2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

February 2020

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

DIRTY R-NEWS

Khushab Production Capacity

Source: https://www.globalsecurity.org/wmd/world/pakistan/khushab-production.htm

Pakistan appears poised to bring yet another Plutonium production reactor online in 2020, marking a significant increase in their bomb-making potential. Pakistan's stockpile of nuclear weapons may already be larger than that of former colonial power United Kingdom. Both have about 200 weapons, more than North Korea [about 100], but fewer than Israel and India [both have about 275 bombs]. While the four reactors at Khushab are well attested, most open source analysis of Pakistan's program makes little or no mention of the new fifth reactor [as of 23 January 2020, Nuclear Threat Initiative and Arms Control Association did not mention the fifth reactor].

Wikipedia reports "A further reactor has been speculated on (Khushab-V). Space-based surveillance has not turned up signs that work has begun yet on any fifth plutonium reactor at Khushab, although construction of major facilities continues." In January 2015 ISIS highlighted that new construction activity was taking place in the southwest corner of Pakistan's Khushab nuclear site, south of reactors 2, 3, and 4. At the time, ISIS speculated that the site could be for another reactor.

Indeed, Google Earth imagery discloses a partially complete reactor, with a configuration generally similar to that of Khushab IV, though with a different orientation. Each of the Khushab reactors has a bank of cooling towers of unique configuration. As is well known, reactor thermal power may be estimated based on the size of these cooling towers [John Pike, Tim Brown and Charles Vick were the first open source analysts to apply this principle, in their work on the Israeli Dimona reactor in the late 1990s]. The devil is in the details, but in round numbers of the area of the fifth reactor cooling towers [about 14 meters by about 90 meters, yielding a surface area of about 1250 meters2] is about the same as that of the fourth reactor [about 11 meters by about 110 meters, yielding a surface area of about 1150 meters2]. Both are about twice the size of the early reactors [about 500 meters2]. So, the power of Khushab V is probably about the same as that of Khushab IV, about 90 megawatts-thermal (MWth).

All of the new facilities aimed to support Pakistan's production of plutonium and none of them are safeguarded by the IAEA. The capabilities of the new reactors, initially believed to be about 70-130 MWT, combined could allow Pakistan to produce enough plutonium to manufacture more than 12 nuclear weapons a year. Other estimates suggested that Pakistan's production levels allow for roughly 7-14 nuclear weapons per year. But with all four plants operational, nuclear weapons could be produced at a rate of as many as 19-26 weapons per year, nearly twice the previous rate.

On 23 May 2018, Albright et al reported "the latest reactor built in 2011, Khushab 4, appears to have significantly greater power than the other three reactors, up to 90 megawatts-thermal (MWth). Khushab 1 is estimated to have a power of 30-40 MWth; and Khushab 2 and 3 reactors are estimated to have a power of 40-50 MWth. The uncertainty in these estimate makes these findings preliminary, but overall represent a lowering of our previous power estimates of these reactors."

These are small reactors by international standards. In the United States, the Hanford B Reactor initial power was 250 MWth. The French G-2 Reactors were 250 MWth each. But in North Korea, the Yongbyon reactor has a power of 10-20 MWth, and the Arak reactor in Iran is about 40 MWth.

The "plutonium conversion factor (PF)" translates the energy produced by the reactor into the amount of weapon-grade plutonium discharged. It is expressed in units of grams of weapon-grade plutonium per energy produced, g/MWth-d). For the production of weapon-grade plutonium in the Khushab reactors, values of about 0.95-0.97g/MWth-d are used by ISIS, which believed each reactor to have a relatively low average capacity factor of about 40-50 percent [i.e., operating a little

less than half time]. Typical capacity factors range from 0.5 or 50 percent, to 0.7, or 70 percent.
Typically, 10MWth of reactor power, operating at half time, would produce about 1.6 kg of plutonium per year. A sophisticated implosion weapon might require 2 to 4 kg of plutonium. So, in round numbers, 20MWth of half-time reactor power yields one bomb per year.

reactor	K-1	K-2	K-3	K-4	K-5	annual	total	bombs
MWt	35	45	45	90	90	Pu kg	Pu kg	@ 3 kg
IOC	1998	2010	2013	2015	2020			
1998	5.6					6	6	2
1999	5.6					6	11	4
2000	5.6					6	17	6
2001	5.6					6	22	7
2002	5.6					6	28	9
2003	5.6					6	34	11
2004	5.6					6	39	13
2005	5.6					6	45	15
2006	5.6					6	50	17
2007	5.6					6	56	19
2008	5.6					6	62	21
2009	5.6					6	67	22
2010	5.6	7.2				13	80	27
2011	5.6	7.2				13	93	31
2012	5.6	7.2				13	106	35
2013	5.6	7.2	7.2			20	126	42
2014	5.6	7.2	7.2			20	146	49
2015	5.6	7.2	7.2	14.4		34	180	60
2016	5.6	7.2	7.2	14.4		34	214	71
2017	5.6	7.2	7.2	14.4		34	249	83
2018	5.6	7.2	7.2	14.4		34	283	94
2019	5.6	7.2	7.2	14.4		34	318	106
2020	5.6	7.2	7.2	14.4	14.4	49	366	122
2021	5.6	7.2	7.2	14.4	14.4	49	415	138
2022	5.6	7.2	7.2	14.4	14.4	49	464	155
2023	5.6	7.2	7.2	14.4	14.4	49	513	171
2024	5.6	7.2	7.2	14.4	14.4	49	562	187
2025	5.6	7.2	7.2	14.4	14.4	49	610	203

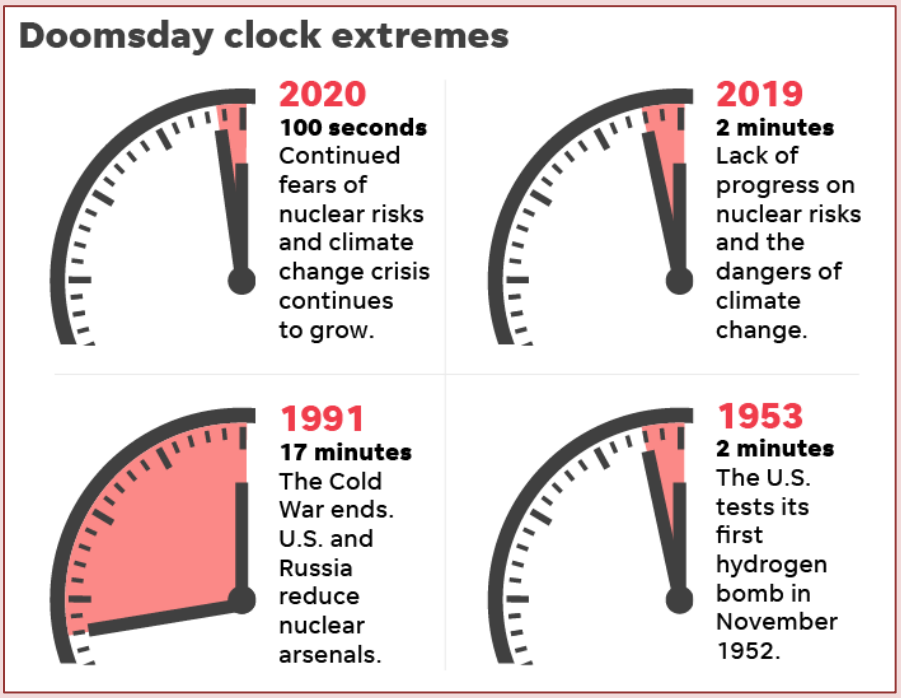
It Is Now 100 Seconds to Midnight

Source: http://www.homelandsecuritynewswire.com/dr20200124-it-is-now-100-seconds-to-midnight

Jan 24 – The iconic Doomsday Clock of the *Bulletin of the Atomic Scientists*, symbolizing the gravest perils facing humankind, is now closer to midnight than at any point since its creation in 1947. To underscore the need for action, the time on the Doomsday Clock is now being expressed in seconds, rather than minutes: On Thursday, the *Bulletin*'s Science and

Security Board, in consultation with the *Bulletin*'s Board of Sponsors, which includes thirteen Nobel Laureates, moved the Doomsday Clock from two minutes to midnight to 100 seconds to midnight.

As the statement issued Thursday by the *Bulletin* explains: "Humanity continues to face two simultaneous existential dangers—nuclear war and climate change—that are compounded by a threat multiplier, cyber-enabled information warfare, that undercuts society's ability to respond. The international security situation is dire, not just because these threats exist, but because world leaders have allowed the international political infrastructure for managing them to erode."



The *Bulletin* notes that the Doomsday Clock has now moved closer to midnight in three of the last four years. While the Doomsday Clock did not move in 2019, its minute hand was set forward in 2018 by 30 seconds, to two minutes before midnight. The Clock was adjusted in 2017 to two and a half minutes to midnight from its previous setting of three minutes to midnight.

Rachel Bronson, president and CEO of the *Bulletin*, said: "It is 100 seconds to midnight. We are now expressing how close the world is to catastrophe in seconds – not hours, or even minutes. It is the closest to Doomsday we have ever been in the history of the Doomsday Clock. We now face a true emergency – an absolutely unacceptable state of world affairs that has eliminated any margin for error or further delay."

Former California Governor Jerry Brown, executive chairman of the *Bulletin*, said: "Dangerous rivalry and hostility among the superpowers increases the likelihood of nuclear blunder. Climate change just compounds the crisis. If there's ever a time to wake up, it's now."

For the first time, experts from the *Bulletin of the Atomic Scientists* were joined in making the Doomsday Clock change by members of The Elders. Founded by Nelson Mandela in 2007, The Elders are independent global leaders working together for peace and human rights.

Former UN Secretary-General Ban Ki-moon, deputy chairman of The Elders; and former South Korean Foreign Minister, said: "We share a common concern over the failure of the multilateral system to address the existential threats we face. From the US withdrawal from the Paris Agreement and the Iran Nuclear Deal, to deadlock at nuclear disarmament talks and division at the UN Security Council – our mechanisms for collaboration are being undermined when we need them most."

Former President of Ireland Mary Robinson, chairperson of The Elders, and former UN High Commissioner for Human Rights, said: "We ask world leaders to join us in 2020 as we work to pull humanity back from the brink. The Doomsday Clock now stands at 100 seconds to midnight, the most dangerous situation that humanity has ever faced. Now is the time to come together – to unite and to act."

The Doomsday Clock statement highlights three worsening factors:

Nuclear weapons: "In the nuclear realm, national leaders have ended or undermined several major arms control treaties and negotiations during the last year, creating an environment conducive to a renewed nuclear arms race, to the proliferation of nuclear weapons, and to lowered barriers to nuclear war. Political conflicts regarding nuclear programs in Iran and North Korea remain unresolved and are, if anything, worsening. US-Russia cooperation on arms control and disarmament is all but nonexistent."

Climate change. "Public awareness of the climate crisis grew over the course of 2019, largely because of mass protests by young people around the world. Just the same, governmental action on climate change still falls far short of meeting the challenge at hand. At UN climate meetings last year, national delegates made fine speeches but put forward few concrete plans to further limit the carbon dioxide emissions that are disrupting Earth's climate. This limited political response came during a year when the effects of manmade climate change were manifested by one of the warmest years on record, extensive wildfires, and quicker-than-expected melting of glacial ice."

Cyber-based disinformation. "Continued corruption of the information ecosphere on which democracy and public decision making depend has heightened the nuclear and climate threats. In the last year, many governments used cyber-enabled disinformation campaigns

to sow distrust in institutions and among nations, undermining domestic and international efforts to foster peace and protect the planet."

At the same time, the Doomsday Clock statement also identifies possible action steps to turn back the hands of the Clock.

- U.S. and Russian leaders can return to the negotiating table to: reinstate the INF Treaty or take other action to restrain an unnecessary arms race in medium-range missiles; extend the limits of New START beyond 2021; seek further reductions in nuclear arms; discuss a lowering of the alert status of the nuclear arsenals of both countries; limit nuclear modernization programs that threaten to create a new nuclear arms race; and start talks on cyber warfare, missile defenses, the militarization of space, hypersonic technology, and the elimination of battlefield nuclear weapons.
- The countries of the world should publicly rededicate themselves to the temperature goal of the Paris climate agreement, which is restricting warming "well below" 2 degrees Celsius higher than the preindustrial level. That goal is consistent with consensus views on climate science, and, notwithstanding the inadequate climate action to date, it may well remain within reach if major changes in the worldwide energy system and land use are undertaken promptly. If that goal is to be attained, industrialized countries will need to curb emissions rapidly, going beyond their initial, inadequate pledges and supporting developing countries so they can leapfrog the entrenched, fossil fuel-intensive patterns previously pursued by industrialized countries.
- The United States and other signatories of the Iran nuclear deal can work together to restrain nuclear proliferation in the Middle East. Iran is poised to violate key thresholds of the deal.
- The international community should begin multilateral discussions aimed at establishing norms of behavior, both domestic and international, that discourage and penalize the misuse of science. Science provides the world's searchlight in times of fog and confusion. Furthermore, focused attention is needed to prevent information technology from undermining public trust in political institutions, in the media, and in the existence of objective reality itself. Cyber-enabled information warfare is a threat to the common good. Deception campaigns—and leaders' intent on blurring the line between fact and politically motivated fantasy—are a profound threat to effective democracies, reducing their ability to address nuclear weapons, climate change, and other existential dangers.

December 2020 marks the 75th anniversary of the first edition of the *Bulletin of the Atomic Scientists*, initially a six-page, black-and-white bulletin and later a magazine, created in anticipation that the atom bomb would be "only the first of many dangerous presents from the Pandora's Box of modern science."

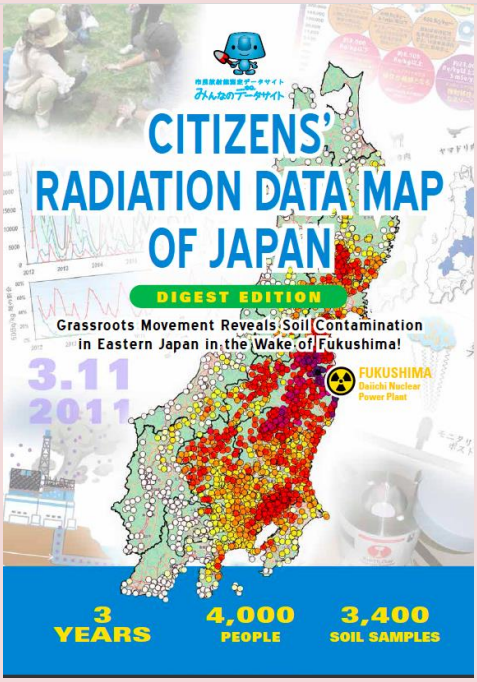
Environment, health and safety concerns towards Tokyo 2020 Olympic Games

Source: https://en.wikipedia.org/wiki/Concerns_and_controversies_at_the_2020_Summer_Olympics

The Tokyo Organizing Committee of the Olympic and Paralympic Games announced that the Olympics torch relay will begin in Fukushima, and the Olympic baseball and softball matches will be played at Fukushima Azuma Baseball Stadium, 55 miles (89 km) from the site of the Fukushima Daiichi nuclear disaster, despite the fact that the scientific studies on the safety of Fukushima are currently in dispute.[22][23] In relation to the 2011 Tōhoku earthquake and tsunami, which resulted in multiple nuclear meltdowns and an official Level 7 disaster, officials from the World Health Organization (WHO) and the United Nations have determined that the risks of dangerous radiation exposure are minimal.[24] Nevertheless, some scientists and citizens remain skeptical.[25][26][27]

For example, Tilman Ruff, a public health expert and a co-founder of the Nobel Peace Prize-winning International Campaign to Abolish Nuclear Weapons (ICAN), urged the Australian Olympic Committee to properly inform its staff and athletes attending the 2020 Tokyo Games about the ongoing health effects of the Fukushima radiation.[28]

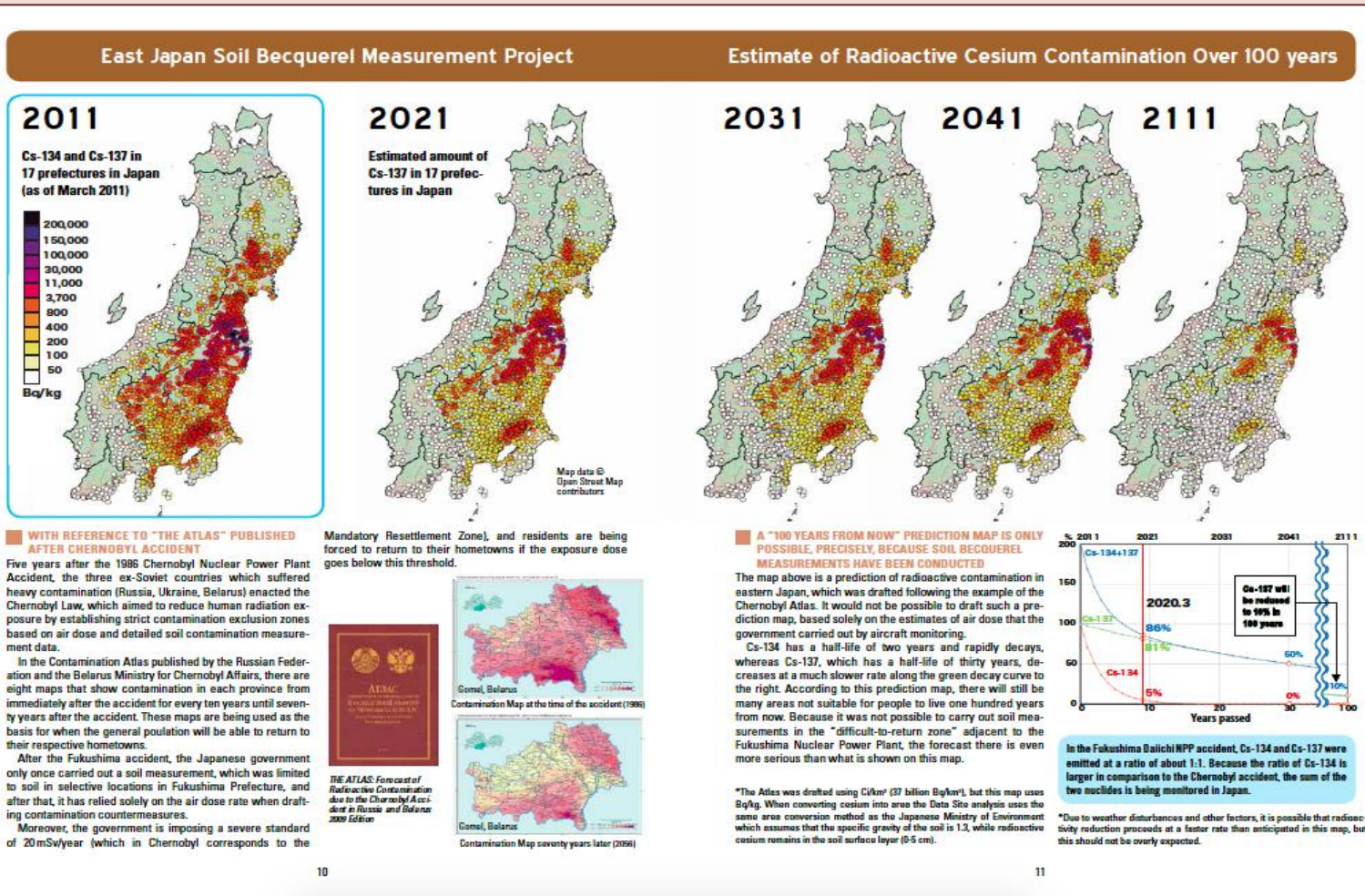
Former nuclear industry executive and whistle blower Arnold Gundersen and his institute, Fairewinds Associates, tested for the presence of radioactive dust on land scheduled to be used for certain events, including baseball, softball and the Olympic torch relay.[29] At these facilities, the legally allowable radiation levels are higher than at other athletic facilities.[30] According to certain models, such as the National Academy of Sciences' "linear, no-threshold" model, small increases in radiation exposure may cause proportional health risks.[31] The Japanese government posted that measured radiation levels in the city of Fukushima are comparable with safe readings in Hong Kong and Seoul, while Tokyo's readings are even lower, in line with Paris and London.[32] However, the data collected by the monitoring posts installed by the Japanese governments are partial and non-representative of the extent of radioactive contamination, as they measure only the atmospheric radiation levels in the form of gamma rays, but not radionuclides, such as cesium-137, which emit alpha and beta particles that are dangerous when inhaled or ingested.[32] It is also pointed out that the government-installed monitoring posts are placed strategically and the areas surrounding the posts were cleaned so that the radiation levels remain lower.[32] Greenpeace reported that the radiation levels measured around the J-Village sports camp in Fukushima, where the Tokyo 2020 Olympic torch relay will begin,



were 1,700 times higher than before the Fukushima Daiichi nuclear disaster.[33][34][35] Even though the Japanese government promised to keep the radiation levels below 0.23 μSv per hour, radiation hot spots at the J-Village showed readings as high as 1.7 μSv per hour at 1 metre (3 ft 3 in) above the surface and over 71 μSv per hour at the surface level.[33][34][35]

Additionally, food from the region, currently under import restrictions in 23 countries,[36] is tested intensively for safety.[37] In October 2019, after tons of poorly-secured radioactive Fukushima waste were swept away by typhoon Hagibis,[38] IOC chief Thomas Bach promised to carry out inspections on radiation safety.[39]

In November 2019, a Japanese citizens' group *Minna-No Data Site* (Everyone's Data Site) published an English version of *Citizens' Radiation Data Map of Japan*, a 16-page booklet featuring radiation-level maps, created using soil samples from 3,400 sites in 17 prefectures in eastern Japan, the results of three-year land contamination surveys with approximately 4,000 volunteers.



RadEye GF-10 Simulator

Source: https://www.argonelectronics.com/radeye-gf-10-sim

Thanks to a combination of Argon's wealth of simulation experience and our relationship with ThermoFisher, the look, feel and response of the RadEye series of training simulators is extremely close to that of actual detectors.
RadEye SIM responds to Radsim electromagnetic sources that safely simulate ionizing radiation eliminating regulatory, environmental, and health and safety concerns for you and your students. You can use the simulation sources in the open or within buildings.
Key simulation features of the RadEye GF-10 Simulator are:

- Inverse square law (1/r2) response within real detector tolerance.
- Simulation of user body shielding for source location.
- Realistic representation of different shielding effects.
- Selectable units of measurement (Sv/hr, Rem, CPS).
- Same human interface as real RadEye.
- Configurable menu settings.
- Dose and dose rate alarm settings.
- Language selection.
- Same commercial batteries as real detector (80 hours operation).
- No regular calibration.
- No preventative maintenance.

RadEye simulators are compatible with PlumeSIM, Argon's proven Live Field and Tabletop CBRN exercise system. In use by many of the world's leading training facilities, PlumeSIM enables real time instrumented wide area tactical field and nuclear / HazMat / Chemical Warfare emergency response exercises to be conducted using single or multiple simulation device types that respond in the real time to simulated hazards.

UAE's nuclear plant 'ready' to begin operations

Source: https://www.thenational.ae/uae/uae-s-nuclear-plant-ready-to-begin-operations-1.970946

Workers from Barakah nuclear power plant mark 75 million 'safe working hours' last week. Courtesy: Emirates Nuclear Energy Corporation

Jan 28 – The UAE is ready to start operating its nuclear power plant's first reactor, Emirates Nuclear Energy Corporation said on Tuesday.
Nawah Energy Company, the operator and subsidiary of Enec, said tests by an independent body concluded that **Unit 1 of Barakah, in the Abu Dhabi desert, is ready to generate energy.**

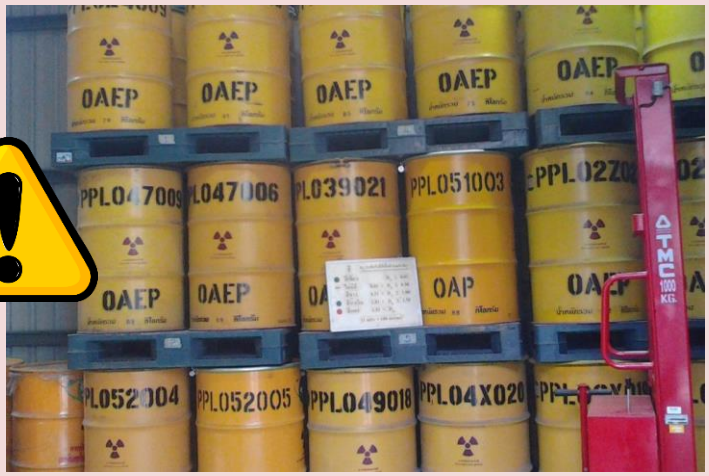
A team of nuclear industry experts from the Atlanta Centre of the World Association of Nuclear Operators assessed the plant in November. Experts reviewed performance, maintenance, and emergency preparedness.
Mohamed Al Hammadi, chief executive of Enec, called the results a "major milestone" for the programme.

"It provides international recognition that our plant, people and processes meet international start up standards," he said.
Mr Al Hammadi said Nawah would continue to work with the Federal Authority for Nuclear Regulation to get approvals and "gradually commence producing clean, safe and reliable electricity to power the growth of the UAE for the next 60 years".
Barakah will be the UAE's first nuclear plant and will make the Emirates the first Arab country to produce nuclear energy. With four reactors, it will add 5.6 gigawatts of capacity to the grid when fully operational — providing a quarter of the UAE's electricity needs and reducing the country's carbon emissions by 21 million tonnes each year. Barakah is being built by Korea Electric Power Corporation and is scheduled to begin operation in the first quarter of this year.
The nuclear plant is also part of plans to significantly increase the ratio of clean power in the UAE's energy mix.
The UAE largely depends on gas and oil to meet its power requirements and, in 2012, got 98 per cent of its energy from hydrocarbons. It aims to cut this down to 76 per cent by next year and for half of its energy to come from renewable sources by 2050.
The country began construction of its South Korean-designed nuclear power plants in 2013, with four reactors each designed with a capacity of 1.4GW.
To begin generating power, the reactors are loaded with uranium pellets, which generate heat through a controlled nuclear reaction. This heat is transferred to water, which creates steam to drive the turbines.
The UAE signed a "123 agreement" with the US for the peaceful civilian use of nuclear energy and also has agreements with Argentina, Japan and Russia to co-operate in the atomic power sector.

Stainless steel may not be the best choice for storing nuclear waste

Source: https://newatlas.com/energy/stainless-steel-storing-nuclear-waste/

Jan 28 – A new study by researchers at Ohio State University suggests that stainless steel may not be the best choice for containing high-level nuclear waste. By simulating long-term storage conditions, the team found that the storage materials interact with each other more than previously thought, causing them to degrade faster.



The storage of nuclear waste is more than a perennial political football, it is an existential problem. Whatever one's opinions about nuclear power or weapons, there are thousands of tons of nuclear waste temporarily stored around the world, meaning that a way must be found to store it all safely in the long term.
The most important type of nuclear waste is the high-level waste left over from reprocessing nuclear fuel or from nuclear weapon production. Such waste is made up of a complex mixture of radioactive isotopes with half-lives ranging from years to millennia. Though reactors have been operating all over the world for over 75 years, **only Finland has started to build a permanent storage facility for such very dangerous waste**.
That may show a remarkable lack of political will or even courage, but perhaps this reluctance will turn out to be serendipitous. **That's because the favored way of storing high-level waste is to vitrify it. That is, to mix the isotopes with molten glass or ceramics to form a chemically inert mass that can be sealed in stainless steel canisters before being sealed in an underground storage facility.**
That plan may now have to change if the Ohio study is correct. Led by Xiaolei Guo, the team took glasses and ceramics and put them in close contact with stainless steel in various wet solutions for 30 days in conditions similar to those that would be found in the proposed US Yucca Mountain nuclear waste repository.
"In the real-life scenario, the glass or ceramic waste forms would be in close contact with stainless steel canisters," says Xiaolei. "Under specific conditions, the corrosion of stainless steel will go crazy. It creates a super-aggressive environment that can corrode surrounding materials."
They found that the steel interacted with the glass or ceramic to produce severe and localized corrosion that both damaged the steel and corroded and cracked the glass and ceramics. According to the team, this is because the iron in stainless steel has a chemical affinity with the silicon in glass, accelerating corrosion.
"This indicates that the current models may not be sufficient to keep this waste safely stored," says Xiaolei. "And it shows that we need to develop a new model for storing nuclear waste."

▶▶ The research was published in *Nature Materials*.

The Cost and Composition of America's Nuclear Weapons Arsenal

Source: https://www.visualcapitalist.com/cost-and-composition-of-americas-nuclear-weapons-arsenal/

Jan 29 – The American nuclear weapons arsenal is nowhere near its 1960s peak, but there are still thousands of warheads in the stockpile today.

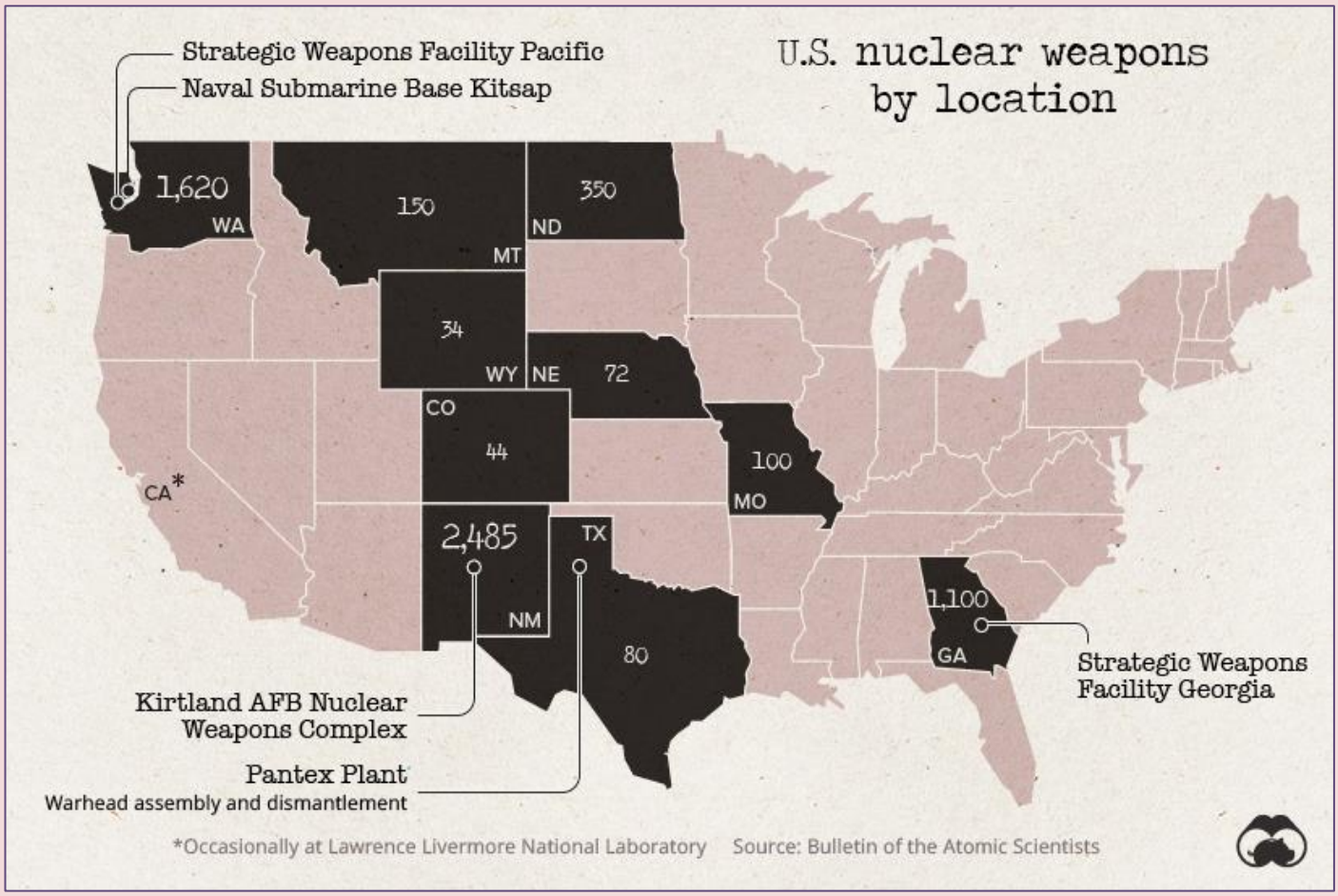
The U.S. nuclear program is comprised of a complex network of facilities and weaponry, and of course the actual warheads themselves. Let's look at the location of warheads, how they're deployed, and the costs associated with running and refurbishing an aging nuclear program.

Let's launch into the data.

Nuclear Weapons Map

As of 2019, the U.S. Department of Defense maintained an estimated stockpile of 3,800 nuclear warheads for delivery by more than 800 ballistic missiles and aircraft. Roughly 1,300 warheads are actually deployed, while most of the remaining inventory is either held in reserve (as a hedge against "technical or geopolitical surprises") or is destined to be dismantled.

These weapons are thought to be stored across 11 U.S. states, with the vast majority residing in New Mexico, Washington, and Georgia.

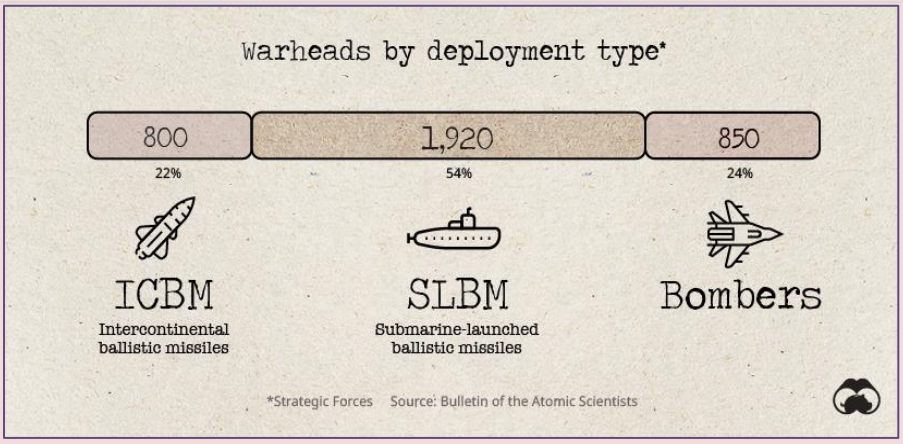


Over 1,500 of the warheads in New Mexico are retired and are destined to be dismantled at the Pantex facility in Texas.

The United States also maintains a small amount of nuclear inventory in and around Europe as well. Turkey's Incirlik Air Base likely holds the biggest supply of warheads outside the U.S., and a few weapons are also located in storage vaults in Belgium, Italy, Germany, and the Netherlands.

Deployment Data

Nuclear warheads, while devastatingly powerful, are nothing without a delivery mechanism. In simple terms, there are three primary methods for actually launching missiles: Silos, bombers, and submarines.



The most common deployment of nuclear weapons is under the sea. The U.S. Navy is thought to operate 14 ballistic missile submarines, with each carrying as many as 24 Trident II missiles.

Missile silos are not as popular as they once were, but the U.S. Air Force still maintains 400 silo-based missiles, and another 50 are kept "warm" in the event of an emergency.

America's Nuclear Weapons Budget

The Congressional Budget Office (CBO) is required to project the 10-year costs of nuclear forces every two years.

Though much of the program is shrouded in secrecy, the budget below provides an overview of the costs of running America's nuclear weapons arsenal.

Projected Costs of Nuclear Forces
in billions

	2019			Total, 2019–2028		
Nuclear delivery systems and weapons	DoD	DOE	Total	DoD	DOE	Total
Strategic nuclear delivery systems and weapons						
Ballistic missile submarines	8.5	1.3	9.8	96	11	107
Intercontinental ballistic missiles	2.6	0.2	2.8	56	5	61
Bombers	3.2	1.2	4.4	38	11	49
Other nuclear activities[b]	1.4	n.a.	1.4	16	n.a.	16
Subtotal	15.8	2.6	18.4	207	27	234
Tactical nuclear delivery systems and weapons	0.2	0.4	0.7	8	8	15
Nuclear weapons laboratories and supporting activities						
Stockpile services	n.a.	2.1	2.1	n.a.	24	24
Facilities and infrastructure	n.a.	3.0	3.0	n.a.	41	41
Other stewardship and support activities[c]	n.a.	3.6	3.6	n.a.	41	41
Subtotal	n.a.	8.7	8.7	n.a.	106	106
Subtotal, Nuclear Delivery Systems and Weapons	16.0	11.8	27.7	214	141	355
Command, control, communications, and early-warning systems						
Command and control	1.4	n.a.	1.4	19	n.a.	19
Communications	2.3	n.a.	2.3	23	n.a.	23
Early warning	2.2	n.a.	2.2	34	n.a.	34
Subtotal, Command, Control, Communications, and Early-Warning Systems	5.8	n.a.	5.8	77	n.a.	77
Total Budgeted Amounts for Nuclear Forces	**21.8**	**11.8**	**33.6**	**291**	**141**	**432**
CBO's Estimates of Additional Costs Based on Historical Cost Growth	n.a.	n.a.	n.a.	35	27	62
Total Estimated Cost of Nuclear Forces	**21.8**	**11.8**	**33.6**	**326**	**168**	**494**

50% weapons
21% infrastructure
16% control & comms
13% overruns

For context, the U.S. budgeted $637B for defense and $1,047B for social security in 2019

Costs in the budget are split between the Department of Energy (DoE) and the Department of Defense (DoD), which handle different parts of the process.

On one hand, the DoD takes care of the delivery systems for warheads. Those submarines, bombers, and missile silos spread around the country will add up to a projected $249 billion in costs over the next decade. Another large portion of the DoD budget accounts for operational aspects of the program, such as funding facilities, control, and early warning systems.

On the other hand, the DoE is responsible for building and maintaining the actual warheads themselves. The U.S. stopped producing new warheads in the 1990s, but all that changed last year.

Back in the Bomb Business

Generally, we think of nuclear weapons stockpiles as a sunsetting resource, slowly being dismantled; however, since the treaty that ended the arms race collapsed in mid-2019, the flood gates may be opening once again.

New warheads are reportedly rolling off the production line, and in the beginning of this year, Lockheed Martin was tapped by the U.S. Navy to manufacture low yield submarine-based nuclear missiles.

The development of lower yield nuclear weapons appears to be a response to efforts by Russia to modernize their arsenal.

With this new weapons development, the U.S. is aiming to create "tailored response options" to any potential conflict. By eliminating the perceived advantages that adversaries may have, the U.S. is hoping to lower the likelihood of a nuclear conflict.

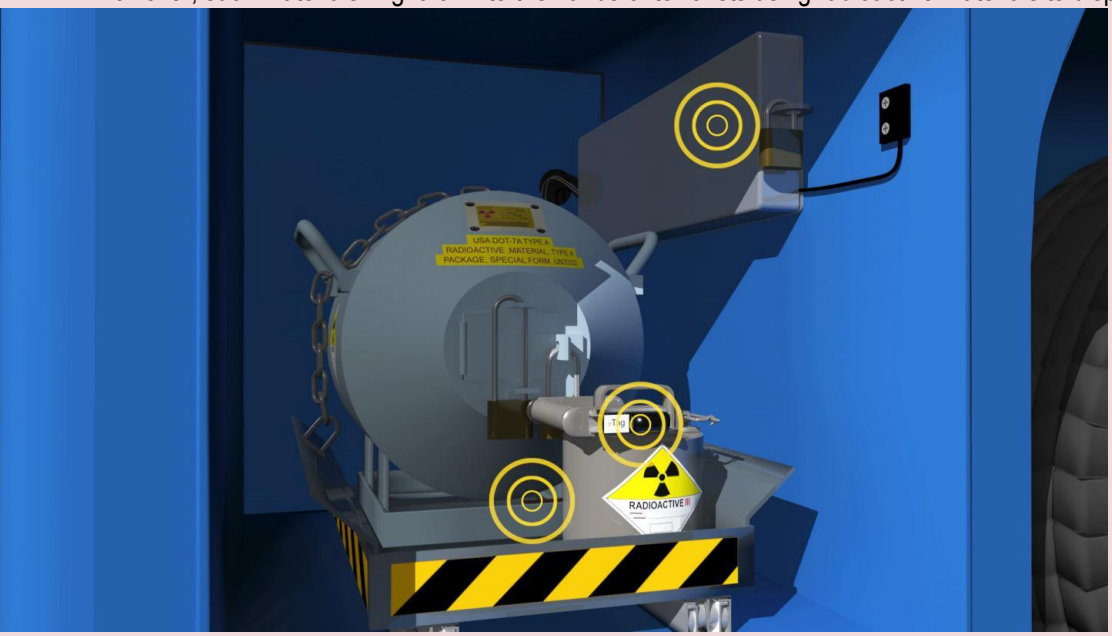
Arms control advocates warn that new lower-yield warheads entering production will lower the threshold for a nuclear conflict.

While advocates and critics of nuclear weapons debate the merits of new weapons, we appear to be entering a new era of weapons proliferation.

First Line of Defense Against Radiological Terrorism

Source: https://i-hls.com/archives/98600

Jan 31 – Radioactive materials are often used by industry for tasks that use radiation to supply information. For example, the radiation can be used to help determine the extent of oil fields or to verify the quality of welding seams at construction or other job sites. However, such materials might fall into the hands of terrorists using radioactive materials to disperse and emit ionizing radiation.



A new system designed to help keep radioactive materials out of the hands of terrorists should soon be available commercially. Developed at the US Department of Energy's Pacific Northwest National Laboratory (PNNL), the technology called Mobile Source Transit Security combines radio frequency tags, global positioning systems, radiation detection and software to keep track of radioactive materials. It also can detect tampering and issue alerts.

The thousands of radioactive sources used by industry worldwide are mostly of limited use for "dirty bombs" with a goal of seriously sickening or killing humans by spewing radiological contamination, according to the US Nuclear Regulatory Commission. However, the solution could form "a first line of defense against radiological terrorism and it provides situational awareness if the material is tampered with or moved from where it is supposed to be," said Brian Higgins, PNNL manager of the project.

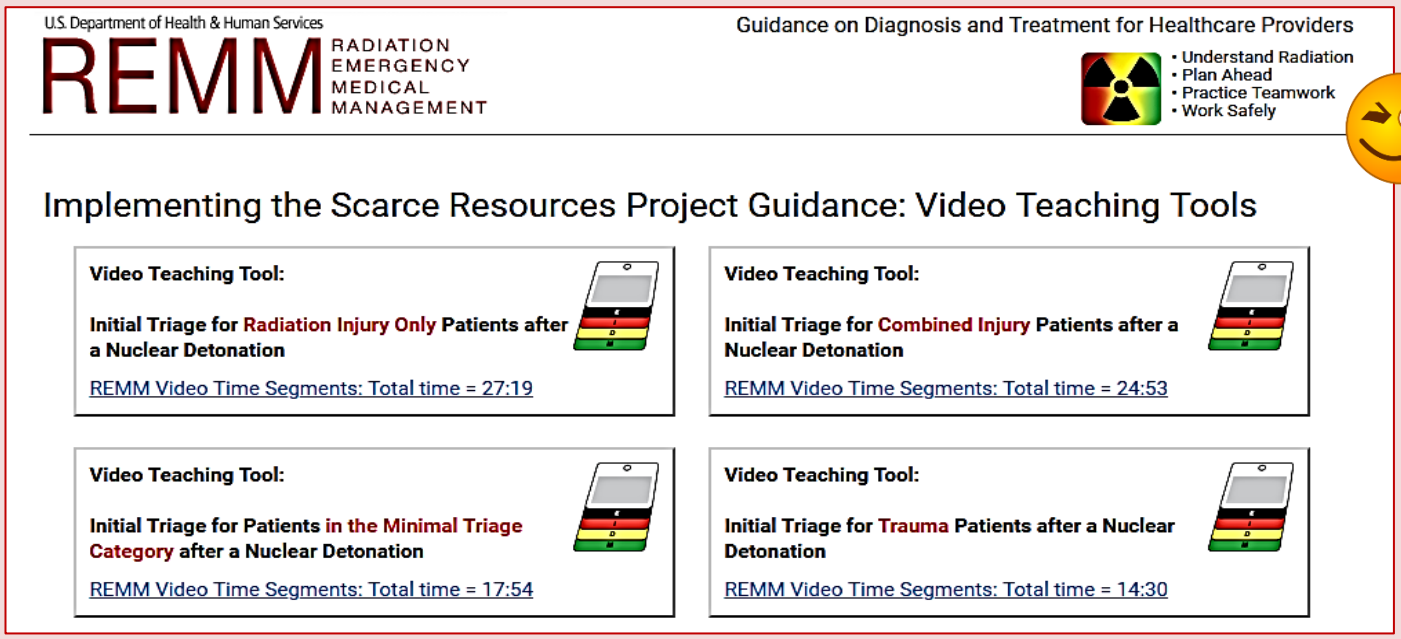
The technology, developed with funding from the National Nuclear Security Administration could be used in industry in the United States or internationally, which would reduce the risk of such material crossing borders to enter the United States. The federal agency already has deployed the technology in a dozen places in the United States, and sales are expected in Latin America first.

Golden Security Services will produce the system and make it available to companies that manage the estimated thousands of radiological sources internationally.

"Technology transfer to industry is an important mission of the laboratory, especially in the area of nuclear security, where the consequences can be severe," said Kannan Krishnaswami, who manages the commercialization of national security technologies for PNNL.

PNNL partnered with Baker Hughes, an international oil field services company, to understand the security issues for radioactive sources security and industries' operational needs.

Oil field mapping is a particular concern because an oil mapping truck can travel several hundred miles from its home base, carrying radiation sources inside casks that shield radiation and help meet U.S. Department of Transportation requirements.
The MSTS sensor technology and software can track the truck and radiation sources and alert officials if the radiation source moves from where it is supposed to be, according to pnnl.gov.



Source: https://www.remm.nlm.gov/triagetool_new_video_tutorials.htm#radiation_only

How Much Radiation-Contaminated Water Will Kill You?

By Natalie Wolchover
Source: https://www.livescience.com/13443-radiation-contaminated-water-kill.html

March 2011 – Radioactive substances are leaching into the water supply near and far from the quake-damaged nuclear reactors in Fukushima, Japan. After an abnormally high level of iodine 131 was detected in the water in Tokyo on March 23, a media frenzy ensued, residents were told not to let their infants drink the city supply, and stores quickly sold out of bottled water.
Are fears of contaminated water justified in Japan? Is the level of contamination actually dangerous?
A 1-sievert (Sv) dose of radiation increases a person's lifetime cancer risk by 4 percent, according to health physicist and radiation safety expert Peter Caracappa of the Renssealaer Polytechnic Institute. To put that in real terms, if 1,000 people are exposed to 1 Sv of radiation, 40 more of them will develop cancer in their lifetimes than would otherwise.
A person would have to ingest 77 million becquerels of radioactive iodine in order to receive a 1 Sv radiation dose, Caracappa told Life's Little Mysteries, a sister site of LiveScience.
At its highest level of contamination (recorded on March 23), Tokyo water contained 210 becquerels of radioactive iodine per liter. A simple calculation shows that a person would have to drink about 370,000 liters (97,000 gallons) of that water to expose himself to 1 Sv of radiation, and thus increase his lifetime cancer risk by 4 percent.
At the recommended rate of eight glasses of water a day, it would take someone about 530 years to consume that much water. Besides the obvious fact that no one lives that long anyway, iodine 131 also radioactively decays within days, so the Tokyo water supply will not remain contaminated for nearly that long. On March 24, a day after the high reading, the radioactive iodine level had already fallen to 79 becquerels per liter.
"My opinion is that we're unlikely to see an increase in cancer deaths as a result of the nuclear accident in Japan, given the information I have access to about the levels of dose that the population is being exposed to," Caracappa said.

__Natalie Wolchover__ was a staff writer for Live Science from 2010 to 2012. She hold a bachelor's degree in physics from Tufts University and has studied physics at the University of California, Berkeley.

New Materials Could Help Clean-Up Chernobyl and Fukushima

Source: http://www.homelandsecuritynewswire.com/dr20200213-new-materials-could-help-cleanup-chernobyl-and-fukushima

Feb 13 – **Materials which could be used to help clean-up the Chernobyl and Fukushima nuclear power stations have been developed by engineers at the University of Sheffield.**

The materials, produced by Dr. Claire Corkhill and her team from the University's Department of Materials Science and Engineering, in collaboration with scientists in Ukraine, can simulate the Lava-like Fuel Containing Materials (LFCMs) that are obstructing decommissioning efforts at the nuclear disaster sites.

Published in the journal *Nature Materials Degradation*, the development is the first time a close approximation of a real LFCM has ever been achieved.

LFCMs are a mixture of highly radioactive molten nuclear fuel and building materials that fuse together during a nuclear meltdown.

During the Chernobyl and Fukushima nuclear accidents, radioactive materials mixed with fuel cladding and other building materials in the reactors and are now incredibly difficult and dangerous to remove from the sites. If left untreated, the LFCMs pose an ongoing radiological safety risk to the local environment.

Sheffield notes that **in the case of Chernobyl, the mixture of molten fuel, cladding, steel, concrete and sand formed nearly 100 tons of highly radioactive glass-like lava, which flowed through the nuclear power plant and has solidified into large masses.**

The masses present a highly dangerous risk to personnel and the environment in the surrounding area and could remain a hazard for decades, even millennia, unless something can be done to stabilize or remove them. However, very few samples of these meltdown materials are available to study and the masses are often too hazardous for people or even robots to get close to in order to better understand the behavior of the materials.

Dr. Corkhill said: "Understanding the mechanical, thermal and chemical properties of the materials created in a nuclear meltdown is critical to help retrieve them, for example, if we don't know how hard they are, how can we create the radiation-resistant robots required to cut them out?"

In the new research published today (30 January 2020), the University of Sheffield engineers at the NucleUS Immobilization Science Laboratory (ISL) report their development of small batches of low radioactivity materials that can be used to simulate LFCMs.

These simulated materials have been used to analyze the thermal characteristics and corrosion kinetics of LFCMs, which produced results that are very close to those of real LFCM samples reported by previous studies.

The study of the corrosion behavior is vital to support ongoing decommissioning efforts – both at Chernobyl and the Fukushima Daiichi Nuclear Power Plant – where LFCM-type materials are thought to have formed, and remain submerged in water used to cool the melted core. Using the new simulant materials developed at the University of Sheffield, Dr. Corkhill and her team are collaborating with researchers at the University of Tokyo and the Japan Atomic Energy Agency to investigate the process of highly radioactive dust formation that occurs at the surface of LFCM when water is removed.

Dr. Corkhill added: "The major difficulty in understanding the real materials is that they are too hazardous to handle and, although the Chernobyl accident happened over 33 years ago, we still know very little about these truly unique nuclear materials.

"Thanks to this research, we now have a much lower radioactivity simulant meltdown material to investigate, which is safe for our collaborators in Ukraine and Japan to research without the need for radiation shielding. Ultimately this will help advance the decommissioning operations at Chernobyl and also at Fukushima too."

The investigation into the corrosion behavior needs a lot more work, but having established a starting point, the research team hopes to advance this work quite rapidly. Dr. Corkhill noted**: "Since the clean-up of Chernobyl is anticipated to take around 100 years, and Fukushima at least 50 years, anything we can do to speed up the process will be beneficial to Ukraine and Japan, in both financial and safety terms."**

The development at Sheffield comes ahead of the Olympic Games being held in Japan this year. The Olympic torch relay is due to start in J-village - a sports ground close to the site of Fukushima - where high levels of radioactivity have been found.

Dr. Corkhill added: "Until we have developed an understanding of the meltdown materials inside Fukushima, we can't remove them — and until then, there may always be a small risk that radioactive materials from the reactors may find their way to the surrounding environment."

Dr. Corkhill is part of the University of Sheffield Energy Institute, which is finding low-carbon solutions to some of the world's biggest energy challenges.

The Energy Institute carries out energy research across a wide spectrum of fields, including renewable, nuclear and conventional energy generation, energy storage, energy use and carbon capture, utilization and storage technology. Its multi- and interdisciplinary research teams work with industry and government on sustainable solutions.

Research into nuclear energy is one of the institute's strengths, with its academics conducting world leading research to ensure nuclear power can generate electricity safely, securely and sustainably.

Nuclear reactors are at risk of terrorism attacks

Source: https://www.standardmedia.co.ke/article/2001360830/nuclear-reactors-are-at-risk-of-terrorism-attacks

Feb 18 – **Chernobyl's 30th anniversary on April 26 comes against the backdrop of growing apprehension that nuclear reactors may become a terrorist target.**

Serious concern arose during the recent Islamic State attacks in Brussels. Evidence suggested that the assailants were considering a nuclear-related incident. The terrorists had a senior Belgian nuclear official under surveillance, and two former nuclear power-plant employees were reported to have joined Islamic State.

This may help explain why Belgian authorities rushed military forces to protect its nuclear plants. The scare provided a reminder that nuclear reactors are radiological mines that terrorists could exploit. Destruction of a plant would mark a zenith of terrorist violence. Radioactive elements would spread across national boundaries. It would endanger the lives of many, while creating economic and environmental havoc mimicking the Chernobyl or Fukushima explosions.

How concerned should the West and other regions be? And if the peril remains so serious, why doesn't the international community impose mandatory security standards?

Actually, Washington has tried to do just that. On June 14, 1946, the US proposed the Baruch Plan at the United Nations. It called for an International Atomic Development Authority that would maintain "managerial or ownership of all atomic energy activities potentially dangerous to world security" and "the power to control, inspect and license all other atomic activities."

Had Cold War politics not intervened, reactors would likely be safer and more secure today. Instead, the international community now faces a patchwork of national regulations. The result leaves open a terrorist nuclear Pandora's Box.

Certainly, enforcement of robust security standards — including adequately manned, trained and armed guard forces; physical barriers to vital areas; detection, alarm and communication systems; a careful vetting of all plant employees to ensure against infiltration of terrorists and criminals, along with other measures — are but a small price to pay to avoid yet another intentional or accidental Chernobyl or Fukushima.

Unfortunately, given inertia, we may have to wait for the intentional Chernobyl to take place to get action. Consider that nuclear critics have been concerned for decades that reactors are likely terrorist targets and not enough is being done to protect them.

They insisted that terrorists could breach the containment structures of nuclear power plants using sophisticated hand-held weapons, rocket-propelled grenades, vehicular bombs and water-based or airborne attack. They also warned about insider sabotage of vital plant life lines, which could release the core's deadly radioactive contents.

But with no serious attack so far, complacency has set in. Belgium finally put armed guards at its plants only after last year's Paris terrorist attacks. How many other nations among the 30 with power reactors have been equally complacent?

But smugness has been revealed to be an embarrassment. In 2012, Greenpeace activists broke into a Swedish nuclear installation. The environmental activists scaled fences surrounding two nuclear power reactors and hid four of its party overnight on the roof of one. In 2014, another group of Greenpeace activists broke into a French nuclear power plant and hung a large banner from the reactor building.

These stunts demonstrate there is something seriously wrong with power-plant security practices in the two countries, and in perhaps many others.

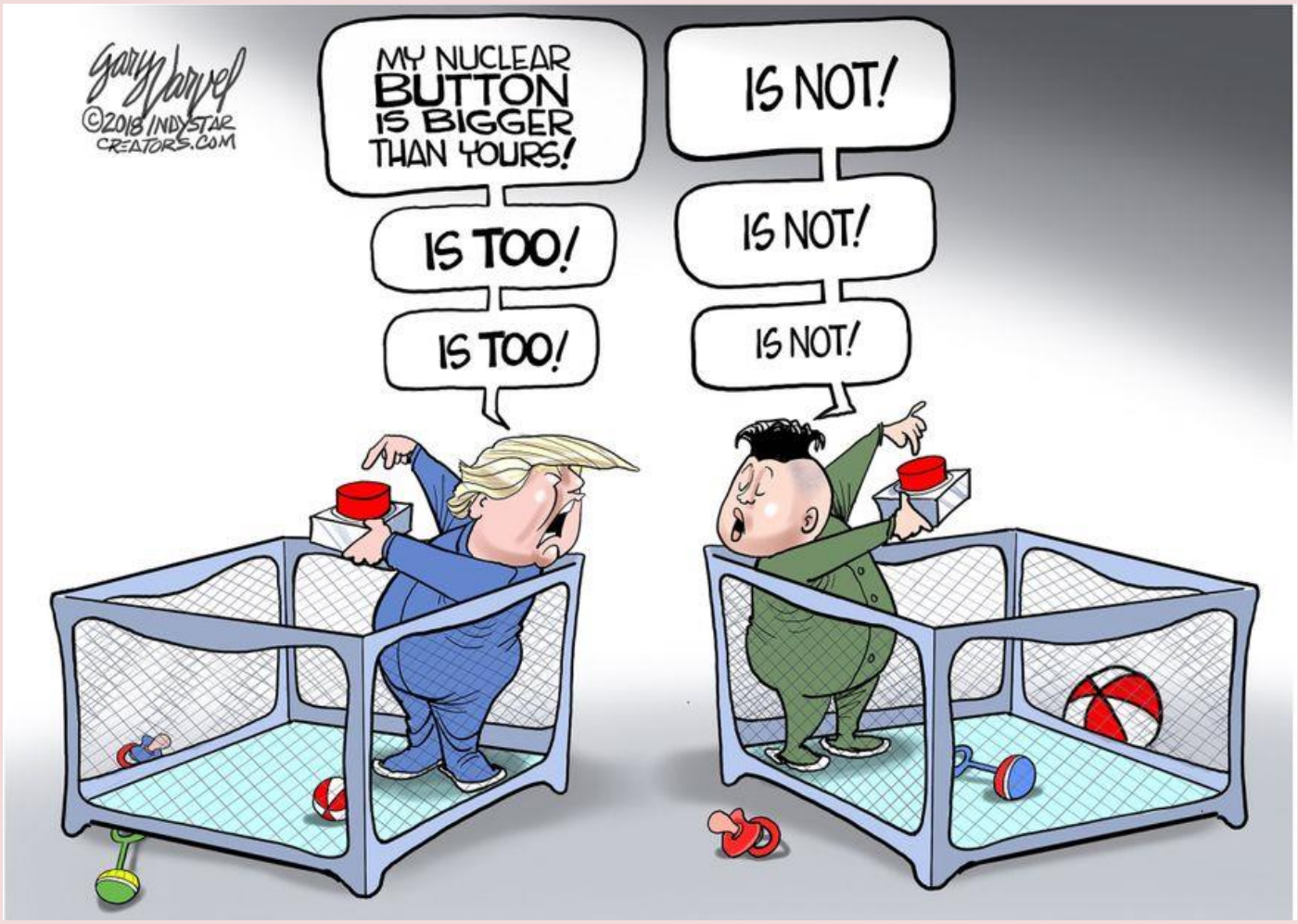
The International Atomic Energy Agency, the World Association of Nuclear Operators and the European Union — all press for reactor security and safety by offering guidelines. They send survey teams to evaluate plant security at the request of the host country. But they cannot force countries to change their security habits.

Generally, such mindsets don't change easily. It takes events, not hypotheticals, to do that.

It took the 1993 truck bombing of the World Trade Center in New York, for example, to push the US into setting tougher standards for protecting reactors against vehicular bombings.

But even in the US, which purports to apply the security gold standard, mock attacks have repeatedly found holes in reactor security.

We should expect that only an intentional Chernobyl incident will get complacent countries to dramatically change their security culture.


Gary Varvel
©2018 INDYSTAR CREATORS.COM
MY NUCLEAR BUTTON IS BIGGER THAN YOURS!
IS TOO!
IS TOO!
IS NOT!
IS NOT!
IS NOT!

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

EXPLOSIVE NEWS

New trends in mine action

By Olaf Juergensen

Source: https://www.undp.org/content/undp/en/home/blog/2020/new-trends-in-mine-action.html

1

Feb 11 – More than 600 delegates are gathered this week at the UN Headquarters in Geneva to discuss an issue that is still of concern to at least 60 countries: mine action.

This is the 23rd International Meeting of Mine Action National Directors and United Nations Advisers (NDM-UN), and it has been interesting to follow how the agenda has evolved over the years, from focusing on technical matters related to the risky job of demining a single square metre of land to addressing challenges of information management and finding best ways to build lasting national institutional capacity to oversee the mine action industry and ensure it operates in a way that is both safe and efficient. Another interesting area of concern lately is around the environmental impact of mine action.

Although the international community's attention remains on the release of land and clearance of mines and explosive remnants of war across thousands of square kilometres in more than 60 countries, what has been most scrutinized in recent years is how these devices are being removed. The large-scale excavation of soils, clearing of vegetation, and use of explosives to destroy discovered munitions and stockpiles represent a new area of concern as we strive to do things better and find balanced solutions that are cognizant of the planet and of the millions of people living in the long shadow of war.

Photo: UNDP Cambodia

New challenges

These new challenges led to the recognition from within the industry that the impact of mine clearance must also be viewed as altering the geographies in which it takes place. This is the reason why the NDM-UN will have its first session on mainstreaming environment and climate change into mine action planning and operations, an initiative by the Norwegian People's Aid, a long-standing partner of UNDP.

UNDP has been a strong advocate for including mine action into the development debate and, more recently, the Sustainable Development Goals (SDGs). Together with the Geneva International Centre for Humanitarian Demining, we are working on tools and methodologies that allow the integration of mine action planning and reporting into broader national development processes, particularly those involving SDG frameworks.

The impact of landmines and explosive remnants of war has grown in scale and complexity over the past 23 years. There has been a proliferation of hard-to-detect improvised explosive devices and an intensification of warfare in urban areas, particularly in the Middle East, which made the challenge of rendering areas safe a much more complex endeavour than the traditional demining of the past.

Detailed evidence

Mine action is heavily dependent on the use of accurate detailed evidence. When this doesn't happen, the results can be deadly. Our work to link mine action to the SDGs relies on the technical data and information management systems used by the mine action centres that we support around the world to help ensure that prioritization and planning are based on expected human development outcomes and expanding the development opportunities of war-torn societies.

Clearly the important humanitarian work of mine clearance must continue apace and supporting the release of land so countries and communities can further develop is also UNDP's focus. But what is becoming more evident is that through a greater appreciation for the 17 SDGs and their interlinkages, the mine action sector is moving towards closing some of the policy and operational gaps between delivering humanitarian support and building the foundations for sustainable development.

***Olaf Juergensen** Is a Development and Mine Action Specialist, UNDP Istanbul Regional Hub.*

Bomb attacks: 'Sweden is either described as a war zone or heaven on earth'

Source: https://www.thelocal.se/20200203/explosions-interview-police-stefan-hector-sweden

Feb 03 – Stefan Hector is the newly commissioned chief for 'Hoarfrost', a Special Incident operation tasked with tackling the rise of shootings and explosions in Sweden.

In an interview with The Local he gives a picture of the recent detonations and shootings in Sweden and what the police are doing to try and stop it.

Why are there so many explosions in Sweden?

"We've seen, over the last couple of years, that the amount of explosions in Sweden have risen to a level not seen anywhere else in Europe. The reasons, or underlying cause, are criminals clashing.

"They range from conflicts of a rational character, like market shares for the illegal narcotics trade, or more personal, such as provocations or insults, old conflicts with causes long-forgotten. Nevertheless, the explosions are an expression of clashes between criminal elements.

"These criminal elements are in large part comprised of street gangs from 'vulnerable areas' in the suburbs but also what we sometimes refer to as 'biker gangs'. There is, however, a lot of overlap between these two groups so as a whole this is about conflicts between different criminal networks."

How do your colleagues abroad view this development in Sweden?

"They are astonished. The prevailing picture of Sweden is that it is a calm and stable country and these expressions of violence, which are without equal, at least in Europe, is a surprise to our neighbouring countries.

"We have ongoing collaboration with many of the European countries, especially with the Nordic countries, and no one has the same kind of problems which is why this is a perplexing and possibly even frightening issue. But they are actively seeking more knowledge and are discussing these issues with us in order to share experiences and trying to understand this phenomenon."

Hand grenades used to be the go-to for criminals in past explosions, have the methods changed?

"These last few years one of the most common explosives were hand grenades. However we've seen a shift from hand grenades towards homemade bombs or IEDs, improvised explosive devices. The devices ranges from simple designs, filling a thermos with explosives and a fuse, to more advanced ones with remotely detonated triggers."

Where does the bomb material come from? Is it external or do criminals get their hands on the components in Sweden?

"We haven't got the full picture but most of the material for homemade bombs are things you can buy over the counter, it *isn't* difficult to obtain. When it comes to the actual explosives our impression is that it's usually commercial grade explosives that are used in construction and road work that gets stolen or misappropriated. We have reason to believe that the majority of the explosives used in homemade bombs in Sweden come from these kinds of sources and then end up on the black market."

Isn't some kind of pre-existing knowledge or information required to make these bombs?

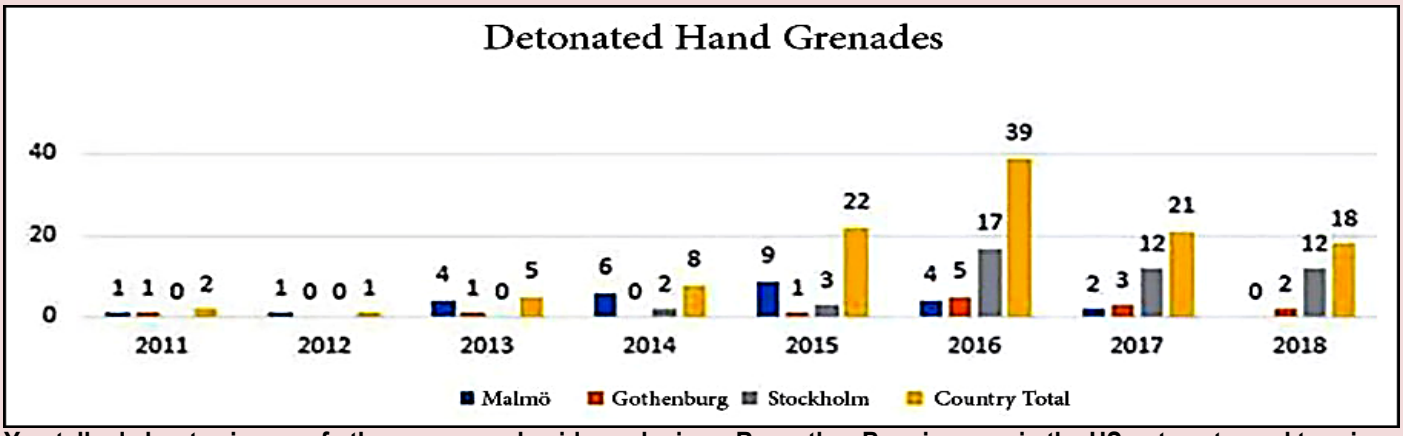
"It does require a certain level of knowledge to build a bomb and what we've seen is that there are a few groupings, or clusters, that make charges and sell or pass them on. With Operation Hoarfrost, this far we've neutralized two such clusters of bomb-makers and are continuing work on getting more of these criminal groupings. It does take know-how and experience though, we are currently trying to map out who these people and networks are in order to neutralize them."

Has Operation Hoarfrost yielded any results?

"It is still too early to say anything certain about the overall effect on our main objective, which is to break the progression of shootings and detonations in Sweden.

"But when it comes to indicators, we can use Malmö as an example where we are showing our strength with reinforcements coming in nationwide. There are signs that the arrests, busts, screenings and seizures done towards these environments, people involved in shootings and detonations, are beginning to have an effect on similar violence in Malmö. It would be strange otherwise, seeing as we've made huge busts of guns, explosives and narcotics."

You have been given quite a lot of resources with Hoarfrost, but has the police shortage in Sweden affected your work?
"Yes, and no. Basically we would have liked to be able to do these kinds of operations without a show of strength, meaning that we take police officers from other parts of Sweden in order to amass resources in Malmö. In an ideal world we would have been able to operate here without reinforcements, but we're not there yet.
"Until we have enough police officers in Sweden we need to move resources around. So these kinds of operations do affect the police organization in Sweden, but we're not taking enough officers from each region for it to make any impact. That's the advantage of having an organization where you can collect people nationwide, the detrimental effect on a specific geographical region is minimal."



You talked about seizures of other weapons, beside explosives. Recently a Bosnian man in the US got sentenced to prison for smuggling weapon parts to, among others, Swedish neo-nazis. How common are criminal international networks when it comes to Swedish gunrunning?
"From what I've seen, one of the most common guns in criminal clashes in Sweden is the AK 47, and they aren't manufactured here. Which means that it needs to be smuggled into the country, so in that sense international players are contributing to shootings in Sweden. These kinds of guns usually come from the Balkans, as they have a surplus of weapons from past decades of conflict."
Are those the kind of weapons you usually seize or are, for example, Swedish hunting weapons also confiscated?
"No. Swedish hunting rifles are extremely rare in these kinds of contexts, it's usually assault rifles such as the AK 47, pistols or submachine guns. It is very, very rare that we see hunting weapons as a part of our work with Operation Hoarfrost."

Where in Sweden do these kinds of crimes, shootings and detonations, happen? Are there geographical differences?
"Yes, there's a difference. But it has also changed over time. I would say that the most frequent shootings and detonations happen in areas that the police define as 'vulnerable' and 'especially vulnerable' areas, there are 62 in Sweden.
"But it has been changing. Before, shootings, gun seizures and detonations were predominant in the big cities: Stockholm, Malmö and in some capacity Gothenburg. But now we see a progression where it is spreading to smaller cities in Sweden as well: Värnamo, Västerås, Uppsala and so on."
Why is that?
"We're seeing that criminal networks get a foothold, or rather, acquire a foothold outside of the big cities. We don't know for sure but a hypothesis is that the criminal market is exhausted in the big cities which is why they seek out smaller cities where market shares are more readily available."
How about the bigger picture? What is the nature of crime in Sweden?
"What I can verify is that shootings and explosions within criminal environments are on a whole other level than the rest of Europe, however the overall crime statistics encompasses so much more than just the shootings and detonations.
"In the end these are conflicts and clashes between criminal groups in Sweden, and it is important to see it in that light. The risk of third parties getting hurt is very, very small, even though it does exist.
"I mean, this is not an embellished view of Sweden. I have noticed a polarization in how people view Sweden. On one hand it's described as a war zone with guns and misery, and on the other hand it is pictured as heaven on earth.
"What you have heard this far is my view, from a standpoint of the crime-fighting mission of the police, and it is dark, that is the nature of the beast. The police deal with bad stuff, that is our mission, which is why my view is just one part of the picture. However, what I can say is that I'm not worried when walking the streets of the city."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

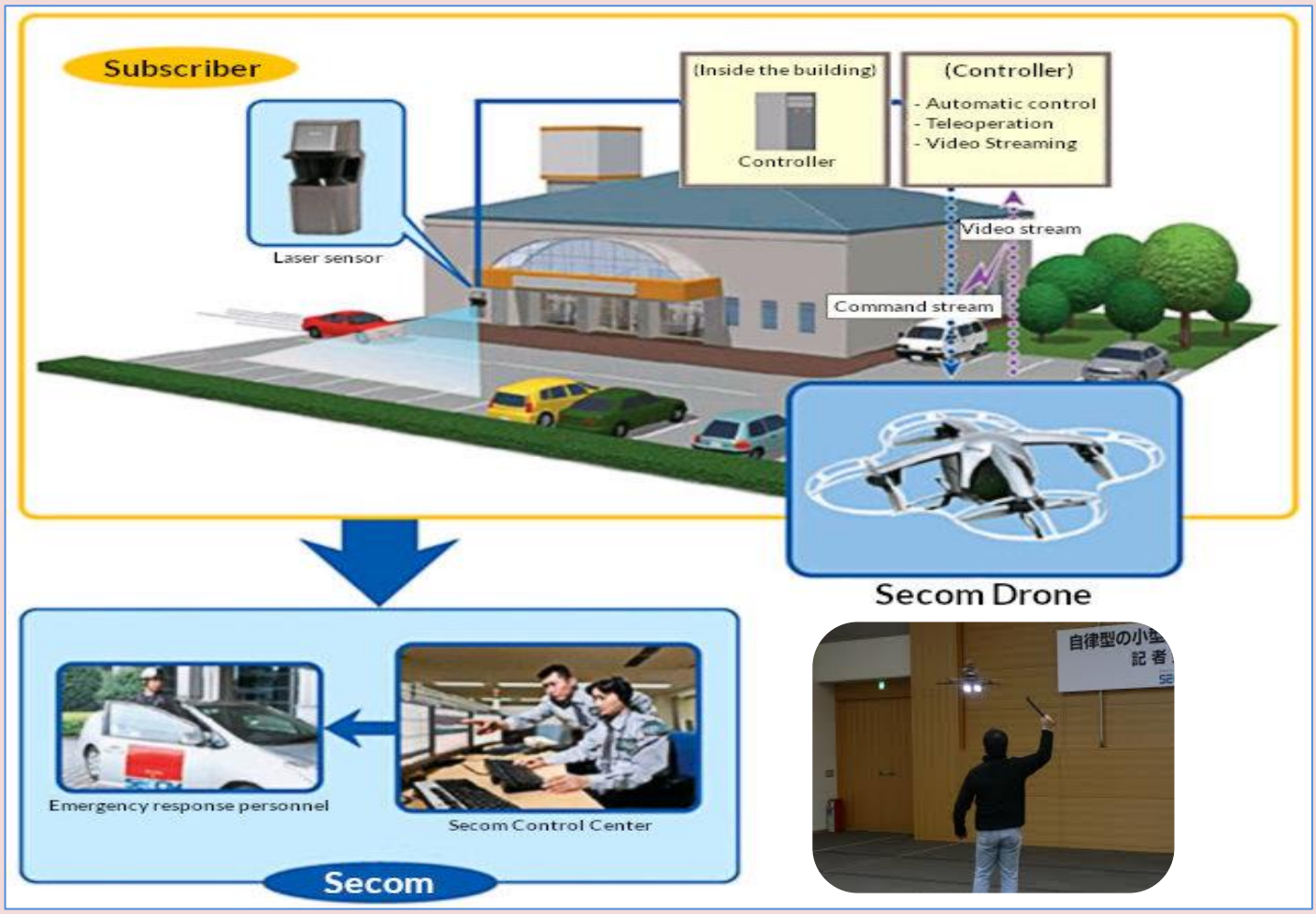
CYBER NEWS

Towards Olympic Games – Smart City Applications in Tokyo

Source: https://i-hls.com/archives/98605

Feb 01 – In preparation for the Tokyo Olympic and Paralympic Games slated for this summer in Japan, demand for drones and security robots has grown. The many spectators from both home and abroad will be unknowingly protected by an upgraded security system, from drones to security cameras. These efforts are also part of the move to make Tokyo a leading smart city.

Secom, a major security company, tested its security service in December using a drone. The drone, measuring about 60 centimeters square, relentlessly pursued a "fugitive" — illuminating him with a searchlight and recording his actions with a camera. The next-generation machine, which is scheduled to be put into practical use in fiscal 2021, will use artificial intelligence and preregistered



information to identify people and cars, according to the-japan-news.com.

Counter-drone measures are also required. The same company is offering a system that will detect drone intrusions using radar and microphones to continue bolstering current security levels.

Security cameras installed in the lighting of trains is becoming widespread in Tokyo as an added security measure. It takes only 15 seconds to attach the lights, which function as a security camera and a data transmission device, to the ceiling of each car. The light sends the recorded images to operation centers located elsewhere.

Tokyu Railways, one of the railway operators in the Tokyo metropolitan area, will install the new fluorescent lights, called IoTube, in all of its 1,257 cars before the Tokyo Olympic Games start. The light can be installed without removing the wall or ceiling panels, and the most attractive point of the light is the low cost, the company said.

The company is expecting the new technology to not only be effective in the prevention of crimes such as pickpocketing and luggage theft but also in the real-time gathering of information on violence and other passenger incidents.

An advanced AI facial recognition system will be in place to identify over 300,000 people at the games, including athletes, volunteers, media and other staff, making it easier to move between venues, as reported by insidesport.co.

Hackers: A Psychological Profile

Source: http://www.homelandsecuritynewswire.com/dr20200212-hackers-a-psychological-profile

Feb 12 – Whether cracking digital security for good or ill, hackers tend to be people who are manipulative, deceitful, exploitative, cynical and insensitive, according to research from the University at Buffalo School of Management.

Recently presented at the Hawaii International Conference on System Sciences, the study analyzed the psychological profiles of college students in computer science and management to see which personality traits led to three different kinds of computer hacking: white hat, gray hat and black hat.

Buffalo notes that White hats are the ethical hackers, who help organizations detect and fix their security vulnerabilities. Gray hats are the "hacktivists," who hack for ideological reasons, such as attacking a political adversary, a company policy or even a nation-state. And black hat hackers, sometimes called crackers, are motivated by personal gain to breach computer systems—or may just be in it for the thrill of the attack, revenge or notoriety.

"Gray hatters oppose authority, black hatters are thrill-seeking and white hatters—the good guys—tend to be narcissists," says Lawrence Sanders, PhD, professor of management science and systems in the UB School of Management. "So even though white hats may be devious and psychopathic, we need them to address nefarious hacking activity."

The researchers surveyed 439 college sophomores and juniors to determine their personality traits, and developed a set of scales to determine the three hat categories, as well as a scale to measure each person's perception of the probability of being caught for violating privacy laws.

"Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently," says Joana Gaia, clinical assistant professor of management science and systems in the UB School of Management. "But they can be deterred if there is a likelihood of punishment—and the punishment is severe."

The results of the study suggest that security compliance will continue to be a problem, but there are several ways businesses and organizations can reduce the impact or prevent security breaches.

"Firms can use monitoring technology and multifactor authentication to prevent unauthorized access to physical and digital spaces," says Gaia. "Organizations could use personality traits to evaluate employees as security threats, but that should be approached cautiously for practical, ethical and privacy reasons."

Scientists develop portable sensors to trace explosives

Source: https://www.dailypioneer.com/2020/india/scientists-develop-portable-sensors-to-trace-explosives.html

Feb 10 – **Indian scientists have developed a cost-effective portable sensor that can trace explosives and toxic metals such as trinitrotoluene (TNT), trinitrophenol (TNP) and RDX even if just a few molecules are present, on the scale of parts per million (ppm). The senor, a solution, can be easily carried in public spaces like airports, railway and hotels or sensitive areas to counter terrorism.**

Developed by Dr CV Yelamaggad, and his team from Bengaluru-based Centre for Nano and Soft Matter Sciences (CeNS), an autonomous institute under the Department of Science & Technology, the solution works on the simple visual detection technique.

Talking about the concept, Dr Yelamaggad, who has been working on the technique for last 3 years, said, "It employs a fluorescent material known as coordination polymer, a hybrid system originating from the interaction between organic and inorganic moieties. This system being electron rich acts as an electron source.

"The explosive materials containing nitro groups are electron deficient and act as electron sink," he said.

"A charge transfer complex or an association of 2 or more molecules is formed between these electron sources and sink that is non-fluorescent and hence the fluorescence intensity decreases drastically which can be observed visually. The sensing can be done in solution as well in thin film forms at very minute part per billion concentrations," he further explained.

Selectivity is very perfect. Currently, there are many different kits which are being used for the sensing of explosive materials but they suffer from major drawbacks such as large size, need of repeated calibration and so on. However, solution phase developed by Dr Yelamaggad and his team can be comfortably transported and used in various places such as airports, rail stations and shopping complexes owing to its compact size and ease of handling. The simple visual detection technique makes it compatible to be used without calibration. A prototype of the sensor has been fabricated and demonstrated in the Bengaluru INDIA NANO-2018 expo under a collaborative project with Tata Steel. " We are also trying to explore possibilities to detect other explosives such as acetonitrile, benzene and toluene etc," said Dr

Yelamagged.Researchers said that with such low-cost sensors they want society to be a much safer place to live. "This is not just a research but in keeping with the societal responsibilities. We still need to do a lot of investigation. If this development can help save a single life it would be a great win for me," summed up the scientist.

Hackers Could Shut Down Satellites – or Turn Them into Weapons

By William Akoto

Source: http://www.homelandsecuritynewswire.com/dr20200214-hackers-could-shut-down-satellites-or-turn-them-into-weapons

Feb 14 – Last month, SpaceX became the operator of the world's largest active satellite constellation. As of the end of January, the company had 242 satellites orbiting the planet with plans to launch 42,000 over the next decade. This is part of its ambitious project to provide internet access across the globe. The race to put satellites in space is on, with Amazon, U.K.-based OneWeb and other companies chomping at the bit to place thousands of satellites in orbit in the coming months.

These new satellites have the potential to revolutionize many aspects of everyday life – from bringing internet access to remote corners of the globe to monitoring the environment and improving global navigation systems. Amid all the fanfare, a critical danger has flown under the radar: the lack of cybersecurity standards and regulations for commercial satellites, in the U.S. and internationally. As a scholar who studies cyber conflict, I'm keenly aware that this, coupled with satellites' complex supply chains and layers of stakeholders, leaves them highly vulnerable to cyberattacks.

If hackers were to take control of these satellites, the consequences could be dire. On the mundane end of scale, hackers could simply shut satellites down, denying access to their services. Hackers could also jam or spoof the signals from satellites, creating havoc for critical infrastructure. This includes electric grids, water networks and transportation systems.

Some of these new satellites have thrusters that allow them to speed up, slow down and change direction in space. If hackers took control of these steerable satellites, the consequences could be catastrophic. Hackers could alter the satellites' orbits and crash them into other satellites or even the International Space Station.

Commodity Parts Open a Door

Makers of these satellites, particularly small CubeSats, use off-the-shelf technology to keep costs low. The wide availability of these components means hackers can analyze them for vulnerabilities. In addition, many of the components draw on open-source technology. The danger here is that hackers could insert back doors and other vulnerabilities into satellites' software.

The highly technical nature of these satellites also means multiple manufacturers are involved in building the various components. The process of getting these satellites into space is also complicated, involving multiple companies. Even once they are in space, the organizations that own the satellites often outsource their day-to-day management to other companies. With each additional vendor, the vulnerabilities increase as hackers have multiple opportunities to infiltrate the system.

Hacking some of these CubeSats may be as simple as waiting for one of them to pass overhead and then sending malicious commands using specialized ground antennas. Hacking more sophisticated satellites might not be that hard either.

Satellites are typically controlled from ground stations. These stations run computers with software vulnerabilities that can be exploited by hackers. If hackers were to infiltrate these computers, they could send malicious commands to the satellites.

A History of Hacks

This scenario played out in 1998 when hackers took control of the U.S.-German ROSAT X-Ray satellite. They did it by hacking into computers at the Goddard Space Flight Center in Maryland. The hackers then instructed the satellite to aim its solar panels directly at the sun. This effectively fried its batteries and rendered the satellite useless. The defunct satellite eventually crashed back to Earth in 2011. Hackers could also hold satellites for ransom, as happened in 1999 when hackers took control of the U.K.'s SkyNet satellites.

Over the years, the threat of cyberattacks on satellites has gotten more dire. In 2008, hackers, possibly from China, reportedly took full control of two NASA satellites, one for

about two minutes and the other for about nine minutes. In 2018, another group of Chinese state-backed hackers reportedly launched a sophisticated hacking campaign aimed at satellite operators and defense contractors. Iranian hacking groups have also attempted similar attacks.
Although the U.S. Department of Defense and National Security Agency have made some efforts to address space cybersecurity, the pace has been slow. There are currently no cybersecurity standards for satellites and no governing body to regulate and ensure their cybersecurity. Even if common standards could be developed, there are no mechanisms in place to enforce them. This means responsibility for satellite cybersecurity falls to the individual companies that build and operate them.

Market Forces Work against Space Cybersecurity
As they compete to be the dominant satellite operator, SpaceX and rival companies are under increasing pressure to cut costs. There is also pressure to speed up development and production. This makes it tempting for the companies to cut corners in areas like cybersecurity that are secondary to actually getting these satellites in space.
Even for companies that make a high priority of cybersecurity, the costs associated with guaranteeing the security of each component could be prohibitive. This problem is even more acute for low-cost space missions, where the cost of ensuring cybersecurity could exceed the cost of the satellite itself.
To compound matters, the complex supply chain of these satellites and the multiple parties involved in their management means it's often not clear who bears responsibility and liability for cyber breaches. This lack of clarity has bred complacency and hindered efforts to secure these important systems.

Regulation Is Required
Some analysts have begun to advocate for strong government involvement in the development and regulation of cybersecurity standards for satellites and other space assets. Congress could work to adopt a comprehensive regulatory framework for the commercial space sector. For instance, they could pass legislation that requires satellites manufacturers to develop a common cybersecurity architecture.
They could also mandate the reporting of all cyber breaches involving satellites. There also needs to be clarity on which space-based assets are deemed critical in order to prioritize cybersecurity efforts. Clear legal guidance on who bears responsibility for cyberattacks on satellites will also go a long way to ensuring that the responsible parties take the necessary measures to secure these systems.
Given the traditionally slow pace of congressional action, a multi-stakeholder approach involving public-private cooperation may be warranted to ensure cybersecurity standards. Whatever steps government and industry take, it is imperative to act now. It would be a profound mistake to wait for hackers to gain control of a commercial satellite and use it to threaten life, limb and property – here on Earth or in space – before addressing this issue.

***William Akoto** is Postdoctoral Research Fellow, University of Denver.*

Russia, China and North Korea will pose biggest cyber threats to Tokyo Olympics: report

Source: https://thehill.com/policy/cybersecurity/483733-russia-china-and-north-korea-will-pose-biggest-cyber-threats-to-tokyo

Feb 19 – Russia, China and North Korea will pose the biggest cyber threats to the upcoming 2020 Tokyo Summer Olympics, a report released Wednesday found.
The Cyber Threat Alliance (CTA) — which is comprised of major global cybersecurity companies including McAfee, Cisco and Palo Alto Networks — detailed the cyber threats that would likely face the upcoming Olympic Games, due to take place in July and August, in its new report.
CTA wrote that the three countries posed threats due to geopolitical tensions with Japan and based on previous track records of cyberattacks.
"Japan is at the center of several regional conflicts, and its role as Olympics host is likely to make the country a high-priority target for longtime adversaries looking to embarrass Tokyo on the international stage," CTA wrote.

Potential methods of attack the countries might use include disinformation campaigns on social media, disrupting critical systems key to Olympics events and targeted data leaks.

Wi-Fi networks, ticketing systems and anti-doping organizations were judged by CTA to be most at-risk from these types of cyberattacks, along with Japanese officials, partner governments and sponsors of the Olympics.

Of the three countries, CTA concluded that Russia poses the biggest threat. This stems from Russian athletes being banned from competing in the 2020 Olympics under the Russian flag due to evidence that Russia manipulated data to protect athletes involved in state-sponsored doping.

CTA noted that Iran, which is normally included along with the other three countries as a top cyber threat, will likely not pose a threat to the Tokyo Olympics.

"Iran is less likely to conduct Olympics-related cyber threat operations," CTA wrote. "Despite Iran's history of conducting offensive cyber campaigns globally, we assess that it is not in Tehran's strategic interest to compromise the Tokyo Games or affiliated entities."

Beyond foreign cyber threats, CTA also warned that cyber criminals unaffiliated with nation states will also target the Olympics to try to exploit "tourists' poor cybersecurity awareness."

CTA urged the Japanese government to create plans to respond to major cyberattacks, and to check critical systems for vulnerabilities to hackers regularly.

Over the past decade, hackers have stepped up attacks on Olympic Games, with CTA noting that hackers successfully interrupted the stadium Wi-Fi system and took the official Olympics website offline during the opening ceremonies at the 2018 Pyeongchang Winter Olympics.

CTA is not the only group to warn of cyberattacks involving the Tokyo Olympics. Reuters reported earlier this month that the Bank of Japan warned the country's financial institutions of the likelihood that attempted cyberattacks would increase ahead of the Olympics.

The official Twitter accounts for the Olympics and for the International Olympic Committee were hacked last week and temporarily locked by Twitter.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

Coronavirus drone army deployed to spray disinfectant across China cities

Source: https://www.dailystar.co.uk/news/world-news/coronavirus-drone-army-deployed-spray-21399569

One drone managed to spray disinfectant across 16,000 square metres in just one morning in the latest attempt by Chinese authorities to combat the spread of coronavirus

Jan 31 – China has deployed an army of drones to disperse disinfectant over villages and cities in the latest attempt to combat the spread of coronavirus.

At least 213 people have died from the killer disease since it was first contracted from a market in the city of Wuhan, Hubei Province. The World Health Organization has since declared the outbreak a global emergency, with Brits trapped in the regions being evacuated on emergency flights.

Every region across the country has reported cases of coronavirus and China has now taken to using drones to try to prevent the spread.

Footage posted to social media in the coastal provinces of Jilin, Shandong and Zhejiang shows drones hovering in the air as disinfectant liquid is sprayed from their underside.

EDITOR'S COMMENT: What is this new fashion to use drones about everything? Viruses flourish where people are. They do not go for a walk around the (empty) city! Of course, panic gives birth to many unorthodox solutions but during mass emergencies, knowledge is the only effective antidote.

Madrid's Barajas Airport is closed with flights diverted after pilots detect DRONES in the take-off area

Source: https://www.dailymail.co.uk/news/article-7961165/Madrids-Barajas-Airport-closed-flights-diverted-pilots-detect-DRONES-area.html

Feb 03 – Madrid's Barajas Airport was closed for more than an hour today and flights diverted after pilots spotted (3?) drones in the area.

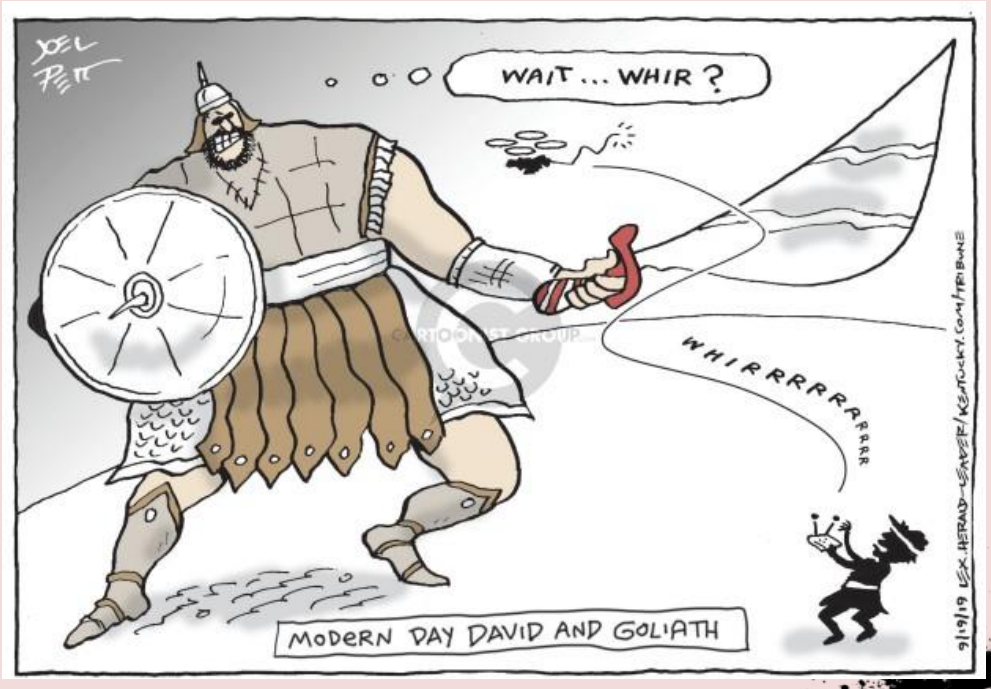
Spain's Transport Ministry said the airspace at the capital's international airport was shut down and 26 flights were immediately diverted elsewhere.

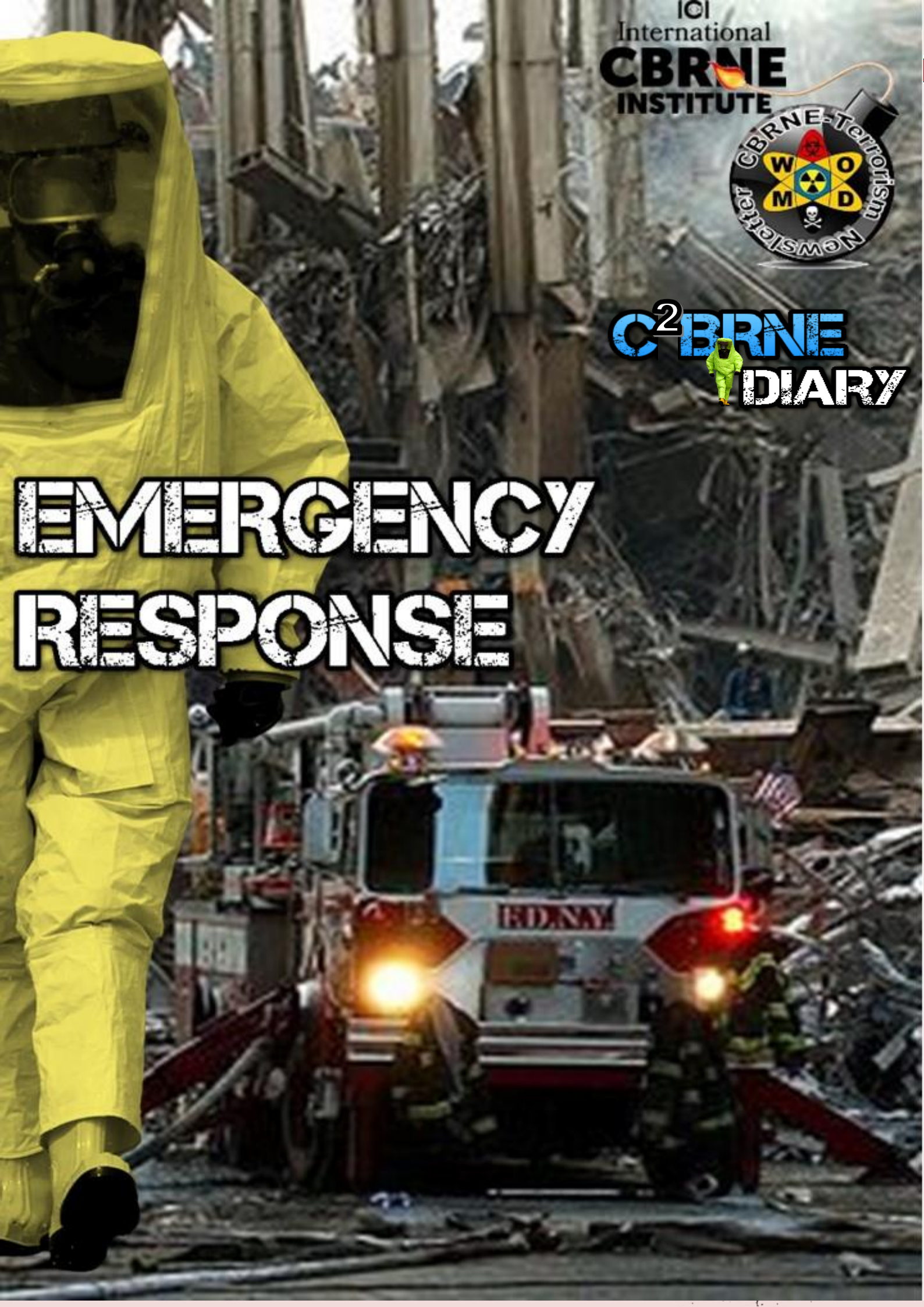
Several flights closest to the airport were allowed to land for security reasons.
Passengers were advised to check with the airport's authorities for further developments.
The airport said later on Twitter that it was 'now in operation' as runways were reopened.
Enaire, Spain's air navigation authority, had earlier reported delays in flights owing to the presence of drones in the area.
Two pilots were said to have seen some drones near the airport, which is located just east of the city centre.
The airport immediately activated a special procedure to halt landings and takeoffs and divert flights to other airports.

Chinese Drones Banned

Source: https://i-hls.com/archives/98789

Feb 09 – The Department of the Interior (DOI) of the United States has recently signed a no-fly order, officially grounding all of its drones that were manufactured in China or use Chinese made parts. The DOI has grounded approximately 800 drones due to cybersecurity concerns. The only drones to avoid the no-fly order are emergency drones used to combat wildfires.
The DOI uses drones for many applications besides fighting wildfires. The department uses drones for inspecting soil erosion, collecting mapping data, and conducting surveys of endangered species. The hope now is to replace the grounded Chinese drones with U.S. made drones.
Ever since the initial grounding, there have been only 12 authorized DOI drone flights to combat wildfires and deal with floods.
The reason for concern with Chinese drones is the same reason the United States is concerned with other Chinese-made technologies and companies, such as Huawei. The DOI doesn't want the potential threat of Chinese espionage to concern them, therefore they grounded all Chinese made drones and parts.
DJI, a popular Chinese drone manufacturer, has shown signs of "extreme disappointment" in the DOI's decision to ground Chinese drones. The company claims that the government's decision to ban drones comes from a politically motivated decision and not one based on cybersecurity, further expanding that the company has built their drones with special security considerations just for the U.S. government agencies.
DJI makes up a small portion of the DOI's fleet of drones, according to Popularmechanics.com. Other drones in the fleet come from France and several different states in the United States.
As of now, the no-fly order has no expiration date. So DJI and other Chinese drone manufacturers will just have to wait for the green light from the United States government.




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

How to Prepare and Respond When Natural Disasters Cause a Nuclear Emergency

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/how-to-prepare-and-respond-when-natural-disasters-cause-a-nuclear-emergency/

Jan 25 – The International Atomic Energy Agency has held its first course to train participants on preparedness and response to a nuclear emergency.

Imagine a nuclear emergency triggered by another emergency, such as a natural disaster like an earthquake, volcanic eruption, or tsunami. Or, imagine a tropical cyclone, hurricane or civil disturbance leading to a radiological emergency. Preparing to respond in complex emergency scenarios is what participants learned to do at a recent course on the topic, the first-ever such course by the IAEA, offered in cooperation with Austria's Civil Protection School in Traiskirchen, near Vienna.

"It is unlikely that a radiological event will be affected by an extreme natural disaster, but it is a possibility we need to be aware of and ready to respond to," said Emiliano Mingorance Sánchez, Head of the Chemical, Biological, Radiological and Nuclear Technical Unit at the Spanish Guardia Civil, who participated in the course.

Participants — mainly nuclear power plant operators, regulators and first responders — learned about the specific requirements different response professionals need to meet to effectively respond to combined emergencies and their associated challenges. Combined emergencies amplify the challenges emergency responders must manage. During the week-long course, they analyzed real case studies. One such case was the accident at Fukushima Daiichi nuclear power plant — a nuclear emergency combined with a natural emergency caused by a severe earthquake and tsunami.

Participants were asked to come up with a response plan for a simulated emergency with a missing radioactive source, combined with a flood. The challenge? To reach a consensus on the response plan and to think of all stakeholders and institutions required.

"Ensuring effective preparedness and response to a combined emergency requires the development and maintenance of an all-hazards emergency management system," said Phillip Vilar Welter, IAEA Emergency Preparedness Officer in charge of the training course. "A necessary element for such an all-hazards emergency management system is the establishment of a unified command and control system, which provides a means for effective communications, coordination, cooperation and integration of operating, local, regional and national emergency response organizations."

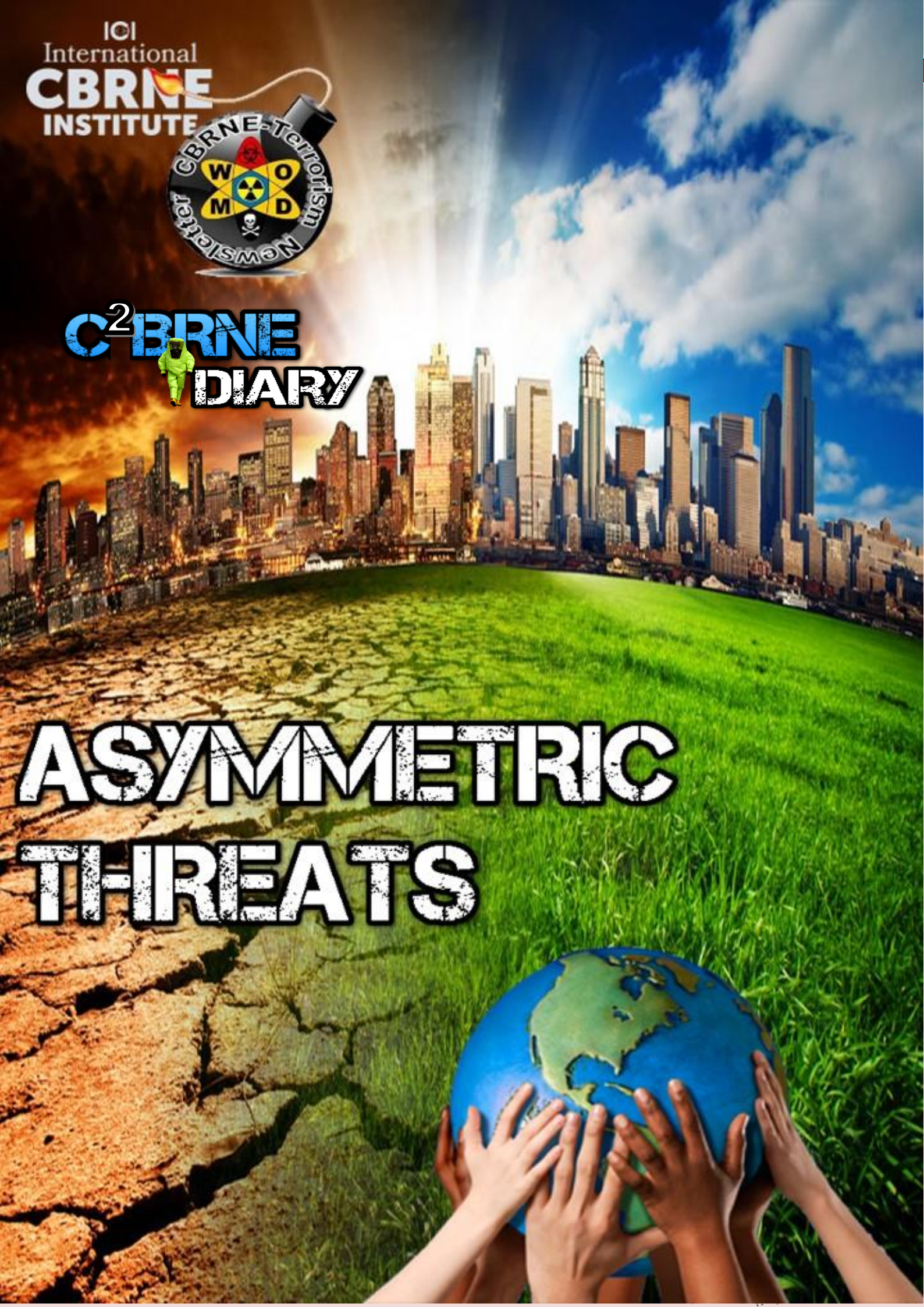
The topic of combined emergencies, Vilar Welter said, became especially relevant and was prioritized by the international community after the Fukushima Daiichi nuclear power plant accident. The IAEA then developed specific guidance that reflects the lessons learned from the accident.

Following this pilot course, the IAEA plans to publish an Emergency Preparedness and Response series publication on nuclear or radiological emergencies combined with other incidents or emergencies.

"After this course, I can reassess some of the procedures back home and try to influence or raise awareness of the need to adapt our norms and intervention protocols in the face of such emergencies," Mingorance Sánchez said.

More than 50 experts from 15 countries attended the course at Austria's Civil Protection School, a national education and training facility for radiation protection where police officers and first responders such as the fire brigade and ambulance services are regularly trained.

"Collaborating internationally in the face of transregional and international disasters is key to responding effectively in crisis situations, which is why we look forward to our continued cooperation with the IAEA," said Almira Geosev, course host and member of the Civil Protection Training Unit of the Austrian Federal Ministry of the Interior.


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

Warming Oceans Could Drive Antarctic Ice Sheet Collapse, Sea Level Rise

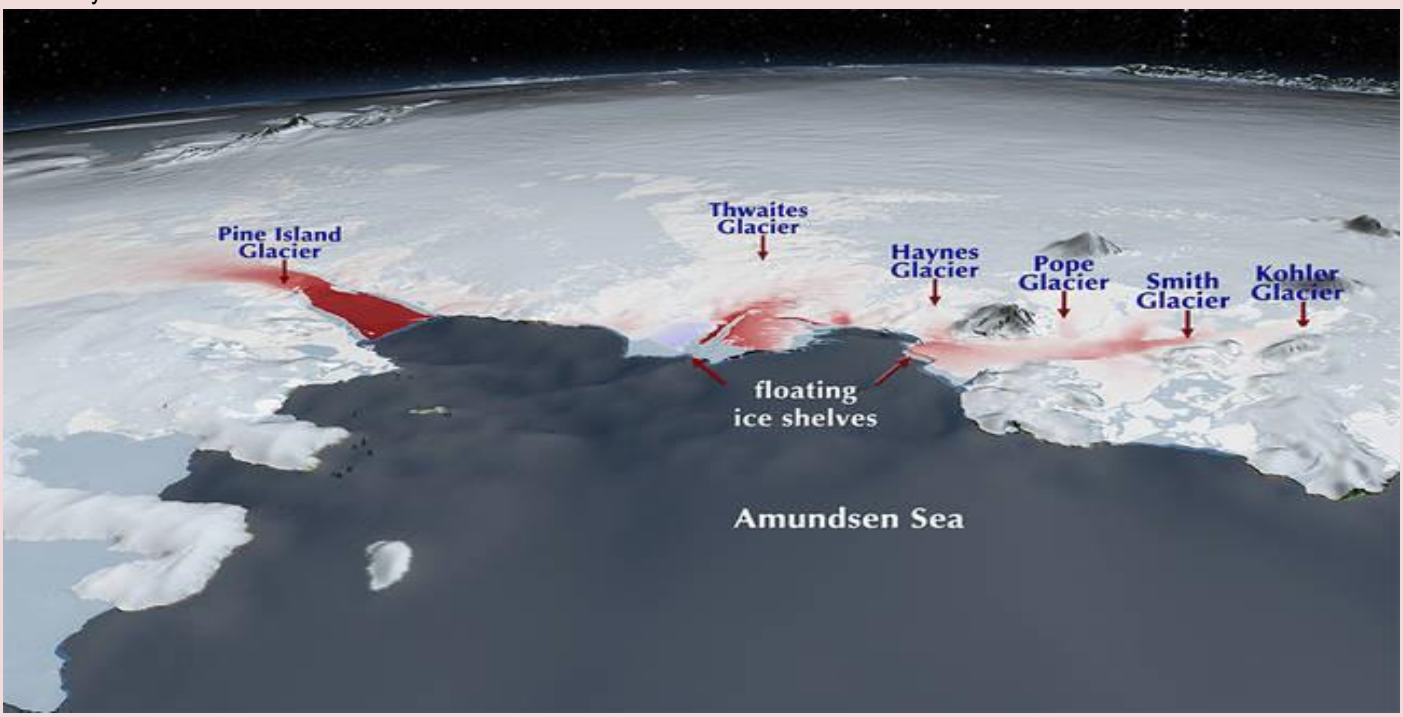
Source: http://www.homelandsecuritynewswire.com/dr20200204-warming-oceans-could-drive-antarctic-ice-sheet-collapse-sea-level-rise

Feb 04 – **A new study suggests the Western Antarctic Ice Sheet is less stable than researchers once thought. As in the past, its collapse in the future is likely.**

The finding is based in part on the results of a paper published in *Nature*, co-led by University of Wisconsin–Madison atmospheric scientist Feng He and Oregon State University's Peter Clark, which looks back at the last two time periods in which the planet transitioned from a glacial state, when ice sheets covered large swaths of the globe, into an interglacial state, such as the one we are in now.

The goal of the study, he says, was to better understand what contributes to rising sea levels. This has challenged researchers because of the large amount of uncertainty involved in understanding the contributions made by the melting of the Greenland and Antarctic ice sheets.

"Essentially, we just don't know how fast they are going to melt, whether the marine-based Antarctic ice sheet will collapse, or how quickly it will happen – whether it's 100 years or 1,000 years," says He, associate scientist in the Center for Climatic Research at the Nelson Institute for Environmental Studies. "By 2200, there is a possibility of 7.5-meter sea level rise when accounting for the instability of the western and eastern Antarctic Ice Sheet."



Wisconsin says that overall, the study found that warming below the surface of the planet's oceans is a significant contributor to ice sheet melt, particularly in the Antarctic, where a large portion of the ice sheet exists under the water.

During the last two transitions from glacial into interglacial periods, that warming was largely driven by the disruption of a process known as the Atlantic Meridional Overturning Circulation (AMOC), akin to an oceanic conveyor belt that carries warm waters northward and cold waters south.

Sub-surface warming, also referred to as oceanic forcing, was likely responsible for the collapse of the Western Antarctic Ice sheet during Earth's last interglacial period going back 125,000 years, which led to three meters of sea level rise. Overall, seas rose by up to nine meters, or nearly 30 feet, during the last interglacial period.

"Even right now, observations show that 50 percent of the mass loss from the Antarctic Ice Sheet is from subsurface ocean forcing," he says.

The study took a modeling approach to gather best estimates of the planetary influences underlying glacial and ice sheet melt as well as sea level rise, including greenhouse gas concentrations, global temperatures, and subsurface ocean temperatures.

Using the Community Climate System Model version 3 from the National Center for Atmospheric Research, the research team ran simulations for more than 25,000 model years using conditions and climate reconstructions surmised from data collected around the globe.
That includes greenhouse gases measured in deep ice cores, sea level indicators in corals, and cave features called speleothems. The simulations also included the position of the planet relative to the sun, ice sheet data and changes in heat transport associated with changes to AMOC.
The study found that AMOC was reduced in a single step at the transition of the last interglacial for roughly 7,000 years. During the transition into the current interglacial period, the Holocene, AMOC reduction lasted only about two-thirds as long and occurred in two steps.
During both transitions, however, AMOC reduction caused subsurface warming throughout the Atlantic Basin, which agrees with observed data. The reduction resulted in more sea ice in the North Atlantic Ocean and the reduction of ocean convection. Both of these reduce heat loss from the surface ocean, warming the subsurface, similar to the way in which winter snow helps insulate the ground below.
"Though we have known for a long time that sea levels rose during this past warm period, this study helps us to identify why and how that happened," says Andrea Dutton, study co-author, professor of geoscience at UW–Madison, and a current Fulbright scholar at the Antarctic Research Centre in New Zealand. "In particular, this new work points to the importance of the warming of the ocean in destabilizing marine-based ice sheets."
In the U.S., four out of ten people live in populous coastal areas, making them vulnerable to the effects of rising seas. Seventy percent of the world's largest cities are located near a coast.
Globally, by 2010, seas had already risen about 10 inches above their average levels in pre-industrial times. According to the National Oceanic and Atmospheric Administration, in 2014 they were rising at an increasing rate of roughly one-eighth of an inch each year.
Also by 2014, global temperatures had increased by 1 degree Celsius (1.8 deg Fahrenheit) relative to pre-industrial conditions, representing the same amount of warming that led to sea level rise during the last interglacial period.
"This is really scary because on paper at least, it shows that six to nine meters of sea level rise can occur with the same amount of global warming happening right now," says He.
"The Antarctic Ice Sheet is very susceptible to warming from the ocean so if we want to reduce the uncertainty of sea level rise from the Antarctic we need to monitor where subsurface warming will occur, with more ice sheet modeling development," He says. "Sea level rise is the number one threat of global warming."

Framing the Climate Crisis as a Terrorism Issue Could Galvanize Action

By Jennifer Zhang
Source: http://www.homelandsecuritynewswire.com/dr20200213-framing-the-climate-crisis-as-a-terrorism-issue-could-galvanize-action

Feb 13 – In many vulnerable regions of the world, the climate crisis has exacerbated loss of farmable land and increased water scarcity, fueling rural-urban migration, civil unrest, and violence. As a result, worsening geopolitical instability has aided the rise of terrorism and violence in the Middle East, Guatemala, and the Lake Chad Basin of Africa. Yet when people hear the words, "global warming," they typically don't think of terrorism. If they did, politicians would be far more likely to undertake drastic action to address the climate crisis.
Syria after 2011 is one example of how the climate crisis multiplied existing threats. Water scarcity, which had been worsening over the years, contributed significantly to the outbreak of conflict. The increased death of livestock, reduced arable land, and rise in food insecurity made it significantly easier for the terror organization calling itself the Islamic State of Iraq and Syria (ISIS) to locally recruit over two thirds of its fighters. Extreme weather phenomena offered ripe opportunities for ISIS to increase support among locals. When a vicious drought swept through Iraq in 2010, ISIS distributed food baskets to local inhabitants. When high winds destroyed vegetation in 2012, ISIS handed out cash to affected farmers. By offering a source of income and opportunity for people when their livelihoods were destroyed by droughts and other extreme weather, ISIS was able to cultivate support and draw members from local populations. In other words, the climate crisis increased geopolitical instability and aided the growth of terrorism.
The U.S. is vehemently opposed to terrorism as a matter of national security. According to the Pew Research Center, in early 2018, over three-quarters of American adults believed terrorism should be a top policy priority for the government, the highest of any given option. Over 46 percent of American adults favored *increasing* spending on anti-terrorism defenses, though the US military budget is already larger than the next seven highest-spending countries combined. The same survey showed that less than half of American adults believed climate change should be a top policy priority, ranking the second lowest of given issues.

Most Americans see "global warming" as an environmental, scientific, and political issue. Over half of Americans do *not* see it as a national security issue. While it is informative to present the climate crisis primarily through scientific data on global temperatures, atmospheric carbon concentration, and emissions levels, it does not galvanize people to action nearly as much as characterizing it as a matter of immediate national security. Doing the latter would make it a much higher priority for people in power.

The U.S. military already quietly recognizes climate change as a matter of national security, in part because it sparks conflict and unrest in other countries. In order to conceptually link the climate crisis to national security for the broader public, climate activists should expand and increase rhetorical focus on how the climate crisis worsens migration, foments geopolitical instability, and thereby aids terrorist organizations. Presenting the climate crisis in security-centric concerns and consequences ensures that *all* Americans — including right-leaning voters and people who would not be swayed by conventional appeals to ecological conservation or species preservation — become aware of how consequential it is. Security-centric framing would also help to shift the tone of climate activism toward addressing immediate threats, rather than simply encouraging global cooperation for the sake of future generations.

Reorienting climate rhetoric around national security also brings the action to a level that feels more achievable — at the *national* rather than global level. Whereas preserving the planet for future generations sounds aspirational and spiritually uplifting, it is an intrinsically international goal that calls upon many countries to work together for success. Framing plans to deal with the climate crisis in a way that requires concerted goodwill tends to encourage cynicism and blame-shifting when countries fail to meet carbon emission reduction targets. The vast majority of countries are failing to lower emissions to levels that would keep global warming below 2 degrees Celsius, as the 2015 Paris Agreement aspires to do. This collective failure dissipates blame and often disincentivizes countries from shouldering the burdens of emission reduction. Furthermore, focusing overtly on country-level climate reduction targets conceals the fact that emissions are largely generated by a handful of international corporations — over a third of all carbon and methane emissions since 1965 have been produced by 20 companies, including Saudi Aramco, Chevron, Exxon Mobil, and Royal Dutch Shell.

Holding corporations accountable for emissions requires immense political momentum, which is more easily galvanized by framing climate action as a necessary defense against immediate danger than as a voluntary restriction of certain economic activities for global well-being. While global cooperation to reduce emissions is what the international community should strive for, using nation-centered rhetoric that focuses on security threats can be an effective conduit to achieving this broader goal. Furthermore, linking the climate crisis to terrorism could increase the motivation and capital for countries to press hard in climate negotiations; in the face of immediate danger, the inertia of other countries or companies seems a paltry excuse for inaction.

***Jennifer Zhang** is a student at Barnard College, Columbia University.*

The World Climate and Security Report 2020

Source: https://imccs.org/report2020/

Feb 13 — The Expert Group of the International Military Council on Climate and Security (IMCCS) released its inaugural "World Climate and Security Report 2020" at the Munich Security Conference (MSC), the annual and influential gathering of senior international security and military leaders. The report was released at the MSC on Feb 13 and featured on the main stage of the MSC on Feb 15.

The Expert Group of the IMCCS consists of the Center for Climate and Security (CCS), an institute of the Council on Strategic Risks (CSR), the French Institute for International and Strategic Affairs (IRIS), the Hague Centre for Strategic Studies (HCSS) and the Planetary Security Initiative of the Netherlands Institute of International Relations (Clingendael).

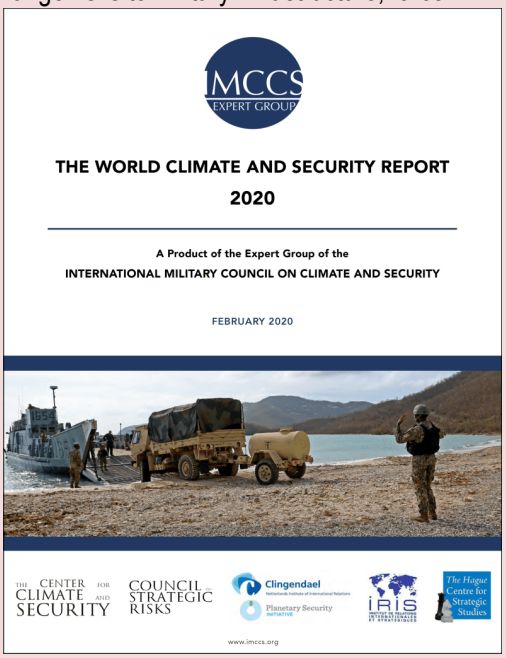
The report is written from the vantage point of international military and security experts, providing a global overview of the security risks of a changing climate, and opportunities for addressing them. It recommends "**climate-proofing**" **international security** – including infrastructure, institutions and policies, as well as major emissions reductions to avoid significant-to-catastrophic security threats. It is the first report of its kind.

While there has been progress over the past decades, with militaries and security institutions increasingly analyzing and incorporating climate change risks into their assessments, plans and policies, the "World Climate and Security Report 2020" shows that the risks are increasingly urgent, and more must be done. This contributed to the report's "Key Risks and Opportunities" findings.

KEY RISKS: Significant or higher risks to global security under current circumstances

1. **Water insecurity a global security risk:** Climate change-exacerbated water insecurity is already a significant driver of instability, and according to 93% of climate security and military experts surveyed for this report, will pose a significant or higher risk to global security by 2030.

2. **All regions facing increase in climate security risks (not just fragile/poor):** Though fragile regions of the world are facing the most severe and catastrophic security consequences of climate change; all regions are facing significant or higher security risks due to the global nature of the risks. For example, 86% of climate security and military experts surveyed for this report perceive climate change effects on conflict within nations to present a significant or higher risk to global security in the next two decades.
3. **Military institutions are increasingly concerned about climate risks:** As reinforced by the 31 nations represented in the International Military Council on Climate and Security (IMCCS), an increasing number of national, regional and international security and military institutions are concerned about, and planning for, climate change risks to military infrastructure, force readiness, military operations, and the broader security environment.
4. **Climate mitigation, adaptation and resilience efforts are increasingly urgent to avert the significant security consequences of climate change**, yet some proposed solutions such as geoengineering could present negative second-order effects to global security, if not implemented carefully.
5. **Rising authoritarianism, sharpened global competition and national agendas are hampering the needed cooperation** among nations to address the security risks of climate change.



KEY OPPORTUNITIES: A path forward for global security cooperation on climate change

1. **National, regional, and international security institutions and militaries around the world should advance robust climate resilience strategies, plans and investments**, especially regarding climate implications for water and food security and their associated effects on stability, conflict and displacement, in their primary mission sets or lines of effort.
2. **Security and military institutions should demonstrate leadership** on climate security risks and resilience and encourage governments to advance comprehensive emissions reductions and adaptation investments to avoid those security disruptions. Military organizations can also lead by example through taking advantage of the significant opportunities to adopt lower carbon energy sources, and make progress on other greenhouse gases beyond carbon dioxide.
3. **Climate-proofing development assistance for vulnerable nations which are likely hotspots of instability and conflict, as well as climate-proofing other policies affecting those regions, should be a priority for conflict prevention**. Assistance should be aimed at climate resilience challenges such as water security, food security, and disaster preparedness.
4. **The international community should embrace a Responsibility to Prepare and Prevent framework, given unprecedented foresight capabilities regarding the unprecedented risks of climate change**. This includes ensuring all levels of government and civil society, including all national, regional and international security institutions, are prepared for the security implications of climate change.
5. **Security institutions around the globe should integrate climate knowledge and training into institutional frameworks to ensure that knowledge and understanding of climate change threats permeates the organizational culture**. For example, climate security curricula should be added to national and regional training and defense colleges, professional military education, and climate security should receive significant treatment in international security and military fora.

Quotes from the Expert Group of the International Military Council on Climate and Security

"Climate change poses significant risks to global security, which could become catastrophic in the next two decades. As this report, and the 32-country International Military Council on Climate and Security shows, more and more military leaders are raising this alarm. It's not just environmentalists. The security community therefore has a responsibility to prepare for and prevent these threats, including through climate-proofing international security at all levels. That's why we've brought the World Climate and Security Report to the Munich Security Conference." **– General (Ret) Tom Middendorp, Chair, IMCCS**

"Major and urgent global emissions reductions are necessary in order to avoid significant, severe or catastrophic global security consequences in the future. We also need to climate-proof all elements of security – including infrastructure, institutions and policies. That's our

judgment from a military perspective. For example, 93% of the climate security and military experts surveyed in our World Climate and Security Report assess that climate-driven water insecurity will pose a significant or higher risk to global security by 2030. That's unacceptable, and the world's security leaders must do as much as they can to avoid that future. We hope that the Munich Security Conference is the beginning of a major effort by the security community to address this global threat." **– The Honorable Sherri Goodman, Secretary General, IMCCS**

"The security landscape is going to be disrupted significantly as a result of climate change. As military and security professionals, we are warning the public about this threat, But the solutions will mostly be civilian. That includes significant emissions reductions to avoid the worst effects of climate change, and climate-proofing security – including by investing heavily in the climate resilience of nations that need it in order to avoid instability, conflict and major humanitarian disasters." **– Captain Steve Brock, U.S. Navy (Ret), Chief of Staff, IMCCS**

"All regions of the world are facing significant security risks from climate change – not just the poorest, as we're seeing in Australia and around the world. Though fragile regions face the most severe consequences in the short term, these risks are global and interconnected. The World Climate and Security Report 2020 shows this clearly – from climate threats to military bases and critical infrastructure in North America and the Indo-Asia-Pacific, to climate-exacerbated political instability in the Middle East, North Africa, Latin America and even Europe, nobody gets to hide behind their gates to weather this storm. It's hitting all of us. And we all need to climate-proof our security." **– Caitlin Werrell and Francesco Femia, Managers and Senior Advisors, IMCCS**

"It is striking that climate change does not only have implications for military missions abroad and threat analysis, but also directly undermines military capabilities at home, because of the need to act more often as first responders in the case of wildfires, floods and ice storms. Militaries therefore must also climate-proof themselves." **– Louise van Schaik, Senior Member of the Executive Committee, IMCCS**

"*As the report notes, 'rising authoritarianism, sharpened global competition and national agendas are hampering the needed cooperation among nations to address the security risks of climate change.' But as we figure out what to do collectively to address this risk, we should be careful. Some proposed solutions, including geoengineering, could create disruptions to global security if not implemented carefully. So as we climate-proof our policies and actions, we need to avoid unintended consequences as much as possible."* **– Bastien Alex, Senior Member of the Executive Committee, IMCCS**

"When thinking about the possibilities to mitigate climate security risks through climate-proofing, it is important to understand that there are multiple ways of doing so. Through the Climate Security Strategic Capability game, we've identified more than 40 specific capabilities that can be utilized either independently or in tandem to help governments and militaries prepare for these myriad and complex risks. Gaming them is a useful way to create better awareness and understanding as well as helping prioritize what to do next!" **– Michel Rademaker, Senior Member of the Executive Committee, IMCCS.**

▶▶ **Read the full World Climate and Security Report 2020:** here