disease and violence.

When you experience stressful events, whether personal (waiting for a medical diagnosis) or public (political turmoil), a physiological change is triggered that can cause you to take in any sort of warning and become fixated on what might go wrong. A study using brain imaging to look at the neural activity of people under stress revealed that this "switch" was related to a sudden boost in a neural signal important for learning (known as a prediction error), specifically in response to unexpected signs of danger (such as faces expressing fear). This signal relies on dopamine—a neurotransmitter found in the brain—and, under stress, dopamine function is altered by another molecule called corticotropin-releasing factor.

Such neural engineering could have helped early humans to survive. When our ancestors found themselves in a habitat filled with hungry animals, they benefited from an increased ability to learn about hazards so as to avoid predators. In a safe environment, however, it would be wasteful to be on high alert constantly. A certain amount of ignorance can help to keep your mind at ease. So a "neural switch" that automatically increases or decreases your ability to process warnings in response to changes in your environment might be useful. In fact, people with clinical depression and anxiety seem unable to switch away from a state in which they absorb all the negative messages around them.

It is important to realise that stress travels rapidly from one person to the next. If your co-worker is stressed, you are more likely to tense up and feel stressed yourself. Our brains are designed to transmit emotions quickly to one another, because they often convey important information. Wendy Berry Mendes, a professor of emotion at the University of California, San Francisco, and her colleagues found that when infants were held by their mothers who had just experienced a socially stressful event, the infants' heart rates went up, too. The message transferred via the mother's pounding heart to the baby was of danger—and as a result, the baby avoided interacting with strangers.

You don't even need to be in the same room with someone for their emotions to influence your behavior. Studies show that if you observe positive feeds on social media, such as images of a pink sunset, you are more likely to post uplifting messages yourself. If you observe negative posts, such as complaints about a long queue at the coffee shop, you will in turn create more negative posts.

In some ways, many of us live as if we are in real danger, like firefighters on call, constantly ready to put out the flames of demanding emails and text messages, and respond to news alerts and social media feeds. Repeatedly checking your phone, according to a survey conducted by the American Psychological Association, is related to stress. In other words, a preprogrammed physiological reaction, which evolution has equipped us with to help us avoid famished predators, is now being triggered by a tweet. Tweeting, according to one study, raises your pulse, makes you sweat, and enlarges your pupils more than most daily activities.

The fact that stress increases the likelihood that we will focus more on alarming messages, *together* with the fact that it spreads like a tsunami, can create collective fear that is not always justified. This is because after a stressful public event, such as a terrorist attack or political turmoil, there is often a wave of alarming information in traditional and social media, which individuals absorb well, but that can exaggerate existing danger. And so a reliable pattern emerges following terrorist attacks and financial market downturns: stress is triggered, spreading from one person to the next, which temporarily enhances the likelihood that people will take in negative reports, which increases stress further. As a result, trips are cancelled, even if the terrorist attack took place across the globe; stocks are sold, even when holding on is the best thing to do; and fearmongering political campaigns attract followers, even if they are not anchored in reality.

The good news, however, is that positive emotions, such as hope, are contagious too, and are powerful in inducing people to act to find solutions. Being aware of the close relationship between people's emotional state and how they process information can help us frame our messages more effectively and become conscientious agents of change.

***Tali Sharot** is the director of the Affective Brain Lab and an associate professor of cognitive neuroscience in the department of experimental psychology at University*

College London. She is the author of The Influential Mind *(2017) and* The Optimism Bias *(2011).*

EDITOR'S COMMENT: I like fire fighters a lot! Perhaps this article is restricted to routine urban operations where the enemy is a building or a storage facility or a factory. From personal experience* I think that they are not as efficient when confronted with mega-fires out in the fields. I think that in cases like these, trained military (ground forces only) could do a much better job (assisted by fire fighters).

* In 2010 when a mega fire stormed our estate and house, a high ranked fire fighter was very busy supervising water crews just 200m from us instead of been in a nearby hill observing the movement of the fire driven by very strong constantly changing winds As a result, my house [as a building] was saved by pure luck despite the fact that our damages costed my retirement compensation after +35yrs in service.

France 24: Bataclan Terror Victims Demand: Who Gave Soldiers Order 'Not To Enter'?

"Survivors and families of victims of the 2015 Bataclan attack in Paris filed a legal complaint Friday over the inaction of some soldiers that night in what could expose egregious failings within France's military and political commands. The legal complaint was triggered by the testimony of a top military commander who gave evidence during a parliamentary investigation of the actions of police and military on the night of the attacks of November 13, 2015. **General Bruno Le Ray, Military Governor of Paris**, defended the order he'd given that prevented eight soldiers located near the Bataclan concert hall from intervening in the attack because he thought **'it was unthinkable to put soldiers at risk just hoping, hypothetically, to save other lives,'** Samia Maktouf, a Paris lawyer for the survivors and victims' families, told FRANCE 24. She said the soldiers were told **not to use their weapons or even administer first aid to the many victims** shot during the two-hour siege by jihadists affiliated to the Islamic State (IS) group at the music venue."

New app tracks locations, vitals, keeping first responders safe

Source: http://www.homelandsecuritynewswire.com/dr20180613-new-app-tracks-locations-vitals-keeping-first-responders-safe

June 13 – When first responders are on a mission, being able to quickly and easily track the location of their fellow responders can be challenging, especially in situations where the team is spread out. Many responders are only able to coordinate their locations by radioing each other or the command post and providing a very detailed message on their exact location. This can be time consuming and can change every second if they are in an emergency situation or on a call.

S&T says that, recognizing this limitation, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) funded the development of the Watchtower mobile application, which – as of 27 February 2018 – is available, free of charge for all public safety users. The app allows users to track and report their location using the GPS already built into a smartphone.

The **Watchtower app** also tracks critical vitals, such as heart rates and oxygen levels, during routine and strenuous situations, potentially saving lives. It connects body-worn and other physiological-monitoring sensors using a smartphone's Bluetooth to a dashboard, allowing users to track vitals and make informed decisions. Through this dashboard, if a responder's vital signs indicate trouble, the responder can be evacuated and receive medical attention.

The Watchtower app allows users to:

- Uniquely identify other Watchtower users and display identities on the operational dashboard;
- View and report locations to other Watchtower users and display locations on the operational dashboard;
- Continuously update the user's location;
- View other responders' locations, incidents, vehicle locations and static GIS info (i.e., Command Control trailer, etc.) on a map; and
- View their physiological sensor information from available sensors (i.e., Hexoskin or Zephyr).

"Responders across the nation face numerous on-the-job challenges. At DHS S&T, we make it our mission to look for solutions to these challenges – such as the ones this free app addresses – to help make responders as safe as we possibly can," said DHS S&T Program Manager Cuong Luu.

The app was initially tested on various smartphones during the June 2017 Next Generation First Responder Spiral 2 Technology Experiment in Grant County, Washington. The test included the FirstNet-enabled Sonim phones (a smartphone commonly used by most responders), Grant County-issued smartphones and first responders' personal smartphones.

Based on user feedback from the Grant County exercise, DHS S&T made several improvements to the mobile app and developed the software into an open source code.

S&T notes thatpublic safety organizations can obtain a copy of the Watchtower software to customize for its environment using the Github download site: https://github.com/1stResponder.

Euralarm's Annual Report 2017-2018 published

Zug, June 2018 – Euralarm has released its Annual Report. The publication of the report coincides with the end of the Euralarm Board's three-year mandate and therefore, beyond the usual account of the past year's activities, it also offers a review of the work achieved during that three-year period, particularly in terms of invigorating the Euralarm community.

One of the highlights of the past year was the opening of the new Extinguishing Section of Euralarm and the de facto expansion of the representation of Euralarm to the whole field of active fire protection. Organised as an umbrella association, Euralarm already comprises an electronic fire alarm Section, as well as a Section for electronic security and another for services related to both fire safety and security.

The report follows the structure of Euralarm, with every Section and Technical Committee of the association summarising their activities over the previous year and, where appropriate, providing forecasts and plans for the future.

A running theme of the report is Euralarm's work on building strategic alliances: the reader can find short interviews with stakeholders, Industry leaders and other prominent partners in the fire safety and security business throughout the Annual Report. A major development in that area was a new cooperation agreement with CEN, the European standardisation platform.

Over the 2017-2018 period covered by the report, running between the General Assemblies of the association usually taking place in May or June, Euralarm can also testify of an ongoing growth in membership with Teletek as a new Member in the Fire Section hailing from Bulgaria, and the very dynamic German association BHE extending its membership from the Services also to the Fire and Security Sections. This continuous growth, in line with the trend of the previous years, is as a sign of trust in Euralarm, its organisation, vision and strategy, which are all detailed in the report.

In a concluding section of the document, Euralarm outgoing President Enzo Peduzzi looks back at the three years of his mandate and how the association was set on course to a successful future development.

You can download the Euralarm Annual Report on the Euralarm website.
https://www.euralarm.org/about-euralarm/annual-report/annual-report-2017-2018

About Euralarm
Euralarm represents the electronic fire and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our Members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm Members are national associations and individual companies from across Europe.

Sensors for Public Safety in Mass Shooting Events

Source: https://i-hls.com/archives/83149

May 26 – **In mass shooting events, first responders often lose precious minutes trying to determine the location of the shooter. In the scramble to get out the doors, some people tragically run into the path of the assailant.** Intelligent devices and data analytics from existing sensor infrastructure may play an important future role in minimizing casualties in events such as these.

Armored Things Inc. hopes to give organizations real-time visibility into the movement of people and things by tapping into and federating networks of smart devices.

Parameters such as the location of smartphones can be tracked by Wi-Fi routers, even if the phones aren't connected. Aggregating and interpreting that data could, for example, enable security administrators to detect such anomalies as a crowd forming or people moving more rapidly than usual through a public space, which might indicate a threat.

Armored Things has been working with developers of devices such as cameras and sound sensors to build algorithms that can pick up abnormal movement caught on video or loud sounds and alert human operators to a potential problem. Ultimately, the company wants to tie in smart devices such as emergency lighting, public-address systems and access control equipment to enable security administrators to define automated responses to emergency situations.

The company wants to correlate and connect the data across existing motion sensors, access control systems and wireless infrastructure. For example, an audio gunshot sensor could pinpoint the location of a shooter and instantaneously send the information to emergency responders. Automatic door locks could be engaged to minimize the assailant's movements while lighted guidance systems could quickly escort people to safe exits.

Crisis Management Training – A Guide to Success

By ICMC
Source: https://www.crisisconferences.com/crisis-management-training-guide-success/

June 04 – **Trying to Manage a Crisis and Crisis Response Team without Any Skills and Limited Knowledge is Dangerous to You and Your Organization. But Good Quality Crisis Management Training is Available and Should Be Your First Step in Becoming a Successful Crisis Management Professional.**

Get Qualified to Lead With Crisis Management Training
Why would a company's senior management pick a person to create a crisis plan and help lead a crisis response team when that person never had any crisis management training? If

you were that appointee, wouldn't it be obvious to you that without any training in crisis management you could actually increase your organization's risk? Your missteps could worsen and prolong a crisis. Yet, unfortunately, this is a common course of action by many organizations: appointing someone who's not qualified to take the lead in crisis preparedness and management.

If you've read this far you're probably a person concerned about crisis preparedness. The good news is that good quality crisis management training is available, and you should seek it out. It's the first step in becoming a successful crisis management professional.

Well-led organizations will insist on having people professionally trained and accredited in crisis management. However, if your organization is not aware of this training, you might want to inform them. Lobby management to get you the training you need to enhance your professional credentials so you can help ensure that your organization is crisis ready.

Increase in Crises Driving Demand for More Crisis Management Training

The growing trend in crisis management courses comes from the fact that organizations of all types, for-profit, non-profit, schools, churches, government offices, etc., are having to face increasing numbers of crises. Today's organizations face an onslaught of new or newly recognized threats, everything from cybercrime to active shooters; from sexual harassment charges to terrorism. A major factor behind the increase in crises is social media. Any crisis management course worth its salt will teach about the central role of social media today in both fomenting crises and in managing them.

Social Media Should be a Major Focus in Crisis Management Training

When choosing a course in crisis management it's important to know in advance that social media would be a key aspect of your training. After all, many crises begin and metastasize on social media. Think of cell-phone videos going viral of American Airlines security people dragging a customer off a plane; or the cell phone videos and Twitter storms documenting a racially charged incident in a Starbucks. But it doesn't have to be a social media-induced crisis. Almost all crises will have a large social media component that, if not well managed, will intensify the crisis.

Social media has changed the very paradigm of how organizations even find out that they're in a crisis. Before social media existed it was typically the company that was first to realize it had a crisis on its hands. Say, for example, a railroad company's tank car overturns and leaks a toxic chemical putting a nearby community in harm's way. The train engineer would inform the company, which would, with the help of local first responders then gather facts and communicate outward to the media, to the community, to elected officials, etc. about the crisis.

Contrast that scenario with what often happens today because of social media. Video taken by a person of the leaking tank car would go viral through Facebook or Twitter and be viewed by thousands of people, people now fired up to disparage the railroad company on various social media sites. And all this *before* the company itself even finds out about the accident. Not only are crises happening more often, in large part because or social media, managing the crisis is even more challenging because of the wild west world of social media, where so many emotionally charged people are inclined to shoot first and aim, maybe never. That's why when choosing a crisis management training course, you'll want a strong social media component.

Skills to be Gained from Crisis Management Training

In addition to having a strong social media component, here are some of the other skills you should seek from Crisis Management Training:

- How to know if an incident actually is a crisis.
- How to gauge the severity of a crisis so your organization's responses are proportional.
- How to identify vulnerabilities and what strategies would work to reduce or eliminate those vulnerabilities.
- How to write a crisis plan.
- How to organize a crisis response team.
- How to organize a crisis "war room."
- How to form a working relationship with the CEO on crisis preparedness to make crisis preparedness a prioritized part of the company's culture.
- How to arrive at a decision-making process customized to suit your organization.
- How to manage crisis communications that are a core element of crisis management.
- How to monitor and engage with social media as well as traditional news media during a crisis.
- How to cultivate relationships with respected third parties who could support you in a crisis.

Organizations like PreparedEx have long been offering crisis management courses. So do the Business Continuity Institute and Continuity Insights. Study their curricula and see which one is right for you.

After you've taken the course that gave you the skills you needed to create a crisis plan and organize a crisis response team, you're not finished. You'll have three other tasks you'll need to take on to maximize your organization's preparedness:

1. **Conduct a crisis exercise.** Once you have a plan and a response team in place, they both need to be tested and validated regularly, at least once a year. The testing is done through a table-top exercise (TTX) that realistically simulates a crisis. You simply cannot consider your organization to be fully prepared for a crisis if you've never tested your plan with a TTX, either by conducting one yourself (yes, there are courses available to do this), or by bringing in an outside consultant that specializes in creating and running crisis simulation exercises.
2. **Equip your employees**. Train your employees to be part of the crisis early-warning system of the organization so they know how to spot a potential or actual crisis and how to report it. Crisis preparedness needs to be communicated from the top down and made an important part of your organization's culture.
3. **Build your brand.** You have to nurture your brand or reputation. A strong brand/reputation is like protective armor – it won't necessarily prevent a crisis, but it will definitely lessen the blow. It's beyond the scope of this article to get into the nitty gritty of building a strong brand as a protective armor against crises. It takes a lot of time and effort. But suffice it is to say that strong, well-cultivated brands are far better able to stave off crises and manage them when they occur. Stakeholders for a strong brand — employees, customers, community members, suppliers, shareholders, even regulators and elected officials — are already well-disposed toward your organization and will tend to be far more supportive when a crisis occurs.

One good resource for exploring crisis management courses and keeping your skills up to date is through the International Crisis Management Conference (ICMC), an online community of the world's leading crisis management professionals. ICMC offers a one-day crisis management course and many other resources. Most importantly, the professional crisis managers of ICMC keep each other current on all things crisis management, so becoming a member of ICMC will keep your crisis management skills sharp long after you've taken a crisis management course.

New Drone-Based Thermal Imagery Can Save Lives

Source: https://i-hls.com/archives/83618

June 20 – Traditionally, thermal inspections have been time-consuming, limited to accessible areas, or required manned aircraft that typically yield low-resolution data at a high price. A new technology, the **Thermal Live Map**, **is a real-time mobile mapping solution which delivers insights only thermal imagery can reveal. Thermal Live Map visualizes temperature range variability and creates instant thermal maps for quick, data-guided decisions on the job site.**

The solution developed by DroneDeploy provides immediate visual context to situations unseen by the naked eye — all without a computer, SD card, or internet connection. The new solution uses the latest advancements in edge computing to generate thermal drone maps locally on iOS devices as a DJI drone flies.

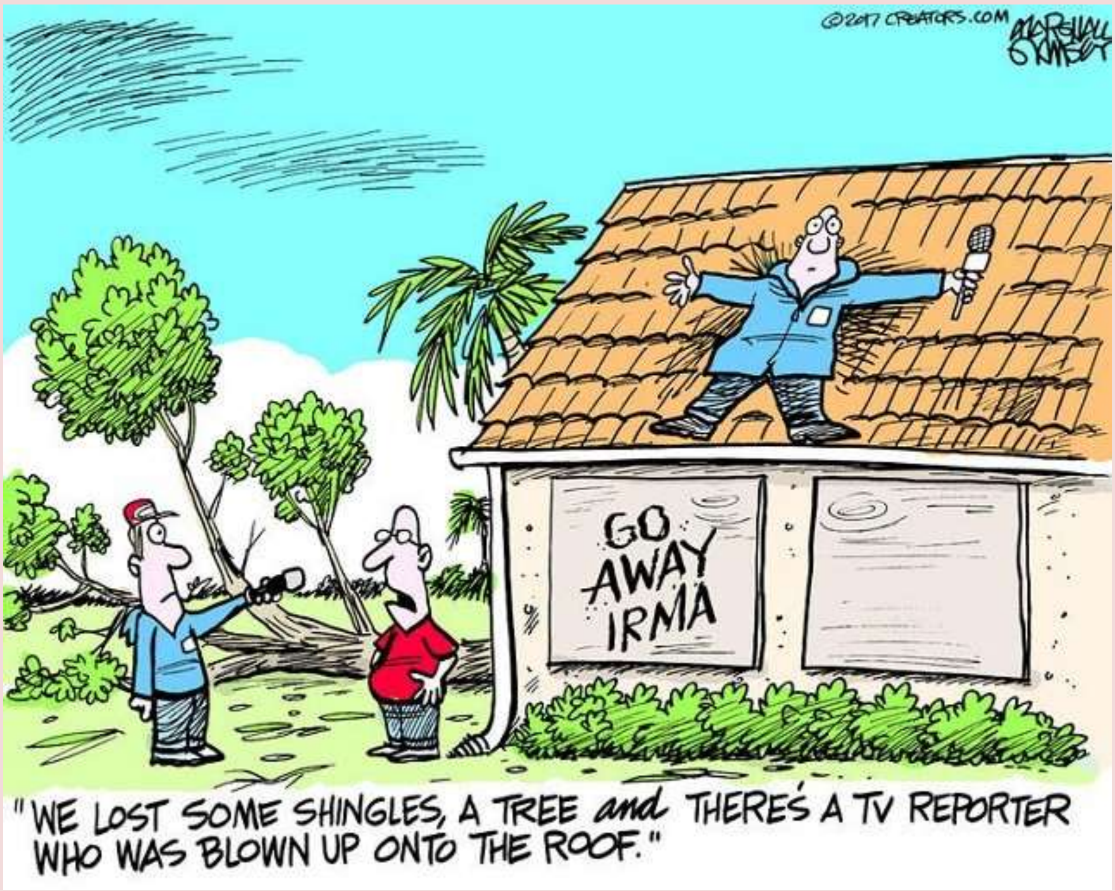
The system allows first responders to view hundreds of acres in minutes, day or night, penetrating hard-to-reach and hard-to-see terrain where missing or injured persons may be awaiting rescue.

The new solution is particularly valuable for firefighting, giving firefighters the ability to see through smoke and keep track of their personnel in large fire scenes. Thermal Live Map also helps locate precisely where the fire is hottest and provides definitive confirmation the fire is extinguished in specific areas, according to businesswire.com.

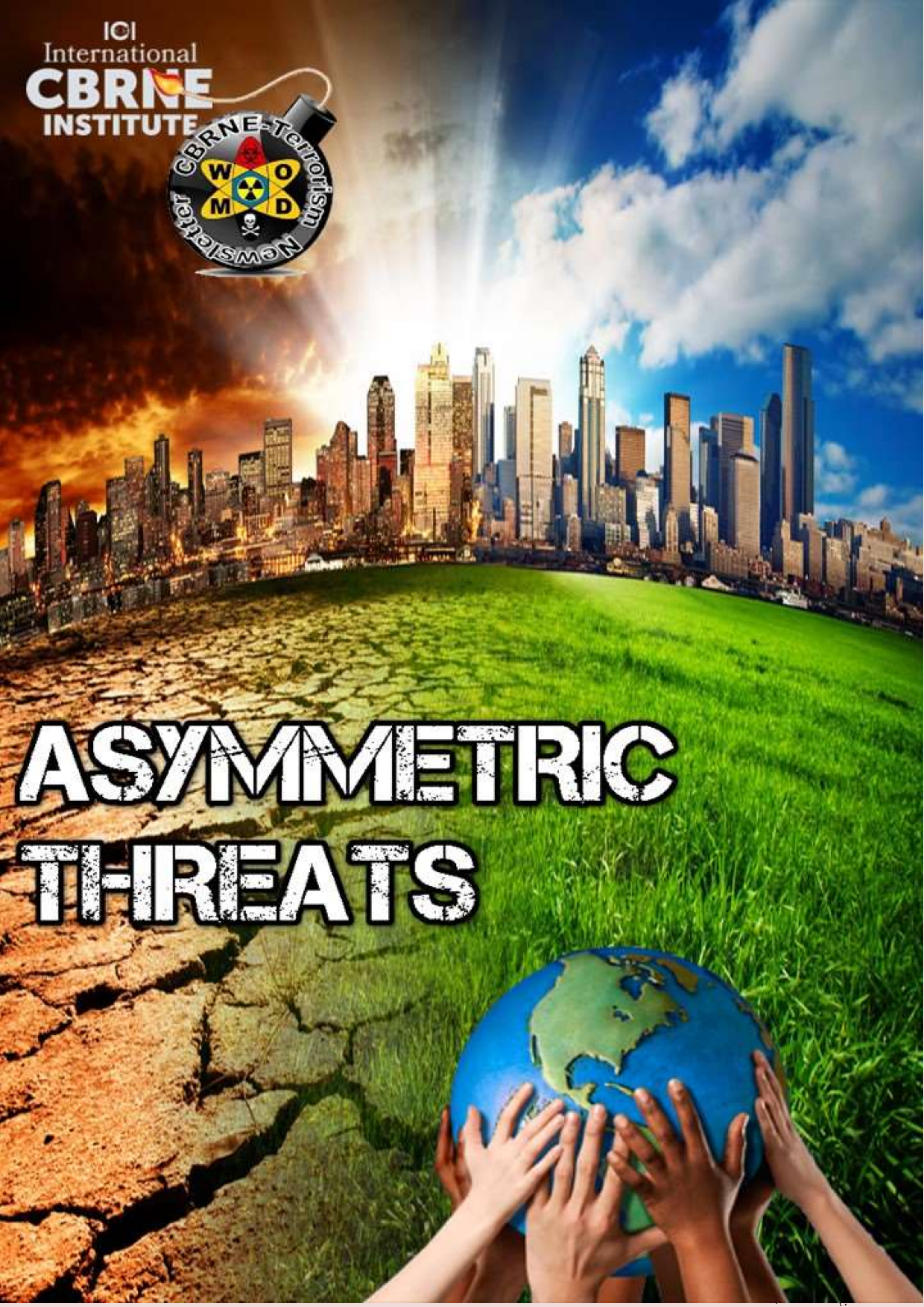
Solar panels often overheat, go offline, or require maintenance due to excess dust, scratches or mechanical deficiencies. It's time-consuming and unreliable to inspect them from the ground. Thermal Live Map can inspect solar farms from the sky in minutes — not days — allowing operators to isolate and measure potential problem areas while the drone is in flight.

Before drones, building and roof inspections were extremely dangerous, time-consuming, and took a physical toll on workers. Thermal Live Map pinpoints cracks, leaks, and structural damage within minutes and minimizes safety risks.

The technology also helps growers spot field stress in real time. They identify irrigation issues, detect ripeness, and analyze plant health early to solve problem areas and avoid lost harvests.



"WE LOST SOME SHINGLES, A TREE and THERE'S A TV REPORTER WHO WAS BLOWN UP ONTO THE ROOF."



ASYMMETRIC THREATS

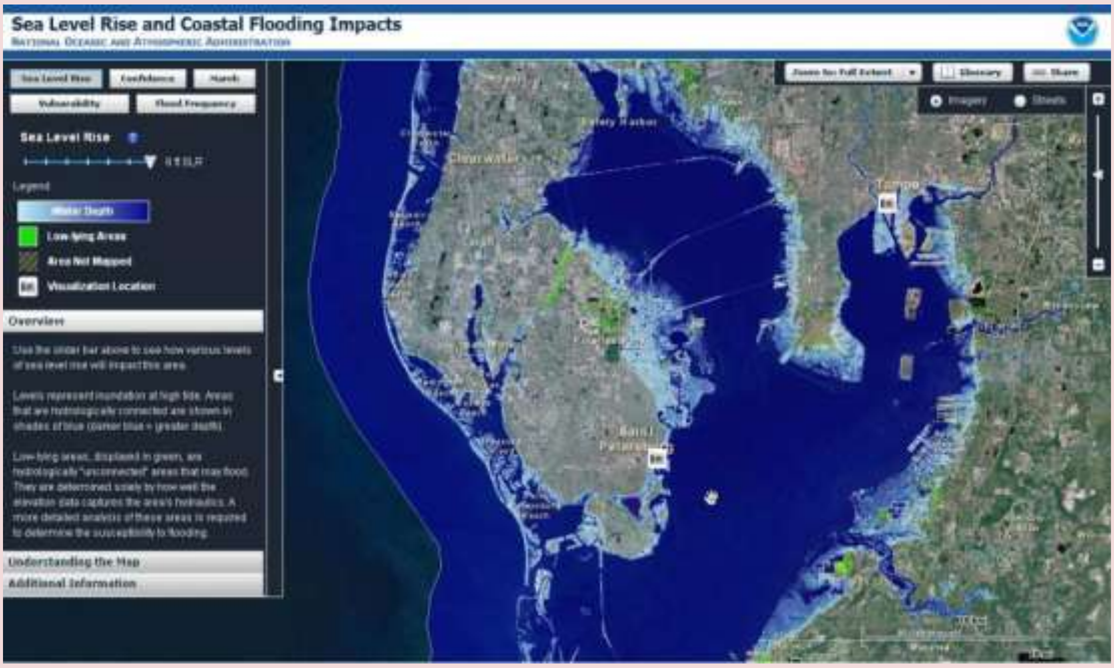
As coastal communities face more frequent, severe disruptions, costly choices loom

Source: http://www.homelandsecuritynewswire.com/dr20180620-as-coastal-communities-face-more-frequent-severe-disruptions-costly-choices-loom

June 20 – Sea levels are rising. Tides are inching higher. High-tide floods are becoming more frequent and reaching farther inland. And hundreds of U.S. coastal communities will soon face chronic, disruptive flooding that directly affects people's homes, lives, and properties.

Yet property values in most coastal real estate markets do not currently reflect this risk. And most homeowners, communities, and investors are not aware of the financial losses they may soon face.

This analysis looks at what's at risk for U.S. coastal real estate from sea level rise—and the challenges and choices we face now and in the decades to come.



Use the slider bar above to see how various levels of sea level rise will impact this area.

Levels represent inundation at high tide. Areas that are hydrologically connected are shown in shades of blue (darker blue = greater depth).

Low-lying areas, displayed in green, are hydrologically "unconnected" areas that may flood. They are determined solely by how well the elevation data captures the area's hydraulics. A more detailed analysis of these areas is required to determine the susceptibility to flooding.

A threshold of disruption

A new report — Underwater: Rising Seas, Chronic Floods, and the Implications for US Coastal Real Estate – from the Union of Concerned Scientists (UCS), notes that long before rising seas permanently submerge properties, millions of Americans living in coastal communities will face more frequent and disruptive high-tide flooding. As this flooding increases, it will reach a threshold where normal routines become impossible and coastal residents, communities, and businesses are forced to make difficult, often costly choices.

For this analysis, that threshold is defined as flooding that occurs 26 times per year (on average, once every other week) or more, a level of disruption referred to as chronic inundation. It is important to note that this flooding is not caused by storms—it is simply the result of high tides rising higher, and reaching farther inland, as sea levels rise.

The results identify the number of residential and commercial properties at risk of chronic inundation—and the total current property value, estimated population, and property tax base affected—for the entire coastline of the lower 48 states.

Billions of dollars of property at risk

The analysis finds that:

- More than 300,000 of today's coastal homes, with a collective market value of about $117.5 billion today, are at risk of chronic inundation in 2045—a timeframe that falls within the lifespan of a 30-year mortgage issued today. Approximately 14,000 coastal commercial properties, currently assessed at a value of roughly $18.5 billion, are also at risk during that timeframe.

- By the end of the century, homes and commercial properties currently worth more than $1 trillion could be at risk. This includes as many as 2.4 million homes—the rough equivalent of all the homes in Los Angeles and Houston combined—that are collectively valued today at approximately $912 billion.
- The properties at risk by 2045 currently house 550,000 people and contribute nearly $1.5 billion toward today's property tax base. Those numbers jump to about 4.7 million people and $12 billion by 2100.
- States with the most homes at risk by the end of the century are Florida, with about 1 million homes (more than 10 percent of the state's current residential properties); New Jersey, with 250,000 homes; and New York with 143,000 homes.

These results reflect a high sea level rise scenario—an appropriately conservative projection to use when estimating risk to homes, which are often the owner's single biggest asset. Even with a more moderate (intermediate) rate of sea level rise, nearly 140,000 homes are still at risk of chronic inundation by 2035 and more than 1.2 million by 2100. (See below for more information about the sea level rise scenarios used in this analysis.)

It is also important to note that these results do not include future development or new homes, nor do they include critical infrastructure such as roads, bridges, power plants, airports, ports, public buildings, and military bases. When all of these are taken together, the effects of chronic flooding could have staggering economic impacts.

The growing risks to homeowners, communities, and the economy

The challenges and choices that come with rising seas are profound and have significant implications for coastal residents, communities, and the broader economy.

Homeowners and commercial property owners are at risk of steep financial losses if their properties flood regularly. Declining property values could erode the tax base for communities, jeopardizing funding for vital local services and infrastructure, such as roads, schools, and police and fire departments.

Mortgages on homes that could become chronically flooded during the term of the loan are inherently riskier. As flooding becomes more frequent, the value of flooded homes will decline and many homeowners could find themselves with mortgages that exceed the value of their homes, or with homes that are increasingly difficult to insure or have even deteriorated to the point of being unlivable. With no obvious option for reversing that trend, some might choose to abandon their homes and allow banks to foreclose on their mortgages. Banks holding these risky mortgages on devalued properties could then find their financial position adversely affected.

Mortgage-backed securities and bonds tied into these riskier coastal real estate mortgages will be at risk of losing value. Real estate developers and investors as well are at risk of losing money invested in properties that become chronically flooded.

Once market risk perceptions catch up with reality, the potential drop in coastal property values could have broad reverberations—affecting banks, insurers, investors, developers, and taxpayers—and potentially trigger regional housing market crises as well as affect the broader national economy.

A national imperative for action

UCS says that given the enormity of the risks from sea level rise, communities, states, businesses, and the federal government all need to take action to prepare.

A crucial first step is for communities, policymakers, and the financial sector to know the risks and amount of time they have available for a robust response.

The nation must also implement policies that reduce the carbon emissions that cause global warming, including investments in clean energy solutions; re-orient policy and market incentives to better reflect the risks of sea level rise and build coastal resilience while also ensuring that resources are targeted to low-income and otherwise disadvantaged communities; and adopt bold, transformative policies that foster new frontiers of opportunity on safer ground for those who may have to retreat from high-risk areas.

The risks of rising seas are profound. Many of the challenges they bring are inevitable. And our time to act is running out. There is no simple solution—but we do still have opportunities to limit the harms. Whether we react to this threat by implementing science-based, coordinated, and equitable solutions—or walk, eyes open, toward a crisis—is up to us right now.

About the analysis

To determine the number of coastal properties at risk from this level of chronic flooding, the analysis uses property data from the online real estate company Zillow combined with the findings of the 2017 analysis, When Rising Seas Hit Home: Hard Choices Ahead for Hundreds of US Coastal Communities, which uses a peer-reviewed methodology to assess areas at risk of chronic inundation.

Three sea level rise scenarios, developed by the National Oceanic and Atmospheric Administration (NOAA) and localized for this analysis, are included:

- A **high scenario** that assumes a continued rise in global carbon emissions and an increasing loss of land ice; global average sea level is projected to rise about 2 feet by 2045 and about 6.5 feet by 2100.
- An **intermediate scenario** that assumes global carbon emissions rise through the middle of the century then begin to decline, and ice sheets melt at rates in line with historical observations; global average sea level is projected to rise about 1 foot by 2035 and about 4 feet by 2100.
- A **low scenario** that assumes nations successfully limit global warming to less than 2 degrees Celsius (the goal set by the Paris Climate Agreement) and ice loss is limited; global average sea level is projected to rise about 1.6 feet by 2100.

— Read more in Underwater: Rising Seas, Chronic Floods, and the Implications for US Coastal Real Estate (Union of Concerned Scientists, June 2018)

How will people move as climate changes?

Source: http://www.homelandsecuritynewswire.com/dr20180620-how-will-people-move-as-climate-changes

June 20 – In coming decades, climate change is expected to displace millions of people through sea level rise, crop failures, more frequent extreme weather and other impacts. But scientists are still struggling to accurately predict how many climate migrants there will be, and where they are likely to go. A new study published this week in the journal *Environmental Research Letters* seeks to address these questions by incorporating climate impacts into a universal model of human mobility. The model also seeks to predict the effects migrants might have on the places to which they move.

To demonstrate the efficacy of the new approach, the authors focused on sea-level rise and human migration in Bangladesh. Here, they estimated that more than 2 million people may be displaced from their homes by 2100 because of permanent inundation by rising sea levels alone. The study used a probabilistic model combined with population, geographic and climate data to predict the sources, destinations and flux of potential migrants.

Lead author Kyle F. Davis, a postdoctoral fellow at Columbia University's Earth Institute, said that more than 40 percent of Bangladesh's population is vulnerable to future sea level rise, as so many people live in low-lying areas that are often exposed to extreme natural events. However, he said, "sea-level rise is a very different type of migration driver from short-lived natural hazards, in that it will make certain areas permanently uninhabitable."

The team's results showed that mean predicted sea-level rise will cause population displacements in 33 percent of Bangladesh's districts–53 percent under more intensive scenarios. By mid-century, they estimated, nearly 900,000 people are likely to migrate because of direct inundation from mean sea level alone. Under the most extreme scenario, of up to 2 meters of mean sea-level rise, the number of migrants driven by direct inundation could rise to as many as 2.1 million people by the year 2100. For all scenarios, five districts – Barisal, Chandpur, Munshiganj, Narayanganj, and Shariatpur – would be the source for 59 percent of all migrants. The analysis considered mean sea-level rise without normal high tides, so the results, both in terms of inundated area and displaced population, are conservative.

The researchers also estimated the extra jobs, housing and food needed to accommodate these migrants at their destinations. They found that to cope with the numbers likely to be displaced by 2050, 600,000 additional jobs, 200,000 residences and 784 billion food calories will be needed.

These results have clear implications for migrant destinations, said Davis. "Migrants are unlikely to search far for an attractive place to move to, and the destination will generally be a trade-off between employment opportunities, distance from the migrants' origin, and how vulnerable it is to sea-level rise itself," he said.

Davis said that the already huge and crowded capital city of Dhaka is consistently favored, coming out as the top destination in all scenarios. This means the city will need to prepare. Dhaka's population has already rapidly expanded in recent years; with at least 18 million people in its wider metropolitan area, it is one of the most densely populated cities on earth.

Davis said inundation and the out-migration it causes will also have significant effects on both agriculture and aquaculture. Some 1,000 square kilometers of Bangladesh's cultivated land could be underwater by the end of the century, with a much larger area made unusable by saltwater intrusion. Given that 48 percent of the labor force works in agriculture, the impact of this would be keenly felt. Similarly, much of the country's coastal aquaculture is vulnerable to climate change, and this will probably have powerful nutritional and economic consequences. Nearly 60 percent of the animal protein in the Bangladeshi diet comes from seafood, and the country is the world's fifth largest aquaculture producer.

"Ultimately, we hope that the modelling tool we have developed can be used by researchers and planners to accurately predict the relocation of climate-induced migrants, and to enable the development of political and economic strategies to face the challenge," said Davis.

The other authors of the study are Abinash Bhattachan of North Carolina State University; Paolo D'Odorico of the University of California, Berkeley; and Samir Suweis of the University of Padova, Italy.

— Read more in Kyle Frankel Davis et al., "A universal model for predicting human migration under climate change: examining future sea level rise in Bangladesh," Environmental Research Letters 13, no. 6 (12 June 2018).

Climate change will soon hit billions of people, and many cities are taking action

Source: http://www.homelandsecuritynewswire.com/dr20180621-climate-change-will-soon-hit-billions-of-people-and-many-cities-are-taking-action

June 21 – By mid-century, billions of people in thousands of cities around the world will be at risk from climate-related heat waves, droughts, flooding, food shortages and energy blackouts, but many cities are already taking action to blunt such effects, says a new report from a consortium of international organizations.

The report, called The Future We Don't Want, estimates that by 2050,

- 1.6 billion people living in more than 970 cities will be regularly exposed to extreme high temperatures.
- Over 800 million living in 570 cities will be vulnerable to sea-level rise and coastal flooding.
- 650 million, in over 500 cities, will be at risk of water shortages.
- 2.5 billion people will be living in over 1,600 cities where national food supplies will be threatened.
- The power supply to 470 million people, in over 230 cities, will be vulnerable to sea-level rise.
- 215 million poor urban residents living in slum areas in over 490 cities will face disproportionate climate risks.

The report was assembled by C40 Cities, a group of big cities working to face climate change; the Global Covenant of Mayors for Climate & Energy, which has signatories in thousands of cities representing some 700 million people; the Urban Climate Change Research Network (UCCRN), a global consortium of institutions and experts based at Columbia University's Earth Institute; and the U.K.-based consultant group Acclimatise. It was presented this week at the Adaptation Futures conference in Cape Town, South Africa, where representatives of cities around the world are sharing ideas on how to become more resilient to changing climate.

"For decades, scientists have been warning of the risks that climate change will pose. Now we have the clearest possible evidence of just what these impacts will mean for [the] world's cities," said Mark Watts, executive director of C40 Cities. "Our research should serve as a wake-up call."

The report features steps that major urban areas already taking to adapt. Cynthia Rosenzweig, co-chair of the UCCRN and head of the climate impacts group at Columbia's Center for Climate Systems Research, said that if such efforts are scaled up and widely adopted, they would stem some of the worst effects.

Some of the efforts covered by the report include:

- To battle extreme heat, Seoul has planted 16 million trees and expanded its green space by 3 square kilometers. The city has also set up shaded cooling centers for those unable to access air conditioning.
- New York City is improving coastal flood mapping, strengthening large-scale coastal defenses and building smaller, strategically placed local storm surge barriers around the city.
- São Paulo has set up reward schemes to encourage citizens to use less water, while investing in the city's pipeline system to reduce water leakage.
- Paris plans to establish more than 80 acres of urban agriculture within the city's boundaries by 2020. By 2050, 25 percent of the city's food supply will be produced in the metropolitan region.
- London is improving drainage to ensure that key infrastructure can withstand heavy flooding, The city is also encouraging decentralized energy supplies to reduce the risk of widespread blackouts if any one power source is damaged.
- Lima has created a poverty map of the city to help policy makers focus resources on the most vulnerable and under-served areas, where people are most exposed to extreme heat.

Many of the solutions being tried out by cities, as well as regional governments, investors and businesses, will be showcased at the Global Climate Action Summit, in San Francisco, 12-14 September 2018.

Transboundary River Basins and Political Tensions," Sustainable Security (13