HZS
C²BRNE DIARY
Dedicated to Global First Responders
March 2021
03\21

# To AZ or Not to AZ? That is the Question!

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

# DIRTY R-NEWS

## Four ways to integrate the Radsim GS4 into your radiological scenarios

**By Bryan W Sommers (SGM U.S. Army, Ret.)**

Feb 23 – The use of simulation within a chemical, biological, radiological or nuclear (CBRN) training environment is not a new concept. Over the years, CBRN instructors have become well used to employing a variety of different simulation types - from notes written on index cards, to the calling out of verbal cues over the trainee's shoulder, or the use of multiple harmful chemicals as false positives that react to chemical detectors.

Read more »

## Iran's Nuclear Timetable: The Weapon Potential

IRAN WATCH

**By Valerie Lincy and Gary Milhollin**

Source: https://www.iranwatch.org/our-publications/articles-reports/irans-nuclear-timetable-weapon-potential

Feb 11 – This timetable estimates how soon Iran could produce the fuel for a small nuclear arsenal. It assumes Iran would try to build an arsenal of five warheads of the implosion type – the goal Iran set for itself when it began to work on nuclear weapons decades ago. With its thousands of gas centrifuges, some operating and some in storage, Iran can enrich uranium to a grade suitable for nuclear reactor fuel or to a higher grade suitable for nuclear weapons. On January 5, 2020, Iran announced that it would no longer observe any limit (such as that set by the nuclear accord of 2015) on the use of its centrifuges, or on the possession of uranium they enrich. Since then, Iran has expanded its stockpile of enriched uranium, increased the enrichment level of that stockpile, and brought more advanced centrifuges into operation.

The data below estimate the weapon potential of Iran's centrifuges and growing stockpile of enriched uranium. The potential is estimated as of November 2020, the date of inspection contained in the latest public report by the International Atomic Energy Agency (IAEA).

### Nuclear Weapon Potential of Iran's Centrifuges

As of early February 2021, Iran was operating 5,060 IR-1 centrifuges and 348 more powerful IR-2m centrifuges at the Natanz Fuel Enrichment Plant, as well as 1,044 IR-1 centrifuges at the Fordow Fuel Enrichment Plant. Iran also has approximately 12,000 IR-1 centrifuges and at least several hundred more IR-2m centrifuges in storage at Natanz and has been testing several other more powerful centrifuge models in smaller numbers at the Natanz pilot plant. Some of these more powerful models are adding to Iran's enriched uranium stockpile. By deploying them in larger numbers, Iran would be able to produce nuclear weapon fuel more quickly.

The operating centrifuges have thus far produced only low-enriched uranium (LEU), which is suitable for nuclear reactors but not nuclear weapon fuel. The estimates below assume that, in a dash to make weapons, Iran would rely on its IR-1 centrifuges and would first use its accumulated stockpile of LEU[2] and then its stockpile of natural uranium to produce nuclear weapon fuel. The estimates also assume that the IR-1s currently operating will perform at the same rate they have in the past.[3]

| **Estimated minimum time it would take Iran's 6,104 IR-1 centrifuges presently operating in production mode to produce the fuel for** | |
|---|---|
| **One bomb:**[4] | At least 2.2 months[5] |
| **Five bombs:** | At least 2 years[6] |

These estimates are the minimum theoretical times it would take Iran's known installed centrifuges, operating continuously at their proved capacity, to accomplish the required amount of work. It assumes that only the IR-1 centrifuges, which have been successfully operating in production mode for some time, would be used. The time actually needed in practice would be greater.

In addition, the enriched uranium produced would be in a gaseous compound (UF6). It would take additional time to convert the uranium in the gas to metallic form, and then to cast and machine the metal into bomb components. According to press reports, Iran began uranium metal production in February and intends to produce 20% enriched uranium metal. The uranium would only be a threat if Iran had already perfected all the other parts needed for a working bomb, such as the high explosives and firing circuit, and had made sure the parts would work together to achieve a nuclear explosion. There is ample evidence in the public domain that Iran has tried to achieve that goal (see Weaponization below), but no conclusive evidence that it has succeeded.

### Nuclear weapon potential of Iran's low-enriched uranium

Iran would need about 590 kg of LEU with an enrichment of 4% (suitable for use in nuclear reactors) to fuel one bomb.[7] As of November 2, 2020, Iran had substantially more than this amount, with a total of about 1,716 kg of uranium in the form of UF6 enriched "up to" reactor grade, according to the IAEA.[8] Iran has been adding to the stockpile since then but does

not yet have a sufficient amount of this material to fuel a small arsenal of five bombs. Accumulating this amount would take about one year from November 2020.[9]

Enriching uranium to reactor grade accomplishes most (about two-thirds) of the work needed to reach weapon grade. Thus, a dash to weapons could succeed much faster by starting with reactor grade uranium than by starting with natural uranium. For that reason, a substantial stockpile of reactor grade uranium in gaseous form is a strategic risk. Iran had accumulated such a stockpile, more than 16,000 kg, before reducing it under the nuclear accord. Such reactor-grade uranium would still need to be further enriched to weapon grade.

| **Estimated minimum time it would take Iran's 6,104 centrifuges, starting with sufficient reactor grade uranium, to enrich the uranium further to weapon grade for** | |
|---|---|
| **One bomb:** | At least 2.2 months[10] |
| **Five bombs:** | At least 11 months[11] |

To fuel a small arsenal, reactor grade uranium needs to be enriched further to about 90% U-235 (the isotope of uranium that explodes in fission bombs). Such enrichment would take at least an additional eleven months, using the IR-1 centrifuges Iran presently deploys. To shorten the time, Iran could add centrifuges or raise the enrichment level of its LEU stockpile. Beginning in January, Iran began enriching uranium to the level of 20%, which is closer to a level suitable for use in nuclear weapons. However, the accumulated amount of this material remains low and it too would have to be further enriched.

In addition, even after enriching to weapon grade, the uranium in gaseous form would have to be converted to metal, and the metal cast and machined into bomb components, as described above.

## The Risk of Secret Sites

Intelligence agencies have long been unanimous in one prediction:  If Iran makes nuclear weapons, it will do so at secret sites. The reasons are clear. If, in a dash to make weapons, Iran was to divert known (and therefore inspected) sites, material, or equipment to bomb making, it would risk detection before success, would violate the Nuclear Nonproliferation Treaty and would make itself an international pariah. It would also invite an attack on the very sites, material and equipment it diverted. No country has ever chosen to make an illicit diversion and dash to weapons, probably for the reasons just stated.

The data below reveal that as Iran develops more powerful centrifuges, it will need ever smaller sites to enrich bomb quantities of uranium. And the smaller the site, the more difficult it will be to detect. For example, at its nominal capacity, Iran's IR-2m centrifuge, of which Iran has about 1,000, could enrich the same amount of uranium as the IR-1 centrifuge in approximately one-fifth the space. Iran's enrichment plant at Fordow, which was publicly exposed in 2009, was built clandestinely by Iran to house about 3,000 centrifuges. For this reason, the estimates below use 3,000 centrifuges as the possible size of a secret enrichment plant.

| **Estimated minimum time it would take 3,000 of Iran's IR-2m[12] centrifuges operating at nominal capacity and starting with natural uranium to fuel** | |
|---|---|
| **One bomb:** | 3.2 months[13] |
| **Five Bombs:** | One year and four months[14] |

These centrifuges would require only about 32,000 square feet, equal to approximately twice the size of the ice surface of a professional hockey rink.[15] Alternatively, Iran could decide to split these 3,000 IR-2m centrifuges equally among three smaller sites of approximately 11,000 square feet each. That would decrease the size of each site and therefore the likelihood of detection. Each site would be about two-thirds the size of the ice surface of a professional hockey rink.[16] In early February 2021, Iran reportedly began installing two cascades of IR-6 centrifuges at the Fordow enrichment plant. According to Iran, this machine is ten times more powerful than the IR-1 and could enrich the same amount of uranium as this machine in much less space.

| **Estimated minimum time it would take 3,000 of Iran's model IR-6[17] centrifuges operating at claimed capacity and starting with natural uranium to fuel** | |
|---|---|
| **One bomb:** | 1.6 months[18] |
| **Five bombs:** | Eight months[19] |

These centrifuges would require approximately the same space as the model IR-2m centrifuges above, or approximately twice the size of the ice surface of a professional hockey rink. The space requirements above reveal that as Iran develops more efficient centrifuges, it will need ever smaller sites to enrich bomb quantities of uranium.

## The Status of Weaponization Efforts

The analysis above assumes that Iran would use 16 kg of highly enriched uranium metal (about 90% U-235) in the finished core of each nuclear weapon. Sixteen kilograms are assumed to be sufficient for an implosion bomb. This was the amount called for in a design for such a device that has circulated on the nuclear black market, to which Iran has had access.

Some experts believe that Iran could use less material, assuming Iran would accept a lower yield for each weapon. According to these experts, Iran could use as few as seven kilograms of this material if Iran's weapon developers possessed a "medium" level of skill, and if Iran

were satisfied with an explosive yield slightly less than that of the bomb dropped on Hiroshima, Japan.[20] If Iran chose to use an amount smaller than 16 kg, the time required to make the fuel for each weapon would be less than estimated here. Or, in the amount of time estimated here, Iran could make a greater number of weapons. Iran could decide not to use such a smaller amount of uranium if Iran wanted to have more confidence that its weapons would work, or if it wanted to reduce the size of its weapons by reducing the amount of high explosive.

According to an investigation by the IAEA into "possible military dimensions" of Iran's nuclear program, Iran had a coordinated nuclear weapon program between 1999 and 2003. Specifically, the IAEA found that Iran developed several components of a nuclear weapon and undertook related research and testing. The investigation revealed Iran's efforts in the following areas:

- computer modeling of implosion, compression, and nuclear yield;
- high explosive tests simulating a nuclear explosion using non-nuclear material in order to see whether an implosion device would work;
- the construction of at least one containment vessel at a military site, in which to conduct such high explosive tests;
- studies on detonation of high explosive charges, in order to ensure uniform compression in an implosion device, including at least one large scale experiment in 2003, and experimental research after 2003;
- support from a foreign expert in developing a detonation system suitable for nuclear weapons and a diagnostic system needed to monitor the detonation experiments;
- manufacture of a neutron initiator, which is placed in the core of an implosion device and, when compressed, generates neutrons to start a nuclear chain reaction, along with validation studies on the initiator design from 2006 onward;
- the development of exploding bridgewire detonators (EBWs) used in simultaneous detonation, which are needed to initiate an implosive shock wave in fission bombs;
- the development of high voltage firing equipment that would enable detonation in the air, above a target, in a fashion only making sense for a nuclear payload;
- testing of high voltage firing equipment to ensure that it could fire EBWs over the long distance needed for nuclear weapon testing, when a device might be located down a deep shaft; and
- a program to integrate a new spherical payload onto Iran's Shahab-3 missile, enabling the missile to accommodate the detonation package described above.

Information obtained by Israeli intelligence and revealed in April 2018 indicates that Iran sought to preserve this program after 2003 by dividing its nuclear program between covert and overt activities and retaining an expert team to continue work on weaponization. This "atomic archive" includes blueprints, spreadsheets, charts, photos, and videos – apparently official Iranian documents – that provide additional detail about Iran's efforts to develop a working nuclear weapon design that could be delivered on a ballistic missile.

## Need for Enriched Uranium?

Iran has no need to enrich large quantities of uranium for reactor fuel, which is the stated aim of its centrifuge enrichment program. Russia is fueling Iran's only power reactor (at Bushehr) and stands ready to do so indefinitely at a cost much lower than Iran would incur by enriching the uranium itself.[21]

If Iran did try to make the fuel itself, it is unlikely that Iran could field enough centrifuges to do so within the next ten years, or even longer. A standard sized power reactor (1,000 MWe) such as Iran's reactor at Bushehr requires about 21 metric tons of low-enriched uranium fuel per year, which would require generating nearly 100,000 separative work units, or SWU.[22] Iran's IR-1 centrifuges now produce about one metric ton per year. Thus, Iran's program would have to increase its capacity about twenty-one fold to have any plausibility as a civilian effort.

In an October 2015 letter to President Hassan Rouhani, Iran's Supreme Leader Ali Khamenei called upon the government to develop a plan for the country's nuclear industry to achieve an annual uranium enrichment capacity of 190,000 SWU within 15 years. In order to accomplish this, Iran would have to manufacture, install, and operate almost 240,000 additional IR-1 centrifuges, based on their historic output. Or, Iran would have to perfect, manufacture, and deploy in production mode a lesser number of more powerful centrifuges. It is uncertain how long it would take Iran to accomplish either of these steps, but either would take many years.

## Iran's Violations of Nuclear Accord

Following the U.S. withdrawal from the nuclear accord in May 2018, Iranian leaders threatened to stop implementing some of its commitments under the accord. Approximately one year later, it began doing so. The table below summarizes the steps Iran has taken since July 2019.

| Date | Iran's Violation |
|---|---|
| July 2019 | Begins enriching uranium above the 3.67% U-235 limit set by the accord, to a level of up to 4.5% U-235. |
| August 2019 | Exceeds the cap of 300 kg of UF6 on its stockpile of low-enriched uranium set by the [illegible] |

| | |
|---|---|
| September 2019 | Expands its centrifuge research and development beyond the limits set by the accord, both in the number and type of more powerful centrifuge it operates. |
| November 2019 | Resumes uranium enrichment at locations beyond those mandated by the accord, including the Fordow plant and the Natanz pilot plant. |
| January 2020 | States it will no longer limit the number of centrifuges in operation, which had been capped at 5,060 IR-1 centrifuges operating at the Natanz Fuel Enrichment Plant. |
| July 2020 | Announces plans to transfer more powerful IR-2m, IR-4, and IR-6 centrifuges from the Natanz pilot plant to the Natanz Fuel Enrichment Plant. The accord limits Iran to the use of IR-1 centrifuges at the Fuel Enrichment Plant. |
| October 2020 | Installs IR-2m centrifuges and begins installing IR-4 centrifuges at the Natanz Fuel Enrichment Plant. |
| November 2020 | Begins uranium enrichment in a cascade of 174 IR-2m centrifuges at the Natanz Fuel Enrichment Plant. |
| January 2021 | According to media reports, begins enriching uranium to the level of 20% U-235 at the Fordow plant. |
| February 2021 | According to media reports, begins installing IR-6 centrifuges at the Fordow plant and uses a facility in Isfahan to produce uranium metal, which the accord prohibits for 15 years. |

**Footnotes:**

[1] In a dash, Iran would be expected to use its uranium to fuel a bomb using an implosion design, such as the bomb dropped on Nagasaki, Japan; such a bomb would have to be tested to prove it worked, as was the Nagasaki bomb. A gun-type device such as the one dropped on Hiroshima without being tested, would require more than twice as much uranium.

[2] According to the IAEA, as of November 2, 2020, Iran's stockpile contained 2.408.5 kg of uranium in the form of uranium hexafluoride (UF6), some of which was enriched up to 4.5% in the fissionable isotope U-235 and some of which was at lower levels of enrichment. U-235 makes up about .7% of natural uranium; its concentration can be increased, or enriched, using centrifuges. Uranium enriched to 90% or more U-235 can be used to fuel nuclear weapons.

[3] According to pre-2016 production data from Natanz, Iran's IR-1 centrifuges have achieved an average annual output of about .8 separative work units, or SWUs, per machine. The SWU is the standard measure of the effort required to increase the concentration of the fissionable U-235 isotope. See http://www.urenco.com/index.php/content/89/glossary.

[4] Twenty kilograms of uranium enriched to 90% U-235 are assumed to be sufficient for one bomb. The uranium would need to be further processed into finished metal bomb components, which could cause about a 20% loss of material.

[5] Iran would need about 880 SWU to produce 20 kg of uranium enriched to 90% U-235 from nuclear reactor grade feed enriched to 4% U-235, assuming 1% tails. This theoretical calculation is generated using a SWU calculator published by URENCO, a European uranium enrichment consortium. With an output of .8 SWU annually, Iran’s 6,104 IR-1 centrifuges make about 4,880 SWU per year or about 400 SWU per month. Thus, it would take approximately 2.2 months to produce the 880 SWU. Iran's LEU stockpile contains 1,535 kg of uranium enriched "up to" 4.5%, according to the IAEA and is assumed here to be at an average enrichment of 4% U-235. This amount would be sufficient to fuel one bomb.

[6] This calculation assumes that Iran would use its stockpile of LEU, which is held at various levels of enrichment, and then its stockpile of natural uranium and that a total of 100 kg of uranium enriched to 90% U-235 would be needed to fuel an arsenal of five nuclear weapons.
- As of November 2, 2020, Iran's stockpile of 1,535 kg of LEU enriched "up to" 4.5% U-235, if assumed to have an average enrichment level of 4% U-235, would require about 2,280 SWU and yield about 52 kg of uranium enriched to 90% U-235, assuming tails of 1%.
- Iran’s stockpile of about 181 kg of LEU (in the form of UF6) enriched "up to" 3.67%, if assumed to have an average enrichment of about 3.2%, would require about 225 SWU and yield about 4.5 kg of uranium enriched to 90%, assuming tails of 1%.
- Iran’s stockpile of about 693 kg of LEU enriched "up to" 2%, if assumed to have an average enrichment level of 1.5%, would require about 300 SWU to produce about 3.9 kg of uranium enriched to 90%, assuming tails of 1%.

Thus, Iran’s stockpile of LEU would require a total of about 2,800 SWU to produce about 60.4 kg of uranium enriched to 90%. Iran would then have to use its stockpile of natural uranium to produce the remaining 39.6 kg of uranium enriched to 90% needed to fuel an arsenal of five bombs. Iran would require about 6,750 SWU to produce these 39.6 kg, assuming tails of .4%. Iran would have to produce a total of about 9,550 SWU, which would take its 6,104 IR-1 centrifuges about 2 years at their historic production rate of 4,880 SWU per year. This time will diminish as Iran accumulates more LEU.

[7] This amount of uranium enriched to an average of 4% U-235 would be sufficient feedstock to fuel one bomb after further enrichment, assuming uranium tails of 1% and that 20 kg of 90% U-235 are sufficient for one bomb. This theoretical calculation is generated using the SWU calculator published by URENCO.

[8] On November 2, 2020, Iran had a total of about 1,716 kg of uranium in the form of UF6 enriched "up to" reactor grade, according to the IAEA. This 1,716 kg included 1,535.1 kg enriched "up to" 4.5% and 180.7 kg enriched “up to” 3.67%. It does not include the uranium enriched "up to" 2%.

[9] Fuel for five bombs would require about 2,970 kg of LEU with an average enrichment of about 4%., assuming 1% tails, and that a total of 100 kg of uranium enriched to 90% U-235 are needed. In addition to the 1,716 kg enriched "up to" 4.5% or 3.67% that Iran had on hand in November 2020, 1,254 kg of

LEU would still be needed. To produce this amount, Iran would need 5,575 SWU. If the 6,104 IR-1 centrifuges perform at their historic production rate of .8 SWU per machine, this would take a little over one year. This time estimate does not reflect the use of more powerful centrifuges, which Iran is bringing online, or the use of uranium enriched "up to" 2%.

[10] It is assumed that only the IR-1 centrifuges already in production mode would be used in a dash to make nuclear weapons. Iran would need about 880 SWU to produce 20 kg of uranium enriched to 90% using a feed assay of 4% U-235, assuming 1% tails. At their proven production rate of .8 SWU per centrifuge, Iran's 6,104 IR-1s could produce about 4,880 SWU per year, or about 400 SWU per month. Thus, it would take about 2.2 months to make 880 SWU.

[11] Iran would need to generate about 4,400 SWU to make the 100 kg of 90% enriched uranium needed to fuel an arsenal of five bombs, with a feed assay of 4% U-235, assuming 1% tails. If Iran's 6,104 IR-1 centrifuges generated about 4,880 SWU per year, this would take about 11 months.

[12] Iran began operating a 174-machine cascade of IR-2m centrifuges in November 2020, but has not operated large numbers of these machines in production mode. It has about 1,000 such centrifuges and may be producing more. The IR-2m is based on Pakistan's P-2 centrifuge and is assumed in these estimates to have a nominal output of 5 SWU. See Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)," Science and Global Security, Vol. 16, Nos. 1-2 (2008), p. 9.

[13] 3,000 IR-2m centrifuges, with a nominal output of 5 SWU, would produce approximately 15,000 SWU in one year. If about 4,000 SWU are needed to produce the 20 kg of 90% U-235 to fuel one bomb (assuming tails of .3% and a feed assay of .7% U-235) then it would take about 3.2 months to produce the 4,000 SWU.

[14] The same 3,000 IR-2m centrifuges would produce the 20,000 SWU needed to fuel 5 bombs in approximately one year and four months.

[15] Each centrifuge is assumed to require about one square meter (10.7 square feet) of space, the amount used in Iran's enrichment plant at Natanz. The ice surface of a National Hockey League rink is 200 feet long and 85 feet wide.

[16] 1,000 centrifuges at 10.7 square feet each would require about 11,000 square feet.

[17] On November 2, 2020, Iran had about 136 IR-6 centrifuges operating in a research capacity at the Natanz pilot plant, according to the IAEA. By early February 2021, Iran had reportedly begun installing two cascades of these machines at the Natanz commercial plant. Iran has claimed that these centrifuges are ten times more powerful than the IR-1. Therefore, the IR-6 is assumed in these estimates to have a nominal output of 10 SWU. See Kiyoko Metzler, "UN Atomic Watchdog Raises Questions of Iran's Centrifuge Use," Associated Press, May 31, 2019.

[18] 3,000 IR-6 centrifuges each producing 10 SWU per year would produce in one year 30,000 SWU, or 2,500 SWU per month. Thus, it would take 1.6 months to produce the 4,000 SWU needed to fuel one bomb.

[19] 3,000 IR-6 centrifuges would produce the 20,000 SWU needed to fuel five bombs in about 8 months.

[20] See Thomas B. Cochran and Christopher E. Paine, "The Amount of Plutonium and Highly Enriched Uranium Needed for Pure Fission Nuclear Weapons," (Washington, DC: Natural Resources Defense Council, revised April 13, 1995).

[21] Russia and Iran signed a nuclear fuel agreement in 1995. Under the agreement, Russia committed to supplying fuel for Bushehr for ten years and Iran committed to returning the spent fuel to Russia. Reportedly, the original 1992 nuclear cooperation agreement between Russia and Iran stipulated that Russia would supply fuel for the Bushehr reactor "for the entire lifespan of the nuclear power plant." See Mark Hibbs, "Iran's Russia Problem," Carnegie Endowment for International Peace, July 7, 2014.

[22] See the nuclear fuel cycle simulation system published by the IAEA (http://infcis.iaea.org/NFCSS/NFCSSMain.asp?RightP=Calculation&EPage=2&Refresh=0&ReactorType=1).

▶ **Read also:** https://www.iranwatch.org/our-publications/weapon-program-background-report/iran-nuclear-milestones-1967-2017

## China said to speed up move to more survivable nuclear force

**By Robert Burns** (AP National Security Writer)

Source: https://abcnews.go.com/Politics/wireStory/china-speed-move-survivable-nuclear-force-76176562

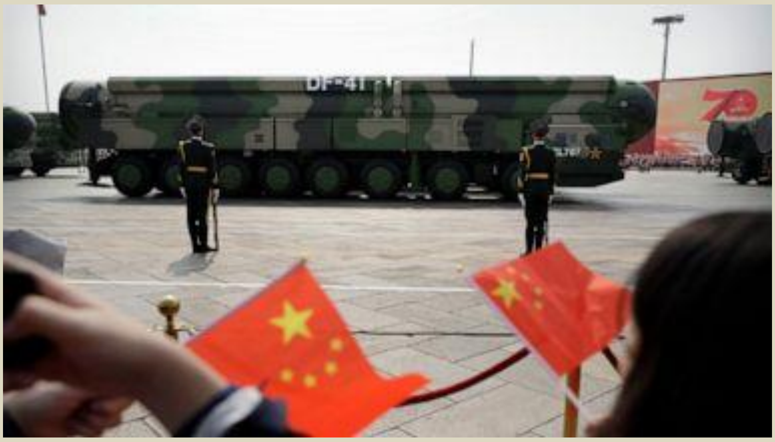
Mar 01 – China appears to be moving faster toward a capability to launch its newer nuclear missiles from underground silos, possibly to improve its ability to respond promptly to a nuclear attack, according to an American expert who analyzed satellite images of recent construction at a missile training area.

Hans Kristensen, a longtime watcher of U.S., Russian and Chinese nuclear forces, said the imagery suggests that China is seeking to counter what it may view as a growing threat from the United States. The U.S. in recent years has pointed to China's nuclear modernization as a key justification for investing hundreds of billions of dollars in the coming two decades to build an all-new U.S. nuclear arsenal.

There's no indication the United States and China are headed toward armed conflict, let alone a nuclear one. But the Kristensen report comes at a time of heightened U.S.-China tensions across a broad spectrum, from trade to national security. A stronger Chinese nuclear force could factor into U.S. calculations for a military response to aggressive Chinese actions, such as in Taiwan or the South China Sea.

The Pentagon declined to comment on Kristensen's analysis of the satellite imagery, but it said last summer in its annual report on Chinese military developments that Beijing intends to increase the peacetime readiness of its nuclear forces by putting more of them in underground silos and operating on a higher level of alert in which it could launch missiles upon warning of being under attack.

"The PRC's nuclear weapons policy prioritizes the maintenance of a nuclear force able to survive a first strike and respond with sufficient strength to inflict unacceptable damage on an enemy," the Pentagon report said.



More broadly, the Pentagon asserts that China is modernizing its nuclear forces as part of a wider effort to build a military by mid-century that is equal to, and in some respects superior to, the U.S. military.

China's nuclear arsenal, estimated by the U.S. government to number in the low 200s, is dwarfed by those of the United States and Russia, which have thousands. The Pentagon predicts that the People's Liberation Army Rocket Forces will at least double the size of its nuclear arsenal over the next 10 years, still leaving it with far fewer than the United States.

China does not publicly discuss the size or preparedness of its nuclear force beyond saying it would be used only in response to an attack. The United States, by contrast, does not rule out striking first, although President Joe Biden in the past has embraced removing that ambiguity by adopting a "no first use" policy.

This satellite image provided Maxar Technologies, taken April 17, 2019, shows one of the underground missile silos under construction at a missile training range in north-central China. (Satellite image ©2021 Maxar Technologies via AP)

Kristensen, an analyst with the Federation of American Scientists, said the commercial satellite photos he acquired appear to show China late last year began construction of 11 underground silos at a vast missile training range near Jilantai in north-central China. Construction of five other silos began there earlier. In its public reports the Pentagon has not cited any specific number of missile silos at that training range.

These 16 silos identified by Kristensen would be in addition to the 18-20 that China now operates with an older intercontinental ballistic missile, the DF-5.

“It should be pointed out that even if China doubles or triples the number of ICBM silos, it would only constitute a fraction of the number of ICBM silos operated by the United States and Russia,” Kristensen wrote on his Federation of American Scientists’ blog. “The U.S. Air Force has 450 silos, of which 400 are loaded. Russia has about 130 operational silos.”

Nearly all of the new silos detected by Kristensen appear designed to accommodate China's newer-generation DF-41 ICBM, which is built with a solid-fuel component that allows the operator to more quickly prepare the missile for launch, compared to the DF-5's more time-consuming liquid-fuel system. The DF-41 can target Alaska and much of the continental United States.

China already has a rail- and road-mobile version of the DF-41 missile.

“They’re trying to build up the survivability of their force,” by developing silo basing for their advanced missiles, Kristensen said in an interview. “It raises some questions about this fine line in nuclear strategy,” between deterring a U.S. adversary by threatening its highly valued nuclear forces and pushing the adversary into taking countermeasures that makes its force more capable and dangerous.

“How do you get out of that vicious cycle?” Kristensen asked.

Frank Rose, a State Department arms control official during the Obama administration, said recently there is little prospect of getting China to join an international negotiation to limit nuclear weapons. The Trump administration tried that but failed, and Rose sees no reason to think that will change anytime soon.

“They're not going to do it out of the goodness of their heart,” he said, but they might be interested in talking if the United States were willing to consider Chinese concerns about related issues like U.S. missile defenses.

Rose says China's main interest is in building up its non-nuclear force of shorter- and intermediate-range missiles, which, combined with a cyberattack capability and systems for damaging or destroying U.S. satellites, could push the United States out of the western Pacific. This would complicate any effort by the United States to intervene in the event Beijing decided to use force against Taiwan, the semi-autonomous democracy that Beijing views as a renegade province that must eventually return to the communist fold.

## Israeli Nukes Threaten World Security: Iranian Envoy

Source: https://www.tasnimnews.com/en/news/2021/03/06/2464820/israeli-nukes-threaten-world-security-iranian-envoy

Mar 06 – In a statement addressed to the International Atomic Energy Agency’s Board of Governors, Kazem Gharibabadi said the “development of a clandestine nuclear weapon program by this regime (Israel) poses a continuing serious threat not only to the security and stability of the region and the world, but also to the effectiveness and efficiency of the NPT and the Agency's safeguards regime.”

All in the Middle East region, except the Israeli regime, are parties to the nuclear Non-Proliferation Treaty (NPT) and have undertaken to accept the Agency's comprehensive Safeguards, he added, saying Israel is also not a party to any other major treaties governing weapons of mass destruction (WMD).

The Iranian envoy further said despite many resolutions adopted by the United Nations General Assembly and the IAEA over decades about Israel’s nuclear capabilities and the associated threats, the regime regrettably continues to ignore the international community by downplaying the significance of the NPT and refusing to place all its nuclear facilities and activities under the IAEA’s comprehensive safeguards regime.

“Ironically, Israel is now even enjoying a more preferential treatment as compared with that of the nuclear weapon states, since they are members to the NPT and have several obligations specifically under Articles I and VI of the Treaty,” Gharibabadi added.

He also criticized as a “clear contradiction” the fact that Israel, a non-member to the NPT, enjoys the full rights and privileges of the IAEA due to its membership while at the same time, it considers itself free from any responsibility and participates in all deliberations of the agency related to the NPT members.

“Such a situation has given this regime the audacity to ridicule the authority and mandate of the Agency in preventing the diversion of its nuclear materials and activities,” he added, Press TV reported.

“Most importantly, this regime has become so cynically bold as to manipulate the realities and criticize other members of the NPT on the account that they have obligations due to their membership in the Treaty, but Israel has not. This is a very serious shortcoming and failure in the work of the Agency, which should be addressed properly.”

Gharibabadi warned that overlooking such an important issue directly affects regional and international peace and stability, challenges the established global disarmament and arms control norms, and damages the credibility and viability of the current disarmament and arms control architecture, including the IAEA and its safeguards regime.

He urged the IAEA to take a clear stand on unacceptability of the Israeli regime’s remaining outside the NPT framework and its continuing defiance to placing all its nuclear activities and facilities under the UN nuclear agency’s comprehensive safeguards system.

“The Agency has no choice but to take appropriate measures to ensure that Israel places all its nuclear installations under the Agency’s safeguards and accedes to the Non-Proliferation Treaty as a non-nuclear weapon party,” the Iranian diplomat pointed out, Press TV reported.

He said it is an irony that the IAEA, its Secretariat, the Board of Governors and the General Conference are all concentrating on the NPT members “while the chronic strategic mistake is to overlook Israel’s nuclear materials and activities in the volatile region of the Middle East.”

“Doesn’t the policy of silence and negligence about Israel’s nuclear program and the inaction policy in this regard send a negative message to the members of the NPT, meaning that being a member of the Treaty equals accepting the most robust monitoring and verifications, while being outside the Treaty means to be free from any obligation and criticism, and even be rewarded”?!” Gharibabadi asked.

**EDITOR’S COMMENT:** This article reveals what is called the “Iranian humor”! The moment they emphatically pursue the aquizition of nuclear weapons they accuse another country that already has a nuclear arsenal that is violating the NPT. The solution to the problem is rather simple: Iran will not wipe out Israel with a missile storm and Israel will not turn Iran into a radioactive dessert following retaliation of first strike. Same applies if Iran one day will announce that it has two or three or more nuclear bombs. Life is too short to deal with stupid rooster fights that affect the survival and the well being of populations in between. Humor is good; so, let us keep it that way!

## How Nuclear Power Has Navigated COVID-19’s Critical Infrastructure Threats

**By Gaoshan Li, et al.**

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/how-nuclear-power-has-navigated-covid-19s-critical-infrastructure-threats/

Mar 04 – Nuclear accounts for 20 percent of electricity production in the United States today and is therefore part of the nation’s critical infrastructure. The nuclear industry’s response to the ongoing and evolving COVID-19 crisis has been largely ad hoc, based on generic pandemic plans. From regulatory oversight to day-to-day plant operations, most pandemic mitigations have been reactionary rather than proactive. And yet, at least for the time being, the industry appears to be performing admirably under adverse and unprecedented conditions.

Our team looked, first and foremost, at the health and safety of personnel involved in the nuclear industry, from plant workers to regulators, and from reactor operators to instructors. We also considered cybersecurity in the context of massively expanded work-from-home settings. Finally, we examined the pandemic impact on the industry’s infrastructure, including fuel cycle interruptions, supply chain issues, and transportation.

With regard to personnel safety, we found that in addition to expanded leave and telework options, the industry moved to increase protection for essential workers, mostly without any federal guidance. Plants set up temperature screening points, procured PPE and hand sanitizer, enforced social distancing, and mandated intensive cleaning protocols of shared spaces. Outage tasks and staffing were reduced, preventative maintenance was postponed, and essential workers were subjected to extensive questions about travel and other possible exposure.

The Nuclear Regulatory Commission moved all possible activities to remote, including, perhaps controversially, inspections. The agency’s overall emphasis was on monitoring, making information available online, shifting application processes to online portals, and providing increased flexibility with regard to schedules and shifts. Most prominently, the NRC approved multiple exemptions to work hours, which allows for longer (and fewer) shifts, reducing personnel overlap, while assuring Fitness for Duty (FFD) requirements. Operator training and requalification seems to have been only minimally impacted. The few reported outbreaks occurred among transient, temporary workers and likely originated in the common practice of worker cohabitation.

In terms of infrastructure, our team found minimal pandemic impact. The long refueling cycle characteristic for nuclear plants greatly assisted the industry’s resilience to supply chain disruptions during the first 10 months of the pandemic. As the pandemic enters its second year, however, we are likely to see more of an impact, as refueling becomes necessary, and maintenance outages cannot be deferred indefinitely.

Our group recognizes the successes of the nuclear industry in navigating this public health crisis, but we must not lose sight of the fact that the pandemic will likely get worse before it gets better. We must remain vigilant against complacency and maintain a “healthy sense of uneasiness”: some “near misses” should serve as warnings for the future. Going forward, we recommend prioritizing the following:

- Add a systematic approach to testing to the nuclear industry's COVID mitigation strategy. Without adequate testing, triggering sequestration (where the typical crew rotations are stopped and fewer crews maintain rotation and remain sequestered on-site) might prove ineffective.
- Return NRC inspections to in-person and on-site, as there is valid concern for the effectiveness of virtual/online inspections.
- Subsidize separate housing for workers to prevent outbreaks and promote worker health and morale.
- In the light of the recent IT security breaches of federal agencies, pay extra attention to our work-from-home cybersecurity infrastructure. The nuclear industry should regularly probe their employees' cybersecurity practices, and consider new challenges arising from an environment of "smart" home devices.
- The NRC should continue tracking the effectiveness of exemptions and reliefs granted to licensees. A "readiness crisis" from changes in annual force-on-force drill requirements, e.g., may not be fully apparent until the NRC restarts triennial force-on-force drill site assessments.
- Continue efforts to prioritize the development of domestic fuel sources, proactively invest in Gen IV and advanced reactor designs with the explicit intention of hardening the U.S. electrical grid against disruptions of any kind.

Since the future of COVID-19 is still uncertain and the next pandemic will likely be very different, we should approach pandemic preparedness with a flexible mindset. We may not know how the next challenge to the nuclear industry will look, but we can proactively prepare for the conditions on the ground.

***Gaoshan Li*** *is a Ph.D. student in chemical engineering at Virginia Tech. She received her master's degree in chemical engineering at the Johns Hopkins Whiting School of Engineering and bachelor's degree in chemical engineering from the Rose-Hulman Institute of Technology.*

## Armenia's nuclear power plant is dangerous. Time to close it.

**By Brenda Shaffer**

Source: https://thebulletin.org/2021/03/armenias-nuclear-power-plant-is-dangerous-time-to-close-it/

Mar 05 – In late 2020, the Armenian government announced that its Metsamor nuclear power plant would close for five months in 2021 to attempt significant upgrades. Soon after, the EU urged Armenia to make the closure permanent since the plant "cannot be updated to fully meet internationally accepted safety standards." A major nuclear or radiation accident at Metsamor would not only affect the people of Armenia, but citizens in neighboring Turkey, Georgia, Azerbaijan, Iran, Russia, and southern Europe. Besides, Armenia can meet its energy needs without Metsamor's output, especially as it exports to Iran over half of the plant's electricity. Further, thermal plants and renewable sources could replace what is used domestically. Metsamor does not even help Armenia achieve its declared goal of energy independence, as Russia–Armenia's main energy supplier–provides the country with most of its natural gas, along with nuclear fuel and specialized technicians for the plant. But none of these arguments have swayed Armenia to close Metsamor in the past.

GEORGIA
Kura
Alaverdi
Debed
Kura
LESSER
Ijevan
Gyumri
Vanadzor
Aragats
Lernagagat'
AZERBAIJAN
Hrazdan
Ejmiatsin
Abovyan
Lake Sevan
Vardenis
Hrazdan
Aras
Armavir
YEREVAN
Artashat
CAUCASUS
TURKEY
Goris
MTS
Naxçıvan
(Nakhichevan)
AZER.
Kapan
Aras
IRAN
0 20 40 km
0 20 40 mi
44
45
46
41
40
39

Is there an argument that could work now?

The EU might urge Armenia to consider a closure in light of recent developments. Post-war road, railway, and energy-development plans should increase trade and transportation linkages in the South Caucasus region after the recent conflict between Armenia and Azerbaijan. The new infrastructure and financing provide Armenia with a fresh opportunity to tap newer, safer, and more diverse energy supplies. By closing Metsamor, Armenia would not only contribute to the safety of its own citizens and those in neighboring countries but strengthen peace in the South Caucasus.

**Metsamor nuclear power plant**

Metsamor is located in a major seismic zone close to Armenia's capital, Yerevan, and near Armenia's border with Turkey. The original, Soviet-built plant included two 400 megawatt reactors. Unit 1 began commercial operation in 1977. Both units were closed by the Soviet authorities in 1989, following the Chernobyl accident and the massive Spitak earthquake in

Armenia in 1988, which killed over 25,000 people. In 1995, following Armenia's independence, Metsamor Unit 2 was restarted at 375 megawatts electrical with Russian funding and technical support. The plant's original operating license was supposed to end in 2016, but Yerevan extended it to 2021, and late in 2020 announced its intent to extend the plant's operation even longer. Unit 1 has remained closed.

Metsamor is one of five of the last operating Soviet-era reactors without a containment vessel, which is a requirement of all modern reactors. (The other reactors without containment vessels are located in Russia.) Nuclear fuel for the Metsamor plant is flown in from Russia, with no special announcements to the Armenian public or regional aviation authorities. In contrast, most nuclear fuel is delivered in the world by sea or rail to minimize the impact of potential accidents. Since the restart of Metsamor Unit 2, the reactor's spent nuclear fuel has remained on site. Then-Armenian Deputy of Energy Areg Galstyan stated in 2004 that details on the air shipments of the nuclear fuel were kept secret to "avoid alarming the people."

has had multiple safety upgrades and also dozens of low-level safety incidents, according to the International Atomic Energy Agency. Hakob Vardanyan, Armenia's deputy minister of territorial administration and infrastructure, who oversees the energy sector, explained that upgrade work at Metsamor had fallen behind schedule because Armenian workers have an "acute lack of experience" in nuclear plant construction and repair.

A nuclear or radiation accident at Metsamor would not only affect the majority of the population of Armenia due to its close proximity to the capital, but also citizens in many nearby countries. Further, an accident or leak at the plant, which is located on the Metsamor River, which feeds into to Araz River, would create damage downriver in Azerbaijan and Iran.

### EU efforts to close Metsamor

Since the late 1990s, the EU has repeatedly encouraged Armenia to close Metsamor as part of a program aimed at shutting down nuclear power plants it has viewed as dangerous, including some located in the EU. Indeed, Lithuania, Bulgaria, and Slovakia agreed to shut down their plants as a condition of joining the EU.

Armenia had agreed to close Metsamor by 2004 as part of a 1998 EU agreement. The EU had even supplied Armenia with funds to close the plant and find substitute energy supplies. However, Armenia did not use the funds to transition its energy sector, leading the EU to freeze the loans in 2005. Around that time, Armenian Head of the EU Delegation Alexis Louber underscored the need for closure when he said, "(N)uclear plants should not be built in highly active seismic zones. This plant is a danger to the entire region … we wanted to close it as quickly as possible." Likewise, subsequent formal cooperation agreements between the EU and Armenia, including Armenia's action plan for the European Union Neighborhood Policy in 2006 and the EU-Armenia Comprehensive and Enhanced Partnership Agreement in 2017, have planks on closing and decommissioning Metsamor. The European Union Neighborhood Policy even provided technical assistance for decommissioning and managing radioactive waste. Prior to signing that policy, Armenian Minister of Trade and Economic Development Karen Chshmaritian made clear that Metsamor's closure was a precondition for deepening Armenia's links with the EU. Armenia signed the agreement and subsequently adopted a formal decommissioning plan in 2007. Yet Metsamor has remained operational.

In almost every official report related to the European Union Neighborhood Policy implementation, the EU emphasized that it wanted Armenia to close Metsamor. For example, the 2011 European Union Neighborhood Policy Country Progress Report-Armenia states, "The EU continues to request the closure of Metsamor Nuclear Power Plant as soon as possible, as it cannot be upgraded to meet internationally recognized nuclear safety standards."

The next major agreement between the EU and Armenia was the 2017 EU-Armenia Comprehensive and Enhanced Partnership Agreement. This agreement states that both sides will cooperate on "the closure and safe decommissioning of Metsamor nuclear power plant and the early adoption of a road map or action plan to that effect, taking into consideration the need for its replacement with new capacity to ensure the energy security of the Republic of Armenia and conditions for sustainable development."

Meanwhile, as Armenia signed various agreements with the EU to close and decommission the plant, it also negotiated other agreements with Russia to extend the reactor's life. Then in March 2014, the Armenian government formally extended Metsamor's operation. Later, while negotiating the 2017 Partnership Agreement mentioned earlier, then-President of Armenia Serzh Sargsyan stated that the agreement with the EU had not required Metsamor's closure, despite the explicit commitment in the agreement.

Fast forward to December 2020, when the European Commission reaffirmed the EU position: "The nuclear power plant located in Metsamor cannot be upgraded to fully meet internationally accepted nuclear safety standards, and therefore requires an early closer and safe decommissioning. It is necessary to rapidly adopt a roadmap or action plan to address this, taking into consideration the need to ensure Armenia's energy security and conditions for sustainable development."

**Armenia's energy security allows Metsamor's closure**

Armenia has a unique energy market with relatively small consumption of electricity and a large proportion of its electricity exported, mostly to Iran. Armenia has several options for reducing its electricity needs and finding substitutes for Metsamor's output, meaning that Armenia could close its nuclear power plant and still provide reliable energy for its population.

Most energy in Armenia is used for residential purposes and transportation, with only 15 percent consumed by industry. Armenians primarily use natural gas, which accounts for 65 percent of the country's energy consumption. Armenia's relatively mild summers mean that relatively little energy is needed for cooling. As a result, the country's per-person electricity consumption is less than half that of Europe's.

Armenia could provide reliably for its energy needs without the output from its nuclear power plant. Today, Armenia exports over half of Metsamor's electricity to neighboring Iran. If these exports were ended, the remaining domestic needs could be met by building one additional thermal-powered electricity plant.

Armenian officials point to energy independence as a key motivation for Metsamor's ongoing operation. They categorize its output as domestically produced energy, without acknowledging that Russia supplies all of its fuel or that the plant's most complicated work is performed by Russian specialists under the direction of Russian state entities. Since Armenia also imports more than 80 percent of its natural gas from Russia, and the Russian energy corporation Gazprom owns Armenia's gas network, keeping Metsamor open actually represents further dependence on Moscow, rather than less. In fact, Armenia's energy security could be improved by diversifying its energy suppliers and supplies. A new thermal plant could have dual-fuel capacity, enabling a quick transfer to liquid fuel (such as heavy oil or diesel) or to coal, thereby reducing its dependence on natural gas. Armenia could then stockpile back-up fuel or coal and quickly transfer to the stored energy without major disruption to electricity supplies. Armenia also has the ability to increase its hydroelectric generation.

Armenia can significantly lower its energy consumption through greater energy efficiency. Moreover, Armenia's energy demand will decrease in 2021 because it lost control of territories in neighboring Azerbaijan in the 2020 war, where it had provided electricity and gas until late 2020.

**Regional peace initiatives enable new energy trade**

Armenia plans to retain and upgrade its nuclear power plant, despite commitments to the EU to close it. The Armenian Energy Sector Development Strategic Program to 2040 states that "the government will stay committed to the policy to maintain nuclear power plant in the country's generation mix." Within Armenia, there is little public opposition to the plant, despite its lack of modern safety measures and proximity to a third of the country's population. Indeed, Armenian officials frequently note their national pride at being the only country in the South Caucasus to operate a nuclear power plant. Financial factors also likely play a role. The main costs in nuclear power plants lie in their construction and

decommissioning, while operating costs, including fuel, are relatively low. Russia also grants loans to Armenia to cover many of the costs.

During the five months of 2021 in which Metsamor is scheduled to shut down, the EU might seize the opportunity to remind Armenia of its commitments to close the plant altogether. Instead of investing in upgrades, Armenia could put the funds towards building an additional thermal plant. This would safeguard people throughout the region and strengthen the post-war peace process that includes new railway and road linkages and potentially new energy trade. Such an effort would emphasize regional cooperation, including among representatives of Armenia and Azerbaijan

With new roads, new railways, and possibly new energy pipelines in the region, Armenia would be able to diversify its energy supplies. For instance, the planned new rail connections would enable Armenia to import fuel and coal that could be stockpiled as backup to its natural-gas-fired generation. With this increased supply and source diversification, Armenia would actually improve its energy security. In the end, closing Metsamor could improve the physical security of Armenians and their European neighbors while improving Armenia's energy security.

At a minimum, the EU should require that Armenia install an early warning system that would notify its neighbors and EU headquarters in Brussels of leaks or accidents at the Metsamor plant. The EU, the Organization for Security and Co-operation in Europe Minsk Group, the US State Department, and the US embassy in Yerevan could sponsor and support this process.

Following the Fukushima Daiichi nuclear disaster in Japan, Germany and other key EU states shut down their nuclear power production. Also, the EU has succeeded in closing dangerous Soviet era plants among its new members. However, EU citizens remain in danger when problematic plants in their neighborhood remain operational. The EU now has an opportunity to remove one of these dangers while strengthening regional cooperation, but only if it convinces Armenia to scrap plans to repair Metsamor in favor of shutting it down altogether.

***Brenda Shaffer*** *is an international energy and foreign policy specialist and faculty member of the U.S. Naval Postgraduate School. She also is a Senior Advisor for Energy at the Foundation for Defense of Democracies think tank and a Senior Fellow at the Atlantic Council's Global Energy Center in Washington, DC.*

## Bill Gates's next-gen nuclear plant packs in grid-scale energy storage

Source: https://newatlas.com/energy/natrium-molten-salt-nuclear-reactor-storage/

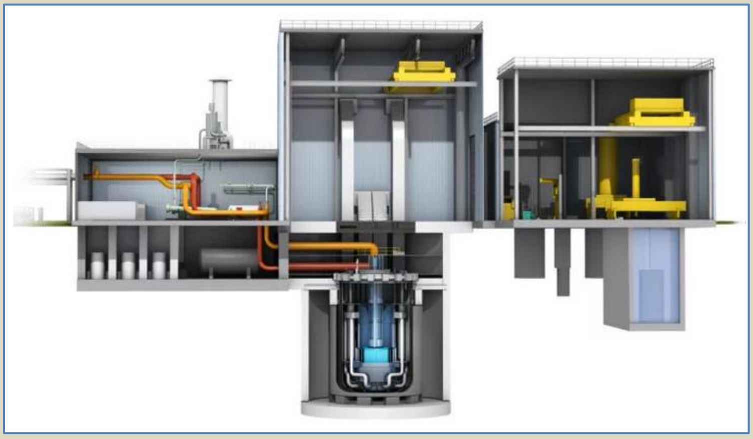
Natrium's advanced nuclear reactor design, which will be up and running as a full-scale trial plant in the late 2020s, also stores several times more energy than most grid scale batteries for rapid load response – Natrium

Mar 08 – Wind, solar, geothermal, hydro, wave energy ... Renewable sources are a crucial pillar of any plan to decarbonize the world's energy generation industries and eliminate fossil fuel use. But for many reasons – intermittency, location dependency, land requirements, and others – they can't do it alone.

To fully remove greenhouse gases from the world's energy sectors, there needs to be a cheap, scalable form of zero-emissions energy that can reliably produce power 24/7/365. All the better if it can rapidly ramp its output up and down to help the power grid cope with load spikes and interruptions in renewable energy supplies. The best candidate to fill this role right now is advanced nuclear power.

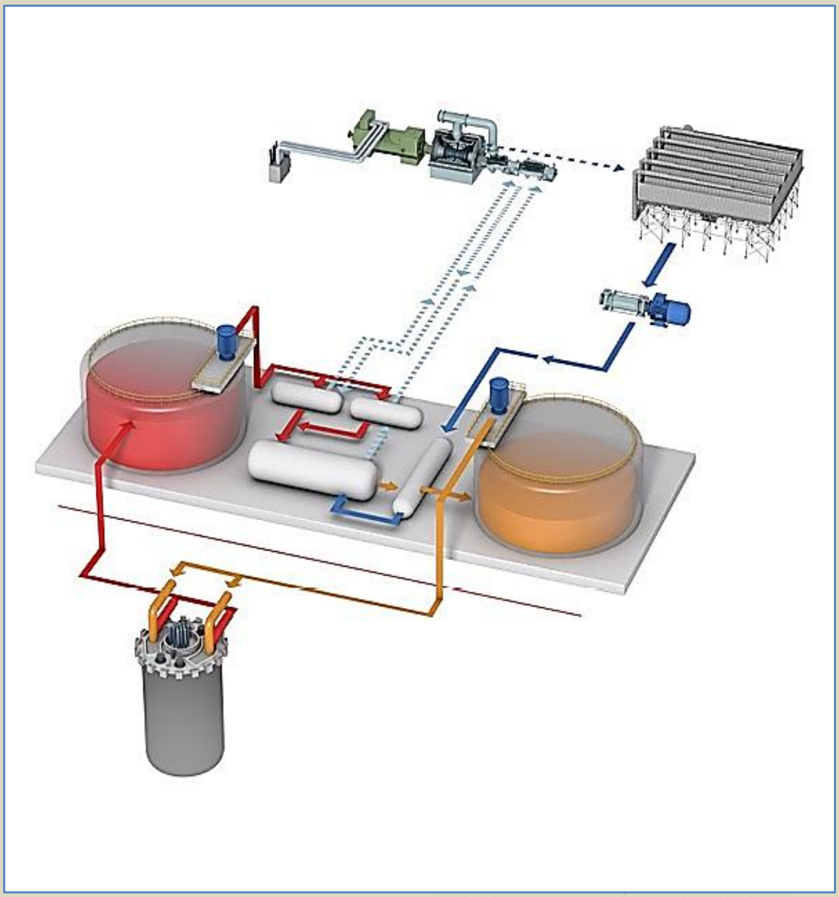
While nobody wants their back yard to become synonymous with Chernobyl or Fukushima, nuclear is demonstrably one of the safest forms of energy generation. Where coal and oil-derived energy cause 24.6 and 18.4 fatalities per terawatt of energy supplied, nuclear power has caused just 0.07 – and that includes the high-profile disasters that have led to its sullied reputation.

Considering the projected death toll of a 2°C temperature rise – somewhere between 300 million and 3 billion premature deaths spread over one to two centuries – the fourth generation of nuclear power is well and truly back on the table, and with many decades of development, advanced modeling and materials technology on its side, it's likely set to improve its already excellent safety record.



One promising initiative that has been backed by heavy private investment as well as the US Department of Energy is a collaboration between Bill Gates's Terrapower and GE Hitachi Nuclear Energy. Natrium (latin for sodium) is getting the chance to demonstrate its "cost-competitive, sodium fast reactor with a molten salt energy storage system" at proper commercial scale thanks in part to a US$80 million DoE grant announced in October.

The sodium fast reactor is designed to run 24/7 at its maximum 345 MWe capacity – Natrium



Natrium's demonstration plant will be fully operational and connected to the power grid in its as-yet-unknown location by the mid to late 2020s. Its fast-neutron reactor will use high-temperature liquid sodium as its reactor coolant instead of water.

One of sodium's key advantages is the huge 785-Kelvin temperature range between its solid and gaseous states; water offers only a 100-Kelvin range, so it needs to be pressurized in order to handle higher amounts of heat energy. High levels of pressure can have explosive consequences, and they also greatly increase the cost of the plant, as nuclear-grade high pressure components are not cheap.

The molten salt thermal energy storage attached to the Natrium generator holds ten times as much on-demand energy as the biggest grid-scale battery projects on the planet – Natrium

Liquid sodium will transfer an impressive amount of heat away from the reactor at normal atmospheric pressures, with the added bonus that it won't dissociate into hydrogen and oxygen, so Fukushima-style hydrogen explosions are out of the question. It's also non-corrosive, sidestepping an issue that puts a question mark over molten salt reactors.

Like many of the next-generation nuclear reactors under development, the Natrium design will use High-Assay, Low Enriched Uranium (HALEU) as its nuclear fuel. Where natural uranium comes out of the ground containing around 0.7 percent of the U-235 isotope that's split to generate nuclear energy, and traditional Low Enriched Uranium (LEU) nuclear reactor fuel is enriched by centrifugal processes or gas diffusion to contain 3-5 percent U-235, HALEU is further enriched, between 5 and 20 percent. For comparison, nuclear weapons need uranium enriched to more than 90 percent.

HALEU fuel can be produced by reprocessing the spent fuel from traditional nuclear power plants, and its higher grade improves reactor performance and efficiency to the point where it allows advanced reactors to be much smaller than LEU plants. Natrium says it should be four times more fuel efficient than light water reactors.

In terms of safety, the control rods will drop by themselves due to gravity in the event of a power outage, and the natural circulation of the air will function as emergency cooling. Thanks to the liquid sodium design, the plant doesn't need a huge containment shield like light water reactors do, and the design puts the reactor underground, again boosting the safety factor while cutting down costs.

The Natrium plant is designed to run at 100 percent output, 24/7, outputting a constant 345 MWe in the form of heat. This heat is transferred out through the liquid sodium cooling system and transferred to a separate molten salt thermal energy storage system similar to what's been proven in many direct solar plants around the world. At the other end of this storage system is a set of steam turbines that can take that constant power and generate enough electricity to power somewhere around 225,000 homes.

And here's where the Natrium design packs a massive extra punch; that storage system means the Natrium plant can react to demand spikes or intermittent renewable energy supply drops by harnessing that stored heat and ramping its turbines up to 150 percent of the nominal reactor power, pumping out 500 MWe for as much as 5.5 or more hours.

That represents nearly a gigawatt-hour of bonus on-demand energy storage; vastly more than even the largest grid-scale battery projects under development. This is an enormous advantage, particularly in the context of decarbonization, where load-reactive systems like this will play a critical role supporting renewable energy sources through the peaks and troughs in their less predictable generation cycles.

The DoE demo plant funding is obviously excellent news for Natrium, which now gets to develop and prove its capabilities before moving to roll similar plants out at scale, which will be significantly larger and more efficient to boot. It's also somewhat of a payback for Terrapower, which was preparing to build an experimental nuclear reactor outside Beijing to trial and demonstrate its separate Traveling Wave Generator technology when US Government sanctions on technology deals with China forced it to abandon the project in 2019.

If it all works out well, the Natrium design promises to be fast to build and commission, and to use far less nuclear-grade concrete than traditional designs – a huge factor in keeping the cost down and reducing the "green premium" on emissions-free energy. Will designs like these helps put some shine back on nuclear power? Opportunities for these companies will be enormous as fossil fuels are scaled down. Time will tell.

## IAEA says Iran starts enriching uranium with third cascade of advanced IR-2m machines at Natanz

Source: https://www.globalsecurity.org/wmd/library/news/iran/2021/iran-210308-presstv02.htm

Mar 08 – Iran has started enriching uranium with a third cascade, or cluster, of advanced IR-2m centrifuges at its Natanz nuclear facility, the International Atomic Energy Agency (IAEA) tells its members.

"On 7 March 2021, the Agency verified ... that: Iran had begun feeding natural UF6 into the third cascade of 174 IR-2m centrifuges," the UN nuclear agency said in a Monday report obtained by Reuters, referring to uranium hexafluoride, the feedstock for centrifuges.

"The fourth cascade of 174 IR-2m centrifuges was installed but had yet to be fed with natural UF6; installation of a fifth cascade of IR-2m centrifuges was ongoing; and installation of a sixth cascade of IR-2m centrifuges had yet to begin," it added.

Iran's representative to the Vienna-based organizations said in February that the country had installed new cascades of advanced centrifuges at two nuclear sites in Natanz and Fordow to increase enrichment capacity.

**"Thanks to our diligent nuclear scientists, two cascades of 348 IR2m centrifuges with almost 4 times the capacity of IR1 are now running with UF6 successfully in Natanz," Kazem Gharibabadi said in a post on his Twitter account.**

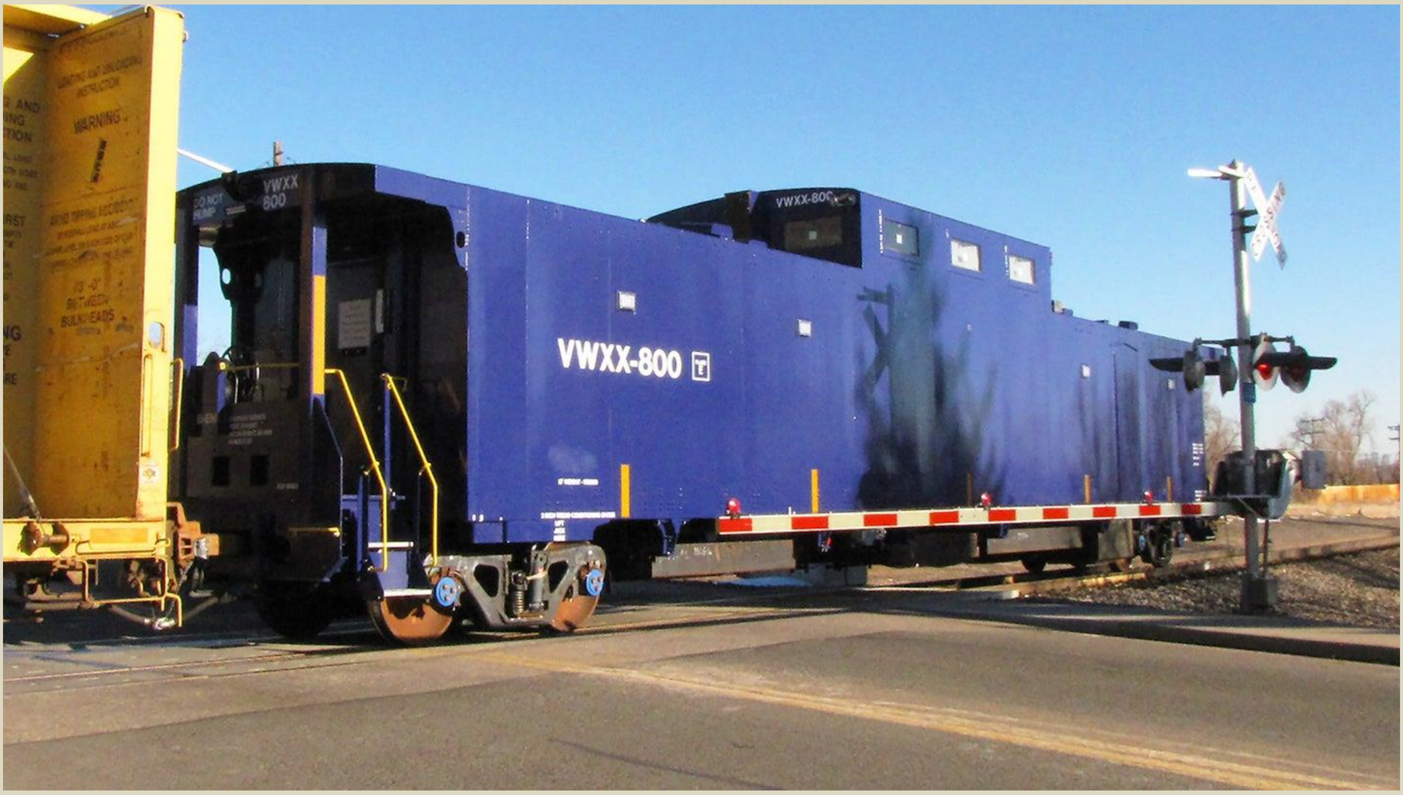
Back in May 2018, former US president Donald Trump pulled Washington out of the multilateral nuclear agreement, officially known as the Joint Comprehensive Plan of Action (JCPOA), reached between Iran and major world states in 2015 and adopted the so-called maximum pressure campaign against Iran with the declared aim of forcing Tehran to negotiate a new deal.

Iran remained fully compliant with the JCPOA for an entire year but as the remaining European parties failed to fulfill their end of the bargain, Tehran began in May 2019 to scale back its JCPOA commitments under Articles 26 and 36 of the accord covering Tehran's legal rights.

In one of its latest steps away from the deal, Iran on January 4 announced the beginning of the process to enrich uranium to 20-percent purity at Fordow to reciprocate the American withdrawal and the European failure.

## Wait, This Mysterious Heavily-Armored Blue Train Caboose Belongs to The Navy?

Source: https://www.thedrive.com/the-war-zone/39654/wait-this-mysterious-heavily-armored-blue-train-caboose-belongs-to-the-navy



## Barakah: first unit to provide power to homes 'soon', as second reactor gets licence

Source: https://www.thenationalnews.com/uae/government/barakah-first-unit-to-provide-power-to-homes-soon-as-second-reactor-gets-licence-1.1180753

Mar 09 – The UAE's nuclear regulator has issued a licence to switch on Barakah's second reactor, officials announced on Tuesday. Barakah nuclear plant's first reactor was connected to the power grid in August last year, and Unit 1 reached 100 per cent power in December.

Now, the plant operators have permission to switch on the second of four units in the coming days.

The Federal Authority for Nuclear Regulation (Fanr) regulates the nuclear plant at Barakah, which is run by Nawah, a subsidiary of Emirates Nuclear Energy Corporation (Enec).

Following the issuing of the licence, Nawah will undertake a period of commissioning to prepare for the commercial operation, during which the fuel load, power ascension and testing processes will take place.

### First reactor close to commercial operations

The first reactor is "very close" to providing commercial supply to the UAE's power grid, said Hamad Al Kaabi, UAE permanent representative to the International Atomic Energy Agency and Fanr's deputy chairman.

"Last year, Unit 1 was licensed by Fanr and started to commission the unit, linked it to the electrical grid, and also increased the power ascension gradually. Now the reactor is connected to grid and provides electricity. We expect the test period will come to an end this year and the commercial use will be announced soon," he said.

He said commercial operations can only start after the testing phase, which is normally around a year, depending on the testing programme.

Some of the Emirati staff behind the nuclear project, which has been more than a decade in the making. (Fanr)

Mr Al Kaabi said Fanr had taken a lot of steps regarding management of nuclear waste in its regulations.

“In the design of the plant, we have many procedures related to where the radioactive waste the placed inside the plant itself. As well, we will store it for 60 years. We have also established a decommissioning fund that includes the management and handling of radioactive waste. “

Overall construction of Barakah has reached more than 95 per cent. The first and second reactor are fully built, while the third and fourth reactors are 94 per cent and 88 per cent complete, respectively.

Once Barakah's four reactors are on line, the plant will deliver reliable electricity for decades, providing about a quarter of the country’s electricity.

Enec previously said the subsequent reduction in fossil fuel use would cut 21 million tonnes of carbon emissions annually. That is the equivalent to taking 3.2 million cars off the roads each year.

The UAE generates about 98 per cent of its domestic power from gas-fired stations, which is expected to steadily fall as Barakah begins to generate power for commercial use.

**UAE exporting expertise**

Countries in the region have sought the UAE’s assistance in developing their nuclear programmes.

Mr Al Kaabi said the UAE was working through the IAEA to provide local expertise to nuclear programmes.

“Our expertise and experience has led to many enquiries from other countries who are interested in developing a nuclear energy,” he said.

“As for Arab countries, we have received some interest to know more about the nuclear energy programme and to establish and communication and co-ordination and training to learn from us.

“Also, in Khalifa University, there is a centre established by the IAEA to develop the infrastructure. It's an important centre to provide more exposure on the UAE's expertise.”

He said Fanr has nearly 260 employees, who have been working in the licensing process and the development of the institution. More than 100 of those are Emiratis, who have trained and developed during the time the UAE advanced its nuclear programme.

### Lessons learnt

This week marks the 10-year anniversary of the disaster at Fukushima Daiichi nuclear disaster in Japan. An earthquake and tsunami in 2011 led to a meltdown at three nuclear units of the nuclear plant and left about 19,000 people dead or missing.

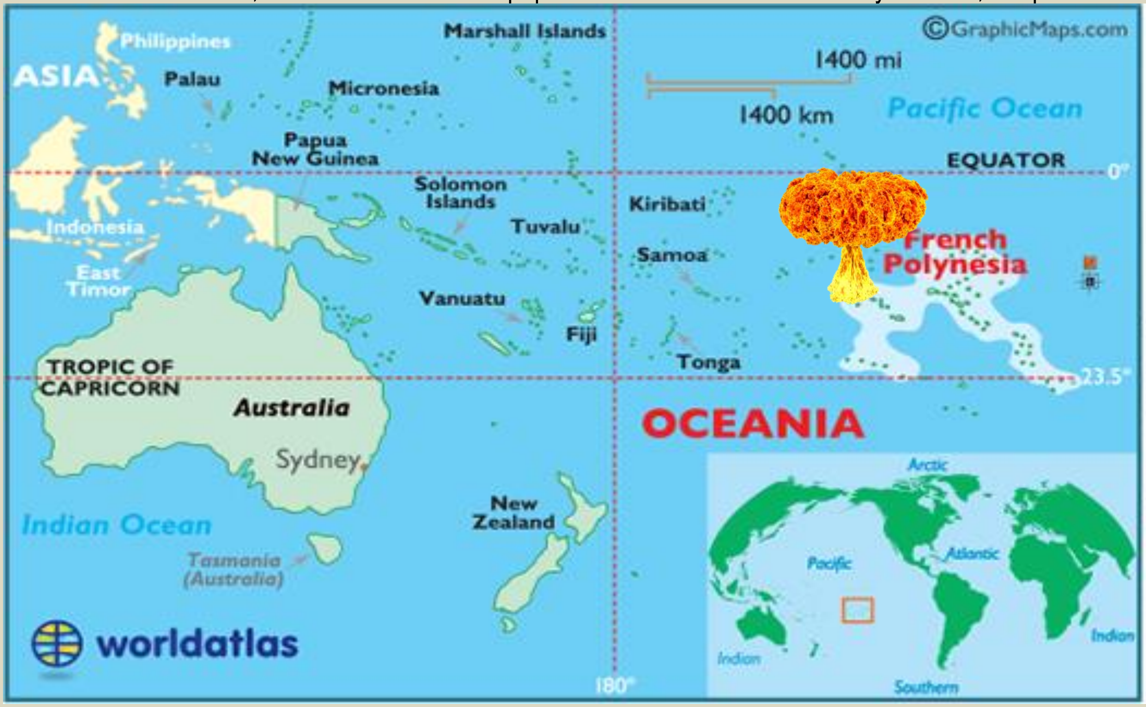
Mr Al Kaabi said at the time of Fukushima, the UAE was in the process of reviewing its licensing application and implemented many of the lessons learnt from that disaster.

“We actually adopted a very systematic approach for the stress test that resulted in the Enec and Nawah proposing additional improvements in the design, based on lessons learned from Fukushima. These improvements have implemented as part of the lessons process,” he said. He said Fanr would continue to monitor updates and the extraction of any new lessons.

## French nuclear tests infected 'almost entire Polynesian population'

Source: https://www.dailystar.com.lb/Life/Health/2021/Mar-09/518262-french-nuclear-tests-infected-almost-entire-polynesian-population-report.ashx

Mar 09 – France concealed the levels of radioactivity that **French Polynesia** was exposed to during French nuclear tests in the Pacific from 1966-1996, with almost the "entire population" of the overseas territory infected, a report said Tuesday.



Online investigation site Disclose said it had over two years analysed some 2,000 pages of French military documents declassified in 2013 by the defence ministry concerning nuclear tests on the archipelago.

It worked alongside the British modelling and documentation firm Interprt as well as the Science and global security programme of the University of Princeton in the United States, it said.

For the Centaur test carried out in July 1974, "according to our calculations, based on a scientific reassessment of the doses received, approximately 110,000 people were infected, almost the entire Polynesian population at the time," it said.

Using the modelling of toxic clouds to back up the findings, Disclose said it also showed how "French authorities have concealed the true impact of nuclear testing on the health of Polynesians for more than 50 years."

It said the investigation was able to reassess the thyroid exposure to radioactive doses of the inhabitants of the Gambier Islands, Tureia and Tahiti during the six nuclear tests considered to be the most contaminating in the history of French tests in the Pacific.

"Our estimates are between two and 10 times higher than those made by the French Atomic Energy Commission in 2006," Disclose said.

Disclose said its interpretation of existing data was different to that of the French Alternative Energies and Atomic Energy Commission (CEA).

For example, for an aerial nuclear test called Aldebaran carried out in 1966 on the Mururoa atoll, CEA scientists "considered that the local population only drank riverwater but not rainwater".

However, many inhabitants of this archipelago drank rainwater, according to the investigation.

It added the examination of data also showed that CEA estimates of radioactive soil deposits were under-estimated by more than 40 percent.

This CEA study served as the reference for the Compensation Committee for Victims of Nuclear Tests (CIVEN) for studying the files of victims of nuclear tests.

Up until now only 63 Polynesian civilians, excluding soldiers and contractors, have received compensation, according to the investigative media.

## Ten Years after Fukushima, Safety Is Still Nuclear Power's Greatest Challenge

**By Kiyoshi Kurokawa and Najmedin Meshkati**

Source: http://www.homelandsecuritynewswire.com/dr20210309-ten-years-after-fukushima-safety-is-still-nuclear-power-s-greatest-challenge

Mar 09 – Ten years ago, on March 11, 2011, the biggest recorded earthquake in Japanese history hit the country's northeast coast. It was followed by a tsunami that traveled up to 6 miles (10 kilometers) inland, reaching heights of over 140 feet (43.3 meters) in some areas and sweeping entire towns away in seconds.

This disaster left nearly 20,000 people dead or missing. It also destroyed the Fukushima Daiichi Nuclear Power Station and released radioactive materials over a large area. The accident triggered widespread evacuations, large economic losses and the eventual shutdown of all nuclear power plants in Japan. A decade later, the nuclear industry has yet to fully address safety concerns that Fukushima exposed.

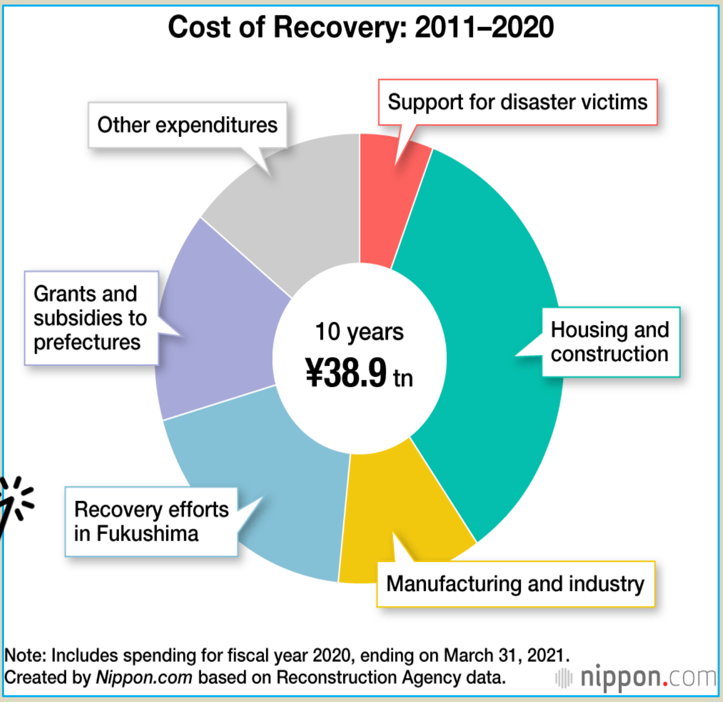
We are scholars specializing in engineering and medicine and public policy, and have advised our respective governments on nuclear power safety. Kiyoshi Kurokawa chaired an independent national commission, known as the NAIIC, created by the Diet of Japan to investigate the root causes of the Fukushima Daiichi accident. Najmedin Meshkati served as a member and technical adviser to a committee appointed by the U.S. National Academy of Sciences to identify lessons from this event for making U.S. nuclear plants safer and more secure.

Those reviews and many others concluded that Fukushima was a man-made accident, triggered by natural hazards, that could and should have been avoided. Experts widely agreed that the root causes were lax regulatory oversight in Japan and an ineffective safety culture at the utility that operated the plant.

These problems are far from unique to Japan. As long as commercial nuclear power plants operate anywhere in the world, we believe it is critical for all nations to learn from what happened at Fukushima and continue doubling down on nuclear safety.

### Failing to Anticipate and Plan

The 2011 disaster delivered a devastating one-two punch to the Fukushima plant. First, the magnitude 9.0 earthquake knocked out off-site electric power. Next, the tsunami breached the plant's protective sea wall and swamped portions of the site.



Note: Includes spending for fiscal year 2020, ending on March 31, 2021.
Created by *Nippon.com* based on Reconstruction Agency data.

Flooding disabled monitoring, control and cooling functions in multiple units of the six-reactor complex. Despite heroic efforts by plant workers, three reactors sustained severe damage to their radioactive cores and three reactor buildings were damaged by hydrogen explosions.

Off-site releases of radioactive materials contaminated land in Fukushima and several neighboring prefectures. Some 165,000 people left the area, and the Japanese government established an exclusion zone around the plant that extended over 311 square miles (807 kilometers) in its largest phase.

For the first time in the history of constitutional democratic Japan, the Japanese Parliament passed a law creating an independent national commission to investigate the root causes of this disaster. In its report, the commission concluded that Japan's Nuclear Safety Commission had never been independent from the industry, nor from the powerful Ministry of Economy, Trade, and Industry, which promotes nuclear power.

For its part, plant operator Tokyo Electric Power Company, or TEPCO, had a history of disregard for safety. The company had recently released an error-prone assessment of tsunami hazards at Fukushima that significantly underestimated the risks.

Events at the Onagawa Nuclear Power Station, located 39 miles (64 kilometers) from Fukushima, told a contrasting story. Onogawa, which was owned and operated by the Tohoku Electric Power Company, was closer to the earthquake's epicenter and was hit by an even larger tsunami. Its three operating reactors were the same type and vintage as those at Fukushima, and were under the same weak regulatory oversight.

But Onogawa shut down safely and was remarkably undamaged. In our view, this was because the Tohoku utility had a deep-seated, proactive safety culture. The company learned from earthquakes and tsunamis elsewhere – including a major disaster in Chile in 2010 – and continuously improved its countermeasures, while TEPCO overlooked and ignored these warnings.

### Regulatory Capture and Safety Culture

When a regulated industry manages to cajole, control or manipulate agencies that oversee it, rendering them feckless and subservient, the result is known as regulatory capture. As the NAIIC report concluded, Fukushima was a textbook example. Japanese regulators "did not monitor or supervise nuclear safety….They avoided their direct responsibilities by letting operators apply regulations on a voluntary basis," the report observed.

Effective regulation is necessary for nuclear safety. Utilities also need to create internal safety cultures – a set of characteristics and attitudes that make safety issues an overriding priority. For an industry, safety culture functions like the human body's immune system, protecting it against pathogens and fending off diseases.

A plant that fosters a positive safety culture encourages employees to ask questions and to apply a rigorous and prudent approach to all aspects of their jobs. It also fosters open communications between line workers and management. But TEPCO's culture reflected a Japanese mindset that emphasizes hierarchy and acquiescence and discourages asking questions.

There is ample evidence that human factors such as operator errors and poor safety culture played an instrumental key role in all three major accidents that have occurred at nuclear power plants: Three Mile Island in the U.S. in 1979, Chernobyl in Ukraine in 1986 and Fukushima Daiichi in 2011. Unless nuclear nations do better on both counts, this list is likely to grow.

**Global Nuclear Safety Grade: Incomplete**

Today there are some 440 nuclear power reactors operating around the world, with about 50 under construction in countries including China, India, Pakistan, Bangladesh, Belarus, Turkey and the United Arab Emirates.

Many advocates argue that in light of the threat of climate change and the increasing need for carbon-free baseload electricity generation, nuclear power should play a role in the world's future energy mix. Others call for abolishing nuclear power. But that may not be feasible in the foreseeable future.

In our view, the most urgent priority is developing tough, system-oriented nuclear safety standards, strong safety cultures and much closer cooperation between countries and their independent regulators. We see worrisome indications in the U.S. that independent nuclear regulation is eroding, and that nuclear utilities are resisting pressure to learn and delaying adoption of internationally accepted safety practices, such as adding filters to prevent radioactive releases from reactor containment buildings with the same characteristics as Fukushima Daiichi.

The most crucial lesson we see is the need to counteract nuclear nationalism and isolationism. Ensuring close cooperation between countries developing nuclear projects is essential today as the forces of populism, nationalism and anti-globalism spread.

We also believe the International Atomic Energy Agency, whose mission is promoting safe, secure and peaceful uses of nuclear energy, should urge its member states to find a balance between national sovereignty and international responsibility when it comes to operating nuclear power reactors in their territories. As Chernobyl and Fukushima taught the world, radiation fallout does not stop at national boundaries.

[*Over 100,000 readers rely on The Conversation's newsletter to understand the world.* Sign up today.]

As a start, Persian Gulf countries should set aside political wrangling and recognize that with the startup of a nuclear power plant in the United Arab Emirates and others planned in Egypt and Saudi Arabia, they have a common interest in nuclear safety and collective emergency response. The entire region is vulnerable to radiation fallout and water contamination from a nuclear accident anywhere in the Gulf.

We believe the world remains at the same juncture it faced in 1989, when then-Sen. Joseph R. Biden Jr. made this perceptive argument:

> A decade ago, Three Mile Island was the spark that ignited the funeral pyre for a once-promising energy source. As the nuclear industry asks the nation for a second look in the context of global warming, it is fair to watch how its advocates respond to strengthened safety oversight. That will be the measure of whether nuclear energy becomes a phoenix or an extinct species.

*__Kiyoshi Kurokawa__ is Professor Emeritus, University of Tokyo.*

*__Najmedin Meshkati__ is Professor of Engineering and International Relations, University of Southern California.*

## Iran Is Starting to Want the Bomb

**By Maysam Behravesh**

Source: https://foreignpolicy.com/2021/03/10/iran-is-starting-to-want-the-bomb/

Mar 10 – On Feb. 8, Iranian Intelligence Minister Mahmoud Alavi, in an interview with Iranian state television, made a veiled threat about his country's pursuit of a nuclear weapon. "The supreme leader [Ayatollah Ali Khamenei] has explicitly said in his fatwa that nuclear weapons are against sharia law and the Islamic Republic sees them as religiously forbidden and does not pursue them," Alavi said. "But a cornered cat may behave differently from when the cat is free. And if they [Western powers] push Iran in that direction, then it's no longer Iran's fault."

The unprecedented public threat captured wide media attention. Domestic critics, particularly hard-liners, slammed President Hassan Rouhani's intelligence minister for harming Iranian interests by undermining Khamenei's religious edict against weapons of mass destruction. Middle East watchers abroad focused on the fatwa factor as well, mostly to demonstrate Iranian leaders' untrustworthiness. Others construed Alavi's statements as a "pressure" tactic to spur the Biden administration into rejoining the 2015 Iran nuclear accord—officially known as the Joint Comprehensive Plan of Action (JCPOA)—or otherwise lifting sanctions.

All these responses misunderstand the real significance of Alavi's "cornered cat" threat. The whole debate over Khamenei's fatwa banning nuclear weapons has always been much ado about nothing; it never really mattered in the first place for either side. (The very fact that world powers engaged in marathon talks with Tehran from 2013 to 2015 to verifiably curb its nuclear program in exchange for economic relief confirms as much.) Far more important is what the comment reflects about an ongoing shift in Iran's thinking about the bomb. Wide swaths of Iranian society, among the public and policymakers alike, seem to increasingly see the weapon not just as an ultimate deterrent but as a panacea for Iran's chronic security problems and challenges to its sovereignty by foreign powers.

Alavi's statement came against a backdrop of repeated national humiliation in the form of a string of embarrassing security breaches and counterintelligence failures. In recent years, Iran has lost Qassem Suleimani, the chief architect of its regional strategy, and seen some of its key military and infrastructural facilities, including at Natanz and Khojir, targeted in a series of mysterious explosions and sabotage operations. The culmination came last November, when Iran's nuclear strategy architect, Mohsen Fakhrizadeh, was assassinated near Tehran.

Picture obtained from the Iranian ISNA news agency on Dec. 16, 2009 shows the test-firing at an undisclosed location in Iran of an improved version of the Sejil 2 medium-range missile which the Islamic republic says can reach targets inside Israel. VAHI REZA ALAEE/AFP via Getty Images

Shortly after the U.S. assassination of Suleimani in January 2020, *Tabnak*—a popular conservative media outlet in Tehran with nationalist leanings—published a rare piece asking its readers about nuclear deterrence and the ways it can advance Iran's national security interests. "Some analysts believe that Iran's possession of a nuclear deterrent will check Israel's regional ambitions, while others maintain that it can deter big powers from stoking tensions and starting new wars in the region," the article read. A similar story in *Alef*—another conservative news source—contended that Washington's "destructive policies" against Iran and "Europeans' inaction" continued to push Tehran to the verge of making the "big decision." "Why should Iran commit to international regulations and refrain from constructing nuclear weapons while its enemies are all equipped with these weapons and threaten to destroy Iran on a daily basis?" asked another analysis published by *Sputnik* in Persian following the drone strike assassination.

These questions and concerns had been a present yet largely marginal part of public debate in Iran ever since its nuclear scientists were targeted for the first time during Mahmoud Ahmadinejad's presidency (2005-2013). It is no accident that self-proclaimed realist theorists such as John J. Mearsheimer, Stephen M. Walt, and his late mentor Kenneth N. Waltz are among the most familiar references and authors whose works and arguments in favor of nuclear deterrence and balance of power have been widely translated into Persian and made available to Iranian news consumers. But it wasn't until after Israel's killing of Fakhrizadeh that popular sympathy for Iran's geopolitical vulnerability and support for nuclear weapons as an effective and sustainable solution to it gained vast traction among the public and ruling elite alike.

"It seems our logical response to this assassination should be a scientific response," Fereydoun Abbasi, the chair of the Iranian parliament's energy committee, said in a December interview, suggesting heightened political proclivity for decisive nuclear capability action among Iranian decision-makers. "So we will take steps toward deepening our scientific and technical knowledge" of nuclear power. Notably, Abbasi himself survived an assassination attempt in 2010 when he was heading the Atomic Energy Organization of Iran. Another commentary run by *Rahborde Moaser*, a state-affiliated strategic news outlet, in December urged Tehran's withdrawal from the Nuclear Nonproliferation Treaty so it could accomplish "sustainable deterrence" against powerful adversaries, a proposal that echoed calls for production of "deterrent weapons" as the "only way" to ensure national security. Other observers have gone so far as to defend the bomb as a prerequisite for economic development in Iran, arguing that nuclear deterrence is the "only option" that can resolve Tehran's chronic "security dilemma" once and for all and enable it to focus on national prosperity. The intelligence minister's "cornered cat" threat was in fact a more explicit expression of these decreasingly marginal and subterranean temptations and tendencies.

In his groundbreaking work *The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy* (2006), the political scientist Jacques E.C. Hymans investigates four various conceptions of national identity held by political leaders—their sense of "what the nation naturally stands for and of how highly it naturally stands" in comparison to others—that ultimately determine their nuclear choices and decisions, from abstention and restraint to threshold nuclearization and full acquisition. He draws special attention to "oppositional nationalism," a certain conception of national identity, driven by fear and pride, that functions as an "explosive psychological cocktail" for nuclear policymaking. Oppositional nationalist leaders "see their nation as both naturally at odds with an external enemy, and as naturally its equal if not its superior," Hymans elaborates, concluding that such leaders "develop a desire for nuclear weapons that goes beyond calculation, to self-expression." By this definition, Khamenei should be a good example of an oppositional nationalist who aspires, in the face of massive international opposition, to elevate his revisionist country into the foremost power in the Middle East.

Yet Khamenei's nuclear decision-making, including his invocation of "heroic flexibility" in 2013 to justify nonproliferation negotiations with world powers, does not fit comfortably in Hymans's "national identity conception" (NIC) model, and the question remains unresolved: Why hasn't Iran gone nuclear yet? The answer does not lie in Khamenei's psychological profile or his nuclear ban fatwa.

A fundamental problem with Hymans's NIC model of nuclear calculus is that it is leader-centric, thus reductionist. By reducing an extremely complex dynamic with manifold variables to a given leader's individual perception of his or her nation and its appropriate place among nations, Hymans in fact neglects the possible presence of such potent inclinations at the collective level—that is, among the public in general and a given state's supporter base in particular. Iran's recent nuclear history offers helpful insights in this respect.

Most foreign-policy analysts attribute the Iranian leadership's 2013 decision—to embark on multilateral nuclear negotiations after an extended period of defiant escalation under Ahmadinejad—to effective international pressure on Khamenei's government, the Obama administration's eventual compromise on demands for uranium enrichment in Iran, or a combination of both. While both arguments are indisputably valid to a certain extent, they overlook powerful domestic-societal drivers of Iran's nuclear policy shift at that historic juncture. In other words, the massive force of public opinion and its prevailing narratives in favor of nuclear diplomacy, which was interrupted by electoral fraud in 2009 but ultimately expressed through the popular election of Rouhani, compelled Iran's top leadership to give diplomacy a decent chance.

The widely held notion that Khamenei wanted talks all along—proponents of which cite his blessing for secret negotiations with the Obama administration in Oman during Ahmadinejad's presidency—is fundamentally flawed. As later manifested by his tactical treatment of the JCPOA and public opposition to the Rouhani administration's proposals about domestic and regional JCPOAs, Khamenei, in fact, favored a pragmatic stopgap to a long-term resolution of the crisis. This cynicism was partly rooted in his deep distrust of the United States but also, and perhaps more importantly, a reflection of the serious concerns Iranian leadership harbored about the JCPOA's transformative potential for instigating domestic political change in Iran. Khamenei and his allies in the Revolutionary Guards feared Iranians' open engagement with the outside world for its impact on his establishment's grip on power.

Now almost eight years on, and under the heavy and humiliating weight of U.S. maximum pressure, the same collective forces that compelled Iran to open up to nuclear compromise are nudging it in the opposite direction, thanks to an incremental resurgence of territorial nationalism across society. And Iran's long-asleep nuclear genie is waking up and dancing its way, to that nationalist tune, out of its bottle.

While there are no public opinion polls to measure Iranians' view of nuclear weaponization or how it may have changed over time since 2013, a new survey organized jointly by the Center for International and Security Studies at the University of Maryland and the Canada-based polling agency IranPoll suggests that anti-compromise views and sentiments have considerably hardened over the past years. Notably, public support for the JCPOA has dropped from 76 percent in August 2015 to 51 percent in February 2021, and 73 percent of respondents endorsed the Strategic Action Plan passed last year by Iran's hard-liner-dominated parliament to systematically reduce its JCPOA commitments unless U.S. sanctions are lifted. Also, 69 percent maintained that "Iran should not hold any talks with the United States until it first returns to the JCPOA and fulfills all of its obligations." Pertinently, more than 88 percent of respondents said they wanted Iran to "fulfill its obligations under the JCPOA after the United States is back in full compliance."

This incremental shift in Iranian public opinion about the nation's nuclear program is as significant as it is unprecedented and a major reason why statements like Alavi's "cornered cat" warning carry considerable strategic weight. Fueled by a growing sense of nuclear injustice and indignation, pro-bomb sentiments in Iran will arguably gain further ground and legitimacy in light of expanding nuclear ventures in Saudi Arabia and Israel, Tehran's chief regional adversaries. Under Crown Prince Mohammed bin Salman's de facto rule, the Saudi nuclear initiative is progressing unimpeded, and Israel is expanding its secret atomic infrastructure in the Negev desert in broad daylight.

The potentially explosive shift in the Iranian national attitude toward nuclear weapons is a direct consequence of the U.S. maximum pressure campaign, from economic strangulation to sabotage operations to targeted assassinations. Washington's decision to exit the JCPOA has served to remove one of Iran's major political obstacles to acquiring the bomb.

Iran has reached a dangerous moment. What if Iran's next leader proves to be a real confrontational nationalist who does not shy away from making the big decision against all odds? What if a confrontation with a militarily superior nemesis, such as the United States or Israel, convinces Iranians and their leaders that nuclear deterrence is no longer a matter of choice but a national security necessity? Because the foreign punishment is perceived as unfair, Iran's societal opposition to nuclear weapons is eroding. If the United States and its regional allies are genuinely determined to prevent Tehran from acquiring nuclear weapons, they need to move beyond conventional reliance on punitive force and consider the unintended strategic consequences of maximum pressure. Otherwise, Alavi's cornered cat may pounce before anyone expects.

***Maysam Behravesh*** *is a research associate at Clingendael, the Netherlands Institute of International Relations, and a Ph.D. candidate in political science at Lund University, Sweden.*

## Explainable AI: A Must for Nuclear Nonproliferation, National Security

Source: http://www.homelandsecuritynewswire.com/dr20210310-explainable-ai-a-must-for-nuclear-nonproliferation-national-security

Mar 10 – As it is with raw human intelligence, so it is with artificial intelligence (AI). We may not know exactly what's going on inside that elaborate black box built by humans, but its decisions can be so accurate that it earns our trust, if not our comprehension. But the need for understanding escalates when the stakes are higher. For national security concerns, it's not good enough to know that a system works; scientists demand to know how and why. That's the foundation for a field of study known as "explainable AI."

## Someone to Watch over AI and Keep It Honest – and It's Not the Public

Source: http://www.homelandsecuritynewswire.com/dr20210310-someone-to-watch-over-ai-and-keep-it-honest-and-it-s-not-the-public

Mar 10 – The public doesn't need to know how Artificial Intelligence works to trust it. They just need to know that someone with the necessary skillset is examining AI and has the authority to mete out sanctions if it causes or is likely to cause harm.

## Fukushima: Ten Years on from the Disaster, Was Japan's Response Right?

**By William Nuttall and Philip Thomas**

Source: http://www.homelandsecuritynewswire.com/dr20210310-fukushima-ten-years-on-from-the-disaster-was-japan-s-response-right

Mar 10 – The world saw something never before caught on camera on March 12, 2011: an explosion ripping the roof off a nuclear power plant – Japan's Fukushima Daiichi. The blast wasn't actually nuclear, it was the result of hot hydrogen gas encountering the cool, outside air during the aftermath of the Tōhoku earthquake and tsunami. But the distinction hardly mattered – something had clearly gone terribly wrong.

A decade on from the tragedy, many people are still mourning the nearly 16,000 people who lost their lives to the tsunami. While no-one died from the radiation after the radiation accident at Fukushima Daiichi, roughly two thousand elderly people died prematurely as a result of their enforced evacuation and undoubtedly many more of the huge number of displaced people experienced distress. In order to minimize suffering in future nuclear accidents, there are important lessons from March 2011 that must be learned.

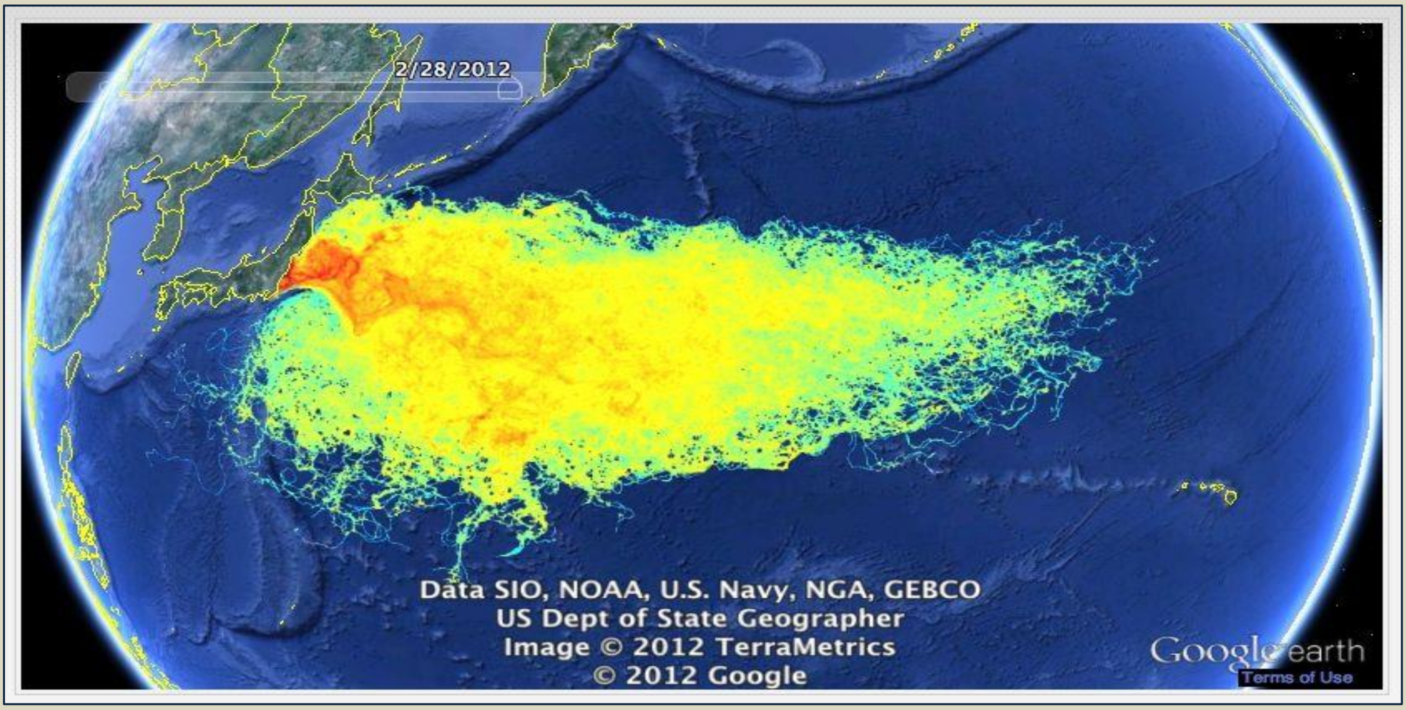
How should a government react when confronted by clear evidence of radioactive material being released into the environment? A precedent was set 25 years before, at Chernobyl in Ukraine. There, authorities evacuated the local population and have kept them away for decades, which was hugely expensive and disruptive for the communities involved.

While Japan was reeling from the natural disaster, the authorities imposed an evacuation order with a radius of 20km around the stricken nuclear plant. A total of 109,000 people were ordered to leave their homes, with a further 45,000 choosing to evacuate from places nearby, which added to the turmoil.

We set out to determine how best to respond to a severe nuclear accident using a science-led approach. Could we, by examining the evidence, come up with better policy prescriptions than the emerging playbook deployed in Ukraine and Japan? Together with colleagues at the universities of Manchester and Warwick, we used research methods from statistics,

meteorology, reactor physics, radiation science and economics and arrived at a surprising conclusion.

Japan probably didn't need to relocate anyone, and the evacuations after Chernobyl involved five to ten times too many people. In fact, because power plants are generally built some distance from towns and cities, very few of even the most severe nuclear accidents would warrant long-term population relocations.


2/28/2012
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
US Dept of State Geographer
Image © 2012 TerraMetrics
© 2012 Google
Google earth
Terms of Use

**The Analysis**

Our team ran a simulation of a Fukushima-style accident at a fictional reactor in southern England and showed that, most likely, only the people in the nearest village would need to move out. That means hundreds of people relocated, rather than tens of thousands.

It's difficult to argue for any relocation after the accident at Fukushima Daiichi in Japan, where the calculated loss of life expectancy from staying put in the worst-affected township, Tomioka, would have been three months – less than Londoners are currently losing to air pollution

Of course, we are not saying nothing should be done, quite the opposite. The University of Bristol researchers had developed the J-value (with "J" standing for judgement) to help arrive at objective answers for safety questions arising from nuclear plants, railways and other infrastructure that improves our lives.

How much should a nuclear power plant spend on protecting its workers? Is it cost-effective to install a new safety system for railway signaling? Should a government be spending more to prevent road deaths? The J-value balances the amount of life expectancy that a safety measure restores against its cost. And it takes the ethical stance that each day of life has the same value for everyone – whether a person is rich or poor, young or old.

In the aftermath of a nuclear accident, the J-value can help prioritize the most useful measures, like cleaning roofs and gutters in towns and cities and reducing radioactive cesium uptake in farmland by adding ferrocyn to cattle feed and replacing contaminated soil.

Why is relocating people rarely one of those? Relocations are not just expensive, they also cause difficult-to-quantify problems for evacuees which can be equally, or more, serious than remaining. The World Health Organization documented the upheaval of the Chernobyl disaster among the relocated community and found a legacy of depression and alcoholism. Across the population, a rise in suicide and substance abuse can shorten evacuees' lives far more than might have been lost to radiation in their old homes. Similar evidence is starting to emerge from Fukushima, especially for male suicide.

**A Greater Threat Looms**

Japan in 2010 was arguably the world leader in civil nuclear power, having opened the first "third generation" nuclear unit at Kashiwazaki-Kariwa in 1996. Mighty conglomerates Toshiba and Hitachi were poised to deliver a nuclear renaissance worldwide. Both have since left the UK with empty spaces where new nuclear power plants were supposed to be.

Hitachi's ambitions for Taiwan (Lungmen) and the US (South Texas) also evaporated, as well as at home in Japan (Shimane). In Japan many, already built, plants remain shutdown.

There is a clear imbalance between the very low risk of a severe nuclear accident that can be expected to kill remarkably few people on the one hand, and the near certainty, on the other, of climate change threatening the futures of all the world's species as a result of the continued burning of fossil fuels. Japan's case illustrates the point.

Carbon-free nuclear power supplied 25% of the country's electricity in 2010, but its share dropped to less than 1% four years after the accident. The shortfall was made up by a 30% rise in the use of coal, oil and natural gas. By 2019, fossil fuels were still providing 70% of Japan's electricity.

Analysts report that Japan could generate almost a third of its energy from renewable sources by 2030. But decarbonizsation could have proceeded even quicker if nuclear power had not been forced from the mix. Though the reaction is understandable – trust was broken.

The sense that something must be done can be powerful amid widespread disaster. The challenge is directing it towards finding the right solutions.

***William Nuttall** is Professor of Energy @ The Open University.*
***Philip Thomas** is Professor of Risk Management @ University of Bristol.*

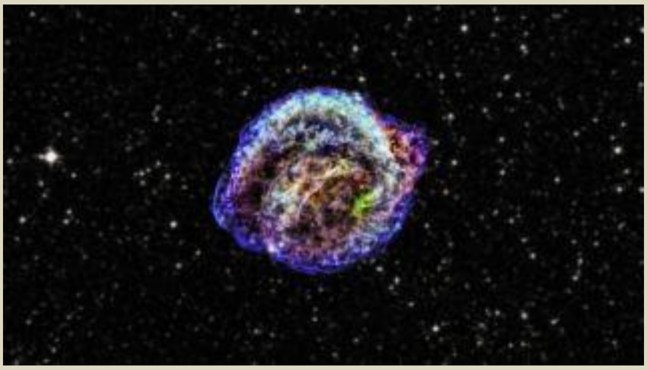
## Radioactive 'snowflakes' act like the tiniest nuclear bombs in the universe

Source: https://www.livescience.com/radioactive-snowflakes-trigger-nuclear-blasts.html

Mar 10 – Tiny snowflakes of radioactive uranium that trigger massive nuclear blasts might explain some of the universe's more mysterious star explosions.

As smallish stars die, they cool into husks of their former selves known as white dwarfs. New research proposes that atoms of uranium sink to the centers of these aging white dwarf stars as they cool, freezing into snowflake-like crystals no bigger than grains of sand. There, these "snowflakes" can act as some of the tiniest nuclear bombs in the universe, becoming the "spark that sets off the powder keg," said study co-author Matt Caplan, a theoretical physicist at Illinois State University.

"It's important to understand how these explosions occur for all sorts of applications, from the production of elements to the expansion of the universe," Caplan told Live Science.



This Chandra X-ray Observatory image shows the remnant of Kepler's supernova, the famous Type 1a supernova explosion that was discovered by Johannes Kepler in 1604. (Image credit: X-ray: NASA/CXC/NCSU/M.Burkey et al; Optical: DSS)

These unusually dim star explosions are part of a class known as Type Ia supernovas. Typically, scientists think these explosions occur when a white dwarf star reaches a critical mass after siphoning gas from a companion star the white dwarf is in orbit with. Because Type Ia supernovas explode when they reach the same mass, they have the same brightness. This uniform brightness allows them to be used as a standard by which t distances in the universe are measured.

However, astronomers have noticed some Type Ia supernovas that are slightly dimmer than they should be. The new research, accepted to the journal Physical Review Letters, proposes an explanation in which lower-mass white dwarfs without a binary star companion can explode as supernovas on their own —even without sipping mass from a nearby star.

"Maybe we don't need the companion," study co-author Chuck Horowitz, a theoretical nuclear astrophysicist at Indiana University, told Live Science. "Maybe a single star on its own can explode."

### The birth of a stellar atomic bomb

White dwarfs are the remnant cores of stars less than 10 times the mass of the sun. Having shed their outer layers, white dwarfs are cold, unburning balls of mostly carbon and oxygen with a few other elements, such as uranium, sprinkled in. As they slowly cool over hundreds of thousands of years, their atoms freeze, with the heaviest atoms — like uranium — sinking to the core and solidifying first. Traditionally, scientists thought these white dwarfs, when solo, eventually dwindled into cold, dark husks. But in some cases, this process could set the stage for a massive nuclear-bomb-like explosion, the scientists said. When sunken uranium atoms bump into one another, they freeze, forming tiny radioactive snowflakes. Within an hour of the snowflake's formation, a rogue passing neutron in the core could smash into the snowflake, triggering fission — the nuclear reaction in which an atom is split. This fission could set off a chain reaction, similar to that in a nuclear bomb, eventually igniting the rest of the star and causing the white dwarf to explode as a supernova all by itself.

For this chain reaction to happen, however, there needs to be plenty of the radioactive isotope uranium-235. Because this isotope decays naturally over time, this type of explosion is only possible in the biggest stars, which have the shortest life spans. Smaller stars, such as the sun, some 5 billion years in the future when it dies, wouldn't have enough uranium-235 left for such explosions by the time they became white dwarfs.

The new paper has been met with interested skepticism by some scientists.

"If it works, it would be a really interesting way to do it," Ryan Foley, an astronomer at the University of California, Santa Cruz, told Live Science. However, Foley noted that dim Type Ia supernovas tend to come from old populations of stars, not those with mostly younger stars, where this type of explosion would occur. "Among young stars, there are very few,if any, dim Type Ia supernovae," Foley said.

While the research has shown that this new mechanism is physically possible, it's not clear yet if these solo star explosions really happen, how often they happen and exactly how the fission that fuels them is triggered.

"Right now, we're eager to run simulations to see if the snowflakes can really ignite the fission chain reaction to explode the star," Caplan told Live Science. "Even if it didn't fully ignite, it would be interesting to see if there is a fizzle or weak burning in the core."

## Soviet Engineers Detonated A Nuclear Bomb to Put Out A Three-Year Fire

**By Aadhya Khatri**

Source: https://mobygeek.com/features/nuclear-bomb-extinguish-three-year-fire-15987

Mar 15 – The nuclear bomb packed the power double that of the one that destroyed Hiroshima, or 30 kilotons

While nuclear bombs are often associated with mass destruction, these weapons have other uses beyond battlefields. And in 1963, a chance came for nuclear bombs to prove their standing.

### The Gas Fire in Uzbekistan

A blowout at a gas well in Southern Uzbekistan in 1963 caused a huge fire that lasted for the next three years. Each day the fire burnt over 12 million cubic meters of natural gas, an amount enough to supply several major cities.

A blowout at a gas well in Southern Uzbekistan in 1963 caused a huge fire that lasted for the next three years

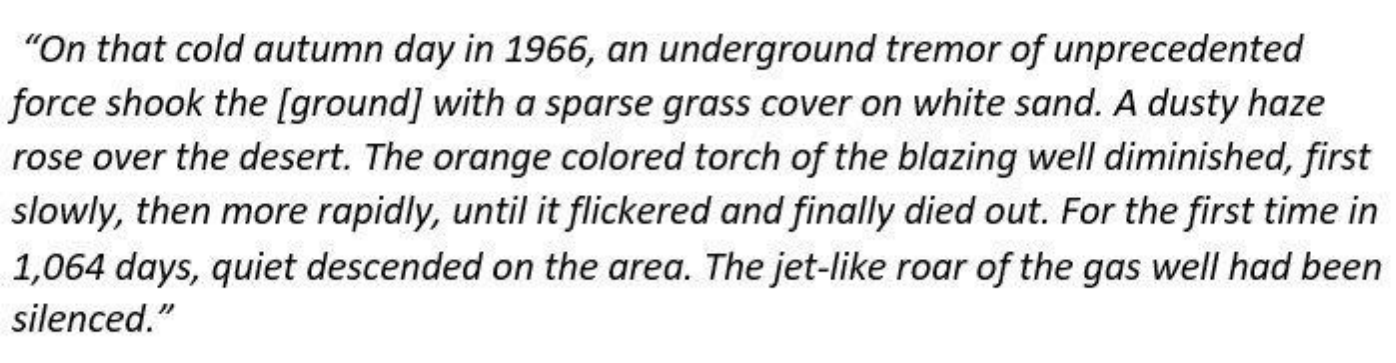
No one had succeeded in putting out the fire in three years and desperate times call for desperate measures, officials and engineers at that time decided to drop a nuclear bomb on the fire.

The plan seemed crazy at first but it actually made a lot of sense. According to physicists, if the bomb exploded at the depth of 1500 meters at a close distance to the shaft, the pressure it created could put out the huge fire. Experts developed the idea further and concluded that the bomb needed to pack the power double that of the one that destroyed Hiroshima or 30 kilotons.

After they had all the needed calculations, experts decided to go with the nuclear bomb plan as it was the best way at that time to stop the fire.

In 1966, the bomb was lowered into one of the two boreholes drilled near the shaft. Experts later filled the hole with cement before detonated the bomb.

Here is what Pravda Vostoka of Tashkent – a Soviet newspaper covered about that fated day:



*"On that cold autumn day in 1966, an underground tremor of unprecedented force shook the [ground] with a sparse grass cover on white sand. A dusty haze rose over the desert. The orange colored torch of the blazing well diminished, first slowly, then more rapidly, until it flickered and finally died out. For the first time in 1,064 days, quiet descended on the area. The jet-like roar of the gas well had been silenced."*

The plan worked. After just 20 seconds, the three-year-long fire was extinguished.

**The Results of The Test**

Soon after the first success, Soviet engineers were put to another test. This time, it was a fire at the Pamuk gas field that needed to be put out. The calculations called for a 47-kiloton bomb to be denoted at the depth of 2.44 kilometers. A few days after the explosion, the fire stopped.

It wasn't until the second success at Pamuk gas field that Soviet engineers started to put their faith in the practical use of a nuclear bomb.

In May 1972, the same method helped extinguished a fire in the city of Mary. Two months later, they solved the issue of a leaking well. The last attempt recorded was in 1981 when engineers detonated a bomb at a well off the Northwestern coast of Russia.

The second explosion at Pamuk was the largest of all the explosions.

## Russia soon inaugurates first nuclear plant in Egypt

Source: https://english.aawsat.com/home/article/2820341/russia-soon-inaugurate-firstnuclear-plant-egypt

Feb 22 – CEO of Russia's nuclear corporation Rosatom in the Middle East and Africa, Alexander Voronkov, announced on Sunday that the company will start construction of the first nuclear plant in Egypt, asserting that the reactors are environment-friendly.

## Secret Israeli nuclear facility undergoes major work

Source: https://www.jamaicaobserver.com/international/secret-israeli-nuclear-facility-undergoes-major-work_215744

Feb 26 — An Israeli secret nuclear facility at the centre of the nation's undeclared atomic weapons programme is undergoing what appears to be its biggest construction project in decades, satellite photos analysed by The Associated Press show.

A dig about the size of a soccer field and likely several storeys deep now sit just metres from the aging reactor at the Shimon Peres Negev Nuclear Research Centre near the city of Dimona. The facility is already home to decades-old underground laboratories that reprocess the reactor's spent rods to obtain weapons-grade plutonium for Israel's nuclear bomb programme.

What the construction is for, however, remains unclear. The Israeli Government did not respond to detailed questions from the *AP* about the work. Under its policy of nuclear ambiguity, Israel neither confirms nor denies having atomic weapons. It is among just four countries that have never joined the Non-Proliferation Treaty, a landmark international accord meant to stop the spread of nuclear arms.

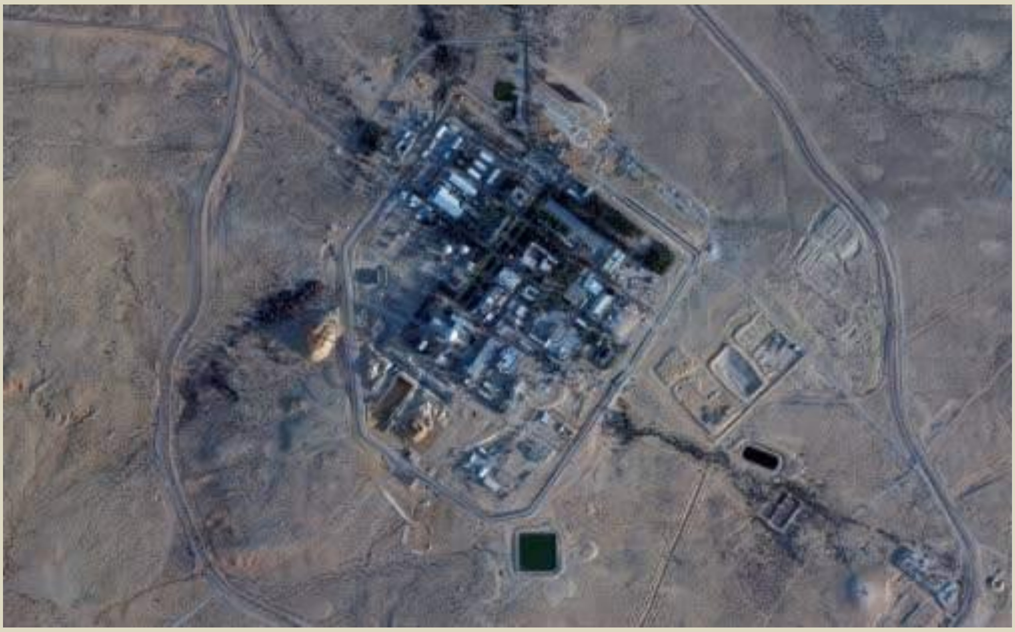
The construction comes as Israel — under Prime Minister Benjamin Netanyahu — maintains its scathing criticism of Iran's nuclear programme, which remains under the watch of United Nations inspectors unlike its own. That has renewed calls among experts for Israel to publicly declare details of its programme.

What "the Israeli Government is doing at this secret nuclear weapons plant is something for the Israeli Government to come clean about", said Daryl G Kimball, executive director of the Washington-based Arms Control Association.

With French assistance, Israel began secretly building the nuclear site in the late 1950s in empty desert near Dimona, a city some 90 kilometres (55 miles) south of Jerusalem. It hid the military purpose of the site for years from America, now Israel's chief ally, even referring to it as a textile factory.

With plutonium from Dimona, Israel is widely believed to have become one of only nine nuclear-armed countries in the world. Given the secrecy surrounding its programme, it remains unclear how many weapons it possesses. Analysts estimate Israel has material for at least 80 bombs. Those weapons likely could be delivered by land-based ballistic missiles, fighter jets or submarines.

For decades, the Dimona facility's layout has remained the same. However, last week, the International Panel on Fissile Materials at Princeton University noted it had seen “significant new construction” at the site via commercially available satellite photos, though few details could be made out.



This Monday, February 22, 2021 satellite photo from Planet Labs Inc shows construction at Shimon Peres Negev Nuclear Research Centre near the city of Dimona, Israel. A long-mysterious Israeli nuclear facility that gave birth to its undeclared atomic weapons programme is undergoing what appears to be its biggest construction project in decades, according to satellite photos analysed by The Associated Press. (Photo: AP)

Satellite images captured Monday by Planet Labs Inc after a request from the *AP* provide the clearest view yet of the activity. Just southwest of the reactor, workers have dug a hole some 150 metres (165 yards) long and 60 metres (65 yards) wide. Tailings from the dig can be seen next to the site. A trench some 330 metres (360 yards) runs near the dig.

Some two kilometres (1.25 miles) west of the reactor, boxes are stacked in two rectangular holes that appear to have concrete bases. Tailings from the dig can be seen nearby. Similar concrete pads are often used to entomb nuclear waste.

Other images from Planet Labs suggest the dig near the reactor began in early 2019 and has progressed slowly since then.

Analysts who spoke to the *AP* offered several suggestions about what could be happening there.

The centres's heavy-water reactor has been operational since the 1960s, far longer than most reactors of the same era. That raises both effectiveness and safety questions. In 2004, Israeli soldiers even began handing out iodine pills in Dimona in case of a radioactive leak from the facility. Iodine helps block the body from absorbing radiation.

Those safety concerns could see authorities decommission or otherwise retrofit the reactor, analysts say.

“I believe that the Israeli Government is concerned to preserve and maintain the nation's current nuclear capabilities,” said Avner Cohen, a professor of nonproliferation studies at the Middlebury Institute of International Studies at Monterey, who has written extensively on Dimona.

“If indeed the Dimona reactor is getting closer to decommissioned, as I believe it is, one would expect Israel to make sure that certain functions of the reactor, which are still indispensable, will be fully replaced.”

Kimball, of the Arms Control Association, suggested Israel may want to produce more tritium, a relatively faster-decaying radioactive by-product used to boost the explosive yield of some nuclear warheads. It also could want fresh plutonium “to replace or extend the life of warheads already in the Israeli nuclear arsenal,” he added.

Israel built its nuclear weapons as it faced several wars with its Arab neighbours since its founding in 1948 in the wake of the Holocaust. An atomic weapons programme, even undeclared, provided it an edge to deter enemies.

As Peres, who led the nuclear programme and later served as prime minister and president of Israel, said in 1998: “We have built a nuclear option, not in order to have a Hiroshima, but to have an Oslo,” referring both to the first US nuclear bomb drop in World War II and Israel's efforts to reach a peace deal with Palestinians.

But Israel's strategy of opacity also draws criticism from opponents. Iranian Foreign Minister Mohammad Javad Zarif seized on the work at Dimona this week as his country prepared to limit access by the UN's International Atomic Energy Agency amid tensions with the West over its collapsing 2015 nuclear deal.

“Any talk about concern about Iran's nuclear programme is absolute nonsense,” Zarif told Iranian state television's English-language arm *Press TV*. “Let's be clear on that: It's hypocrisy.”

The timing of the Dimona construction surprised Valerie Lincy, executive director of the Washington-based Wisconsin Project on Nuclear Arms Control.

"I think the most puzzling thing is ... you have a country that is very aware of the power of satellite imagery and particularly the way proliferation targets are monitored using that imagery," Lincy said. "In Israel, you have one known nuclear target for monitoring, which is the Dimona reactor. So, you would think that anything that they wanted to keep under the radar would be kept under the radar."
In the 1960s, Israel used its claims about adversary Egypt's missile and nuclear efforts to divert attention from its work at Dimona — and may choose to do the same with Iran now.
"If you're Israel and you are going to have to undertake a major construction project at Dimona that will draw attention, that's probably the time that you would scream the most about the Iranians," said Jeffrey Lewis, a professor also teaching nonproliferation issues at Middlebury.

## Brazil's Eletrobras ways nuclear unit hit with cyberattack

Source: https://www.reuters.com/article/us-eletrobras-cyber/brazils-eletrobras-saysnuclear-unit-hit-with-cyberattack-idUSKBN2A41JN

Feb 02 – A nuclear power subsidiary of Brazil's Eletrobras suffered a cyberattack but no operations were impacted, the state-controlled power holding company. The network that was attacked by ransomware is not related to the operational systems of nuclear energy plants Angra 1 and Angra 2, said Centrais Eletricas Brasileiras, as Eletrobras is formally known. The incident now is under investigation.

## Cap on Trident nuclear warhead stockpile to rise by more than 40%

Source: https://www.theguardian.com/uk-news/2021/mar/15/cap-on-trident-nuclear-warhead-stockpile-to-rise-by-more-than-40

Mar 16 – Britain is lifting the cap on the number of Trident nuclear warheads it can stockpile by more than 40%, Boris Johnson will announce on Tuesday, ending 30 years of gradual disarmament since the collapse of the Soviet Union.
The increased limit, **from 180 to 260 warheads**, is contained in a leaked copy of the integrated review of defence and foreign policy, seen by the Guardian. It paves the way for a controversial £10bn rearmament in response to perceived threats from Russia and China.
The review also warns of the "realistic possibility" that a terrorist group will "launch a successful CBRN [chemical, biological, radiological or nuclear] attack by 2030", although there is little extra detail to back up this assessment.

It includes a personal commitment from Johnson, as a last-minute addition in the foreword, to restore foreign aid spending to 0.7% of national income "when the fiscal situation allows", after fierce criticism of cuts in relief to Yemen and elsewhere.

**The 100-page document says the increase in the nuclear warheads cap is "in recognition of the evolving security environment" and that there are "developing range of technological and doctrinal threats".**

Campaigners warned the UK was at risk of starting a "new nuclear arms race" at a time when the world is trying to emerge from the Covid pandemic. Kate Hudson, the general secretary of the Campaign for Nuclear Disarmament (CND), said: "With the government strapped for cash, we don't need grandiose, money-wasting spending on weapons of mass destruction."

The commitment is one of the most notable in the integrated review, a landmark post-Brexit review of defence and foreign policy, which also includes:

- A clear statement that Russia under Vladimir Putin represents an "active threat" but nuanced language on China, which is described as posing a "systemic challenge" in a manner unlikely to please Conservative hawks on the party's backbenches.
- A commitment to launch an additional sanctions regime giving the UK "powers to prevent those involved in corruption from freely entering the UK or channelling money through our financial system" for the first time.
- An aspiration for the UK to be a "soft power superpower" with praise for the BBC as "the most trusted broadcaster worldwide" despite Downing Street boycotting the broadcaster last year. The British monarchy is also cited as contributing.

The review began in the aftermath of the 2019 general election and is intended to help define the prime minister's "global Britain" vision and shape future strategic direction, after leaving the EU, until 2030.

It contains only a handful of passing references to the bloc, arguing instead for an "Indo-Pacific tilt" in which the UK deepens defence, diplomatic and trade relations with India, Japan, South Korea and Australia in opposition to China.

"We will be the European partner with the broadest and most integrated presence in the Indo-Pacific," the review says, while arguing that investing in cyberwarfare capabilities and deploying the new Queen Elizabeth aircraft carrier in the region later this year will help send a message to Beijing.

But it is the commitment to significantly increase the cap on nuclear warhead numbers that is the most significant development, coming after the UK promised to run down stockpiles following the end of the cold war.

**Britain has far fewer warheads stockpiled than Russia, estimated to have 4,300, the US on 3,800 or China, which has about 320. But each warhead the UK holds is estimated to have an explosive power of 100 kilotons.** The atomic bomb dropped on Hiroshima at the end of the second world war was about 15 kilotons.

"A minimum, credible, independent nuclear deterrent, assigned to the defence of NATO, remains essential in order to guarantee our security and that of our allies," the UK review says in a section explaining the context for the stockpile increase.

Stewart McDonald, the defence spokesman for the Scottish National party, which is opposed to Trident renewal, accused the government of being wedded to an outdated defence policy: "For the prime minister to stand up and champion the international rules-based system before announcing in the same breath that the UK plans to violate its commitments to the international treaty on non-proliferation beggar's belief."

China lobby groups said they believed the review did not go far enough. A spokesperson for the Inter-Parliamentary Alliance on China said Beijing should not have been omitted from the list of countries engaged in hostile state activities.

"This is despite repeated Chinese state-backed cyber-attacks on UK targets and attempts by Chinese government agents to intimidate and threaten UK residents on British soil – and in stark contrast to Russia, Iran and other authoritarian states that have also targeted the UK," the spokesperson added.

Further details of the plans for the armed forces will be contained in an official defence command paper to be published on Monday. That is expected to confirm a cut in the size in the British army to 72,500 – not mentioned in the review document – and investments in pilotless killer drones.

One idea not previously mentioned is a tentative proposal to create a citizen's volunteer force – a "civilian reservist cadre" – potentially to work alongside the military in response to the future crises on the scale of the pandemic.

**EDITOR'S COMMENT:** "…developing range of technological and doctrinal threats." – what a silly excuse to add 80 more nuclear warheads as if the already available 180 are not enough to trigger a nuclear holocaust! And if the attack is an asymmetric one, whom they are going to bomb?

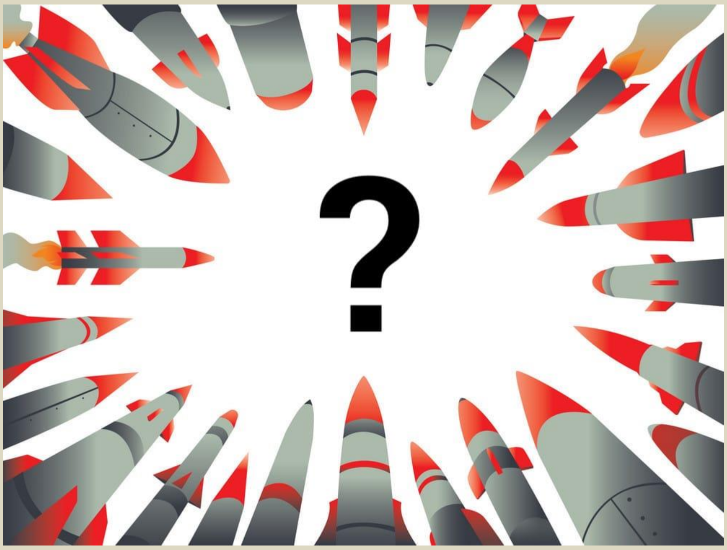
**Watch this movie**

**DIRTY WAR**

## An existential discussion: What *is* the probability of nuclear war?

**By Martin E. Hellman and Vinton G. Cerf**

Source: https://thebulletin.org/2021/03/an-existential-discussion-what-is-the-probability-of-nuclear-war/



Mar 18 – Long before Vinton Cerf and Martin Hellman changed the world with their inventions, they were young assistant professors at Stanford University who became fast friends. Chances are that you relied on their innovations today. Cerf is considered one of the "fathers of the internet" for having invented, along with Robert Kahn, the internet's protocols and architecture, known as Transmission Control Protocol/Internet Protocol (TCP/IP). Hellman is seen as a "father of public key cryptography" for having invented, along with Whitfield Diffie and Ralph Merkle, the technology that protects monetary transactions on the internet every day. More than 50 years and two technological revolutions later, the friendship between Vint and Marty—as they know each other—endures. This is despite, or perhaps because of, their sometimes-different views. You see, while they do not always agree, they both enjoy a good intellectual debate, especially when the humans they sought to bring together with their inventions face existential threats.

Not long after giving the world public key cryptography, Hellman switched his focus from encryption to efforts that might avoid nuclear war. "What's the point of developing new algorithms if there's not likely to be anybody around in 50-100 years?" Hellman recalls thinking at the time. He did not then envision that cybersecurity would also become an existential threat or what it is today—an escalatory step toward nuclear threats that could lead to nuclear use.

Sometime after TCP/IP provided the foundation for the internet, Cerf joined Google as its Chief Internet Evangelist and vice president, where he leads efforts to spread the internet, via global policy development, to billions of people around the world without access. Among other projects, he has also had a hand in supporting NASA's effort to build an interplanetary internet that operates today.

The world has changed in dramatic ways since Cerf and Hellman met 50 years ago. Yet the foundation of their friendship—good intellectual debates—has not. On a recent private phone call with each other, the two friends discussed the National Academies of Sciences, Engineering, and Medicine's project seeking to answer the question, "Should the US use quantitative methods to assess the risks of nuclear war and nuclear terrorism?" While both agree that the US needs to understand the risk of nuclear war, they disagree about whether a quantitative analysis is necessary. What follows are their thoughts, presented here for *Bulletin* readers.

### Quantitative

**Martin Hellman**

Professor Emeritus, Stanford University

#### When the risk is highly uncertain, how do you determine who's right?

Is the risk of nuclear deterrence failing acceptable? Former Secretary of Defense James Schlesinger thought so. In a 2009 interview, he stated that the US would need a strong nuclear deterrent "more or less in perpetuity." In contrast, former Secretary of Defense Robert McNamara stated in the 2003 documentary, *Fog of War*, that "the indefinite combination of human fallibility and nuclear weapons will destroy nations." So, is the risk of failure acceptable or unacceptable? When nuclear

### Qualitative

**Vinton Cerf**

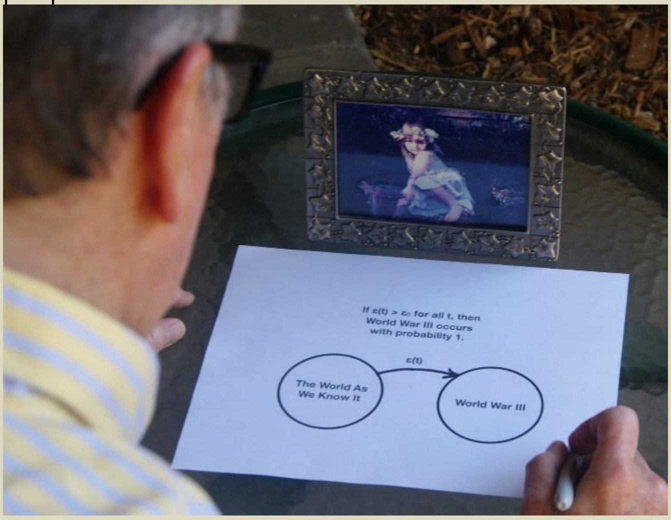
VP and Chief Internet Evangelist, Google

#### Numbers are not needed for people to see the unacceptable risk we face.

Although I am not an expert on nuclear conflict, my good friend, Martin Hellman, has drawn me into a serious discussion about the risk of nuclear war. Along with Robert Kahn, I am the co-inventor of the Internet's architecture and core protocols. I would prefer for humanity to endure and not obliterate itself. Both Hellman and I consider nuclear deterrence—threatening to destroy civilization in an effort to preserve the peace—to be untenable as a long-run strategy. But we differ on the need to risk is stated in generalities, it is difficult to determine who is right.

In the 1970s, such questions were, at best, of passing interest to me. My research in cryptography consumed me. That wasn't all bad since it led to the invention of public key cryptography and the foundation of much of modern cybersecurity. But, slowly and painfully, I came to see that my over-focus on career and logic was killing my marriage. Then, in 1981, Ronald Reagan's assumption of the presidency brought the nuclear threat into sharp focus.

As explained in a book that my wife, Dorothie, and I wrote, I realized that it wasn't smart to neglect risks either to my marriage or to the planet (and there was a surprising connection between the two). I shifted my research from information security to international security, with a focus on the risk of nuclear deterrence failing. Almost as soon as I looked at that question with new eyes, I saw that the risk of nuclear devastation was unacceptably high. I have continued to develop that line of thinking and here I summarize my current perspective.



Martin Hellman considers his quantitative risk analysis for nuclear war.

This article uses a simple, quantitative estimate to show that the risk of a full-scale nuclear war is highly unacceptable, and that a child born today may well have less-than-even odds of living out his or her natural life without experiencing the destruction of civilization in a nuclear war.

Some, including my friend and colleague, Vinton Cerf, prefer a qualitative analysis for reasons he explains in his companion article. Others argue that a quantitative estimate of the risk of a full-scale nuclear war is not possible because such an event has never occurred. They are right in the limited sense that it is not possible to determine if the risk of a nuclear war is one quantify the risk of deterrence failing. In these two companion articles, we explain our different thinking.

I prefer a qualitative approach because most people relate to it better. Many are confused by mathematical arguments. While numbers do not lie, some human beings do. Quantitative estimates run either the real or perceived risk of being twisted to support whatever conclusion is desired.

Instead, I prefer to rely on qualitative arguments like one that Marty has devised: Imagine that a man wearing a TNT vest were to sit down next to you and tell you that he wasn't a suicide bomber. Rather, there are two buttons for setting off his explosive vest. One was in the White House with Trump for the last four years, and recently was given to Biden. The other is with Putin in Moscow. You'd still get away as fast as you can! Why, then, has society "sat here" for decades assuming that, just because the Earth's explosive vest has not yet gone off, it never will? A qualitative argument like that will convince far more people than any mathematical reasoning.

But, most fundamentally, I prefer a qualitative approach because there are too many examples of sheer luck averting the use of nuclear weapons. Numbers are not needed for people to see the unacceptable risk we face.

As one example, during the 1962 Cuban missile crisis, American destroyers attacked three Soviet submarines near Cuba and forced them to surface. No American, not even President Kennedy or his military advisors, knew that each of those submarines carried a nuclear torpedo. According to an officer on one of those submarines, its captain gave orders to arm the nuclear torpedo, but was talked down. The captain's order makes more sense when one remembers that the last he had heard before submerging was that World War III seemed imminent; he was under attack; and surfacing would be a humiliating defeat. Fortunately, luck won out: the captain suffered humiliation, but civilization was not devastated.

Some may object that such Cold War incidents should not be used as guides in today's very different world. Yet, in June 1999, at the start of NATO's peacekeeping mission in Kosovo, an American general gave orders that his British subordinate feared was extremely dangerous. Their memoirs agree that a heated argument ensued, which ended with the British general telling the American, "Sir, I'm not starting World War III for you."

More recently, on January 13, 2018, Hawaiians received the following emergency alert: "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL." Fortunately, it was a false alarm and did not cause a response that might have been misinterpreted by our adversaries.

As of September 2020, it is estimated that there are 13,410 nuclear weapons in the world, with 91 percent of those divided percent per year versus two percent per year. But it is possible to upper and lower bound it.

If someone were to propose that the risk were one percent per day, I'd rule that out as far too high because then nuclear war would be almost certain within the next year. Similarly, if someone were to suggest that the probability were one in a million per year, I'd consider that too low because it would imply that nuclear deterrence as currently practiced could work for approximately a million years. Considering the historical record of nuclear near misses, some of which are detailed in Vint's article, a million years is far too optimistic. (Of course, if humanity survives for another million years, major events will change the risk appreciably. Here, I seek only to estimate the risk over the next year, during which time such changes will be minimal. Extrapolating that annualized estimate to the next several decades also is reasonable, especially given the estimate's large uncertainty bounds.) These two extreme cases—nuclear catastrophe either in the next year or in a million years—establish initial upper and lower bounds on the risk.

Next, I sought to narrow the range. In my estimation, and based on my extensive study of nuclear risks, ten percent per year is also an upper bound since we have survived approximately 60 years of nuclear deterrence without the use of any nuclear weapons in warfare, much less a full-scale exchange. Similarly, 0.1 percent per year seems too low because that would imply that current policies could be continued for approximately 1,000 years before civilization would be expected to be destroyed. Over that time period, and subject to the above caveat about the risk changing over time, I extrapolate from past events and estimate that we would expect on the order of ten major crises comparable to Cuba 1962; 100 lesser crises comparable to the 1995-1996 Taiwan Straits Crisis, the 2008 Russo-Georgian War, or the ongoing conflict in Ukraine that started in 2014; plus a large number of other events that could lead to nuclear threats and therefore, potentially, to nuclear use.

If you agree with my reasoning that the risk of a full-scale nuclear war is less than ten percent per year but greater than 0.1 percent per year, that leaves one percent per year as the order of magnitude estimate, meaning that it is only accurate to within a factor of ten. For related reasons, that one percent per year estimate really spans a range from roughly 0.3 to three percent per year.

A risk of one percent per year would accumulate to worse-than-even odds over the lifetime of a child born today. Even if someone were to estimate that the lower bound should be 0.1 percent per year, that would be unacceptably high—that child would have an almost ten percent risk of experiencing nuclear devastation over his or her lifetime.

between the United States and Russia. Speaking purely qualitatively, I see no scenario in which so many weapons are needed, even under the theory of Mutually Assured Destruction or MAD.

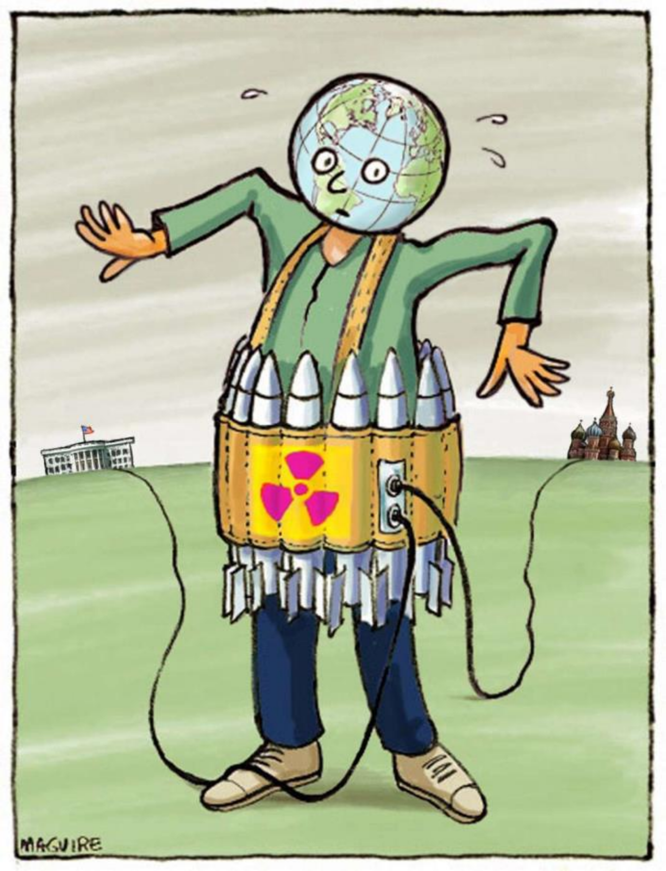


Illustration by Barrie Maguire

Marty argues that risk reduction efforts will languish until the risk of nuclear war is shown to be clearly unacceptable. Society's lack of action, or even concern, might seem to justify his thinking. But, even if a study were to produce an unacceptably high numerical risk value, some would still dispute the numbers or find them unintuitive.

As I read Marty's analyses, I am struck by the thought that any positive risk of a global nuclear exchange is simply unacceptable. The mere existence of nuclear weapons and the possibility that their availability might lead to their use seems self-defeating. As Ronald Reagan and Mikhail Gorbachev stated, "a nuclear war must never be fought and cannot be won."

We would do well to ask ourselves how we might accomplish risk reduction regardless of the quantified risk. If sufficient people desire risk reduction, regardless of their agreement or disagreement as to its quantification, we might succeed in

The above arguments show the importance of not only estimating the risk of a full-scale nuclear war, but also establishing a maximum acceptable level for that risk. If someone argues that 0.1 percent per year or some other value is an acceptable level of risk, society can then judge whether or not it agrees.

This quantitative approach avoids the ambiguity of non-quantitative arguments such as Schlesinger's and McNamara's. When the risk is highly uncertain, how do you determine who's right? A quantitative approach, even to an order of magnitude as done here, requires both proponents and opponents of nuclear deterrence to justify their positions in ways that others can more easily decide who to believe.

I hope you will agree with either my quantitative approach or Vint's qualitative approach, both of which conclude that the risk of a nuclear war is unacceptably high and risk reduction measures are urgently needed. For those who accept neither of our approaches, I have two questions:

First, what evidence supports the belief that the risk of nuclear deterrence failing is currently at an acceptable level?

Second, can we responsibly bet humanity's existence on a strategy for which the risk of failure is totally unknown?

Read Vinton Cerf's *qualitative* argument ↑

making the world a safer place. Is there any other logical course of action?

Read Martin Hellman's *quantitative* argument ↑

*Stanford **Professor Martin Hellman** is best known for his invention (joint with Whitfield Diffie and Ralph Merkle) of public key cryptography, the technology that protects trillions of dollars every day. This work won him the ACM Turing Award, sometimes thought of as "the Nobel Prize in Computer Science." Professor Hellman also has a deep interest in the ethics of technology development.*

***Vinton Cerf** is Google's VP and Chief Internet Evangelist. Cerf co-designed the Internet's TCP/IP protocols and architecture. A former Stanford Professor and US National Science Board member, he serves in advisory capacities at NIST, DOE, and NASA. Cerf is a recipient of numerous awards for his work, including the US Presidential Medal of Freedom, ACM Turing Award, and 29 honorary degrees.*

## Iran Probably Already Has the Bomb. Here's What to Do about It

**By R. James Woolsey, William R. Graham, Henry F. Cooper, and Peter Vincent Pry**

Source: https://www.nationalreview.com/2021/03/iran-probably-already-has-the-bomb-heres-what-to-do-about-it/

Mar 19 – Washington's policy-makers are being misled by the intelligence and defense communities that are grossly underestimating the nuclear threat from Iran, just as they did with North Korea.

Washington's mainstream "worst-case" thinking assumes Iran does not yet have atomic weapons, but could "break out" to crash-develop one or a few A-bombs in a year, which the intelligence community would supposedly detect in time for warning and preventive measures. Rowan Scarborough recently reported in the *Washington Times* that "during a private talk in July 2017 before a Japanese-U.S. audience," the Pentagon's director of Net Assessment James H. Baker briefed that "Iran, if it chooses, may 'safely' possess a nuclear weapon in 10-15 years time."

Another mainstream "worst-case" view is that Iran could abide by the Obama administration's Joint Comprehensive Plan of Action (JCPOA) and legitimately glide toward nuclear weapons capability in ten to 15 years. The Trump administration canceled the JCPOA for legitimate reasons, but the Biden administration has pledged to revive it.

In contrast to these views, we warned in these pages in February 2016 that Iran probably already had atomic weapons deliverable by missile and satellite:

We assess, from UN International Atomic Energy Agency [IAEA] reports and other sources, that Iran probably already has nuclear weapons. . . . prior to 2003, Iran was manufacturing nuclear weapon components, like bridge-wire detonators and neutron initiators, performing non-fissile explosive experiments of an implosion nuclear device, and working on the design of a nuclear warhead for the Shahab-III missile.

When our World War II Manhattan Project reached this stage, the U.S. was only months away from making the first atomic bombs. This was Iran's status 18 years ago. And the Manhattan Project employed 1940s-era technology to invent and use the first atomic weapons in only three years, beginning from a purely theoretical understanding.

So, by 2003, Iran was already a threshold nuclear-missile state. But for at least the last decade, the intelligence community has annually assessed that Iran could build atomic weapons in one year or less. On the other hand, less than a month ago, independent analysts at the Institute for Science and International Security assessed that Iran had a break-out time of as short as three months for its first nuclear weapon and five months for a second.

And there is no reason to believe U.S. and IAEA intelligence capabilities are so perfect that they can assuredly detect Iran's clandestine efforts to build atomic weapons. Indeed, the U.S. and IAEA did not even know about Iran's clandestine nuclear-weapons program until Iranian dissidents exposed it in 2002.

The IAEA and the U.S. intelligence community have long been poor nuclear watchdogs. IAEA inspections failed to discover clandestine nuclear-weapons programs in North Korea, Pakistan, Iraq, and Libya. In 1998, the intelligence community's "Worldwide Threat Assessment" failed to warn that, just a few months later, Pakistan and India would overtly "go nuclear" with a series of nuclear-weapons tests. U.S. intelligence often underestimated nuclear threats from Russia, China, and North Korea. It is likely now doing the same with Iran.

**Contrary to mainstream thinking:**

- *Iran can build sophisticated nuclear weapons by relying on component testing, without nuclear testing*. The U.S., Israel, Pakistan, and India have all used the component-testing approach. The U.S. Hiroshima bomb was not tested, nor have been more sophisticated U.S. thermonuclear warheads during the past 30 years. Pakistan and India's 1998 nuclear tests were done for political reasons, not out of technological necessity.
- *IAEA inspections are limited to civilian sites, and restricted from military bases, including several highly suspicious underground facilities where Iran's nuclear-weapons program almost certainly continues clandestinely*. Imagery of one vast underground site, heavily protected by SAMs, shows high-voltage powerlines terminating underground, potentially delivering enormous amounts of electricity, consistent with powering uranium enrichment centrifuges on an industrial scale. So, IAEA reports on Iran's enriched-uranium stockpile almost certainly are not the whole story.
- The U.S. intelligence assessment that Iran suspended its nuclear-weapons program in 2003 is contradicted both by Iran's nuclear archives, stolen by Israel in 2018, indicating Iran's ongoing nuclear-weapons program (reported at several sites in 2006, 2017, and 2019) and by Iran's rapid resumption of enriching uranium to prohibited levels. This demonstrates an existing capability to quickly produce weapons-grade uranium. Reports from the Congressional Electromagnetic Pulse (EMP) Commission elaborate these and important related issues.
- Most estimates assume Iran needs five to ten kilograms of highly enriched (over 90 percent) uranium-235 or plutonium-239 to make an atomic weapon, as with the first crudely designed A-bombs that destroyed Hiroshima and Nagasaki. But a good design requires only one to two kilograms. Crude A-bombs can be designed with uranium-235 or plutonium-239 enriched to only 50 percent.
- Iran's nuclear and missile programs are not just indigenous, but are helped significantly by Russia, China, North Korea, and probably Pakistan.
- While the intelligence community uses an in-country nuclear test as confirmation that a country, including Iran, has developed a nuclear weapon, this leaves it wide open to deceiving itself, our leadership, and our allies. Iran and North Korea have close working relations, North Korea will do anything for Iranian oil, and Iranians have reportedly been present at some of North Korea's nuclear tests. North Korea could easily have exchanged information with Iran and even tested Iranian nuclear weapons as well as their own — if there is any difference — without the U.S. and its allies knowing whose weapons were being tested. North Korean scientists are known to be in Iran helping the Islamic Revolutionary Guard "space program" that provides cover for developing ICBMs.

As we warned five years ago, it is implausible and imprudent to assume that Iran refrained from making atomic weapons for more than a decade, when they could do so clandestinely:

Iran probably has nuclear warheads for the Shahab-III medium-range missile, which they tested for making EMP attacks. . . . And at a time of its choosing, Iran could launch a surprise EMP attack against the United States by satellite, as they have apparently practiced with help from North Korea.

Why has Iran not gone overtly nuclear, like North Korea? There are several explanations. For one, North Korea is protected by China and lives in a safer neighborhood, where South Korea and Japan are reluctant to support U.S. military options to disarm Pyongyang. In contrast, Iran's neighbors, Israel and moderate Arab states, are far more likely to support air strikes to disarm Tehran. As we warned five years ago, Iran probably wants to build enough nuclear missiles to make its capabilities irreversible:

Iran could be building a nuclear-capable missile force, partly hidden in tunnels, as suggested by its revelation of a vast underground missile basing system. . . Iran is building toward a large, deployable, survivable, war-fighting missile force—to which nuclear weapons can be swiftly added as they are manufactured.

Moreover, Iran wants to preserve the fiction of its non-nuclear status. It has derived far more economic and strategic benefits from the JCPOA and threats to "go nuclear" than has North Korea from "going nuclear" overtly. Ominously, Iran may be forgoing the deterrence benefits of an overt nuclear posture because it is building toward surprise future employment of nuclear capabilities to advance the global theological agenda of the ayatollahs and the Islamic Revolutionary Guard, the world's largest and most sophisticated terrorist organization.

So what can we do to meet this almost-certain threat? Some better options are, unfortunately, far more difficult at this juncture. Arms control non-solutions like the JCPOA will only make matters worse, just as arms control did with North Korea, by offering false hope while the nuclear threat grows. Disarming Iran of nuclear capabilities by airstrikes or invasion would be very risky since we do not know where all of its nuclear missiles are hidden. The U.S. was deterred from disarming North Korea when that nation's nuclear-missile capabilities were merely nascent. Regime change by sponsoring a popular revolution may be a practical solution — the Iranian people would overthrow their Islamist government if they could. But the regime itself has proven adept at suppressing popular uprisings, and may use U.S. involvement, whether purported or actual, as a propaganda tool in such an effort, as it has before.

But there are things we can do right now, including:

- Harden U.S. electric grids and other life-sustaining critical infrastructures against a nuclear EMP attack, which is described in Iran's military doctrine and would be the regime's most easily executed and most damaging nuclear threat.
- The White House and STRATCOM should regard Iran as a nuclear-missile threat right now, increase scrutiny by national technical means of verification and by human intelligence to locate nuclear-weapons capabilities, and prepare preemptive options should action become necessary.
- Strengthen National Missile Defenses and especially deploy modern space-based defenses. For example, the 1990s Brilliant Pebbles project, canceled by the Clinton administration, could begin deployment in five years, cost an estimated $20 billion in today's dollars, and intercept essentially all ballistic missiles ranging more than a few-hundred miles, including from Russia and China. Our national survival should not depend only upon striking first or deterrence. The American people would rather be defended than avenged.

***Ambassador R. James Woolsey*** *is a former director of central intelligence.*

***William R. Graham*** *was President Reagan's science adviser and acting administrator of NASA, and chaired the Congressional EMP Commission.*

***Ambassador Henry F. Cooper*** *was director of the Strategic Defense Initiative and chief negotiator at the Defense and Space Talks with the USSR.*

***Fritz Ermarth*** *was chairman of the National Intelligence Council.*

***Peter Vincent Pry*** *is executive director of the EMP Task Force on National and Homeland Security and served in the Congressional Strategic Posture Commission, the House Armed Services Committee, and the CIA.*

## Ten years later, here's what Fukushima's damaged reactors look like today

**Video:** https://www.youtube.com/watch?v=Lxg38I0P7z4

Mar 19 – On 11 March 2011, an earthquake cut power to the Fukushima Daiichi nuclear power plant, and a tsunami wiped out emergency generators.

Three reactor cores exploded, releasing the highest amount of radioactivity in the environment since the Chernobyl nuclear disaster. Although **cleanup in Fukushima has been in progress for 10 years**, many years remain before all the melted fuel debris will be removed from the damaged reactors. Watch to see what the nuclear power plant looks like today, and how the disaster has impacted the surrounding community.

International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

# EXPLOSIVE NEWS

## Identifying Skin Proteins Left on IEDs

Source: http://www.homelandsecuritynewswire.com/dr20210222-identifying-skin-proteins-left-on-ieds

Feb 22 – Following a terrorist bombing, can the bomb maker be identified by skin proteins left on the bomb components they handled?

To address this question, Lawrence Livermore National Laboratory (LLNL) personnel from Weapons Complex Integration (WCI) and Global Security (GS) Forensic Science and Biosecurity Centers (FSC/BSC) subjected notional bomb components handled by LLNL volunteers to contained precision explosions. A small team of biology and explosives subject matter experts combined their knowledge and experience to successfully carry out a series of 26 confined detonations over a three-day period (see the video).

The identification of individuals through shed skin is an intense area of research for the Intelligence Advanced Research Projects Activity (IARPA) **Proteos program**, led by Kristen Jordan. The program is a culmination of years of IARPA support to the FSC and is underpinned by capabilities developed under a Strategic Initiative Laboratory Directed Research & Development grant on protein-based identification. The FSC team is leading the Test and Evaluation (T&E) effort for the Proteos program.

The Proteos program focuses on human identification using shed skin cells associated with trace forensic samples. This investigation seeks to exploit the relationship between polymorphisms in the skin proteome, or **genetically variable peptides (GVPs)** and their underlying nonsynonymous single nucleotide polymorphisms (nsSNPs) to evaluate peptide mass fingerprinting as a reliable forensic analytic technique. In other words, mutations in our genomes manifest as small differences in our skin proteins.

Using analytical chemistry, these differences in the peptide mass fingerprint can be used forensically to identify someone.

"It has been shown that patterns of GVPs can be used to identify individuals. The big question now is whether that information survives harsh environments such as explosions," said Deon Anex, project principal investigator. "If forensically relevant information in shed skin cells survives conditions that compromise or destroy other evidence, such as latent fingerprints or DNA, this technology could be a game-changer in post-blast investigations."

GVP technology may be further expanded to identify warfighter remains, victims of 9/11 and pilots and crew of downed aircraft, and leveraged in cancer peptide analytics.

The FSC program is now entering Phase 3: dealing with the challenges of detecting proteins in fingerprints deposited on common objects and materials of interest to potential future users of the technology in the U.S. government. In the national security realm, one of those materials is post-blast debris from an improvised explosive device (IED).

"National labs have the ability to cross-pollinate disciplines in a way that gives them a strategic advantage for delivering on difficult national security problems," said Matt Lyman, a BSC biologist that participated in the study. "Nuclear weapon engineers and biologists delivering unique biological specimens for the intelligence community? It seems like science fiction, but it is a reality that we can embrace as LLNL employees. Sharing knowledge from disparate fields often yields new intellectual fruit."

Mark Hart led the WCI team of high explosive experts Drew Carlson and Kurt Ehrenburg. Hart's team led the theoretical design, material procurement, construction and placement of the shots.

"When attempting to do something that has never been done before, you can't expect everything to run smoothly or the way you planned. This first-of-its-kind operation and experiment has been a remarkable exception. All aspects went according to plan and turned out better than expected," Hart said at the end of the study.

The LLNL Global Security team is composed of biologists Matt Lyman, Bonnee Rubinfeld, Cheryl Strout and Jim George who prepared and transported the fingerprint samples on "IED-like" materials, such as wires and wire nuts, galvanized steel coupons and wood components. Anonymous volunteers within the LLNL community donated fingerprints.

The two Proteos performer groups led by the University of Washington and Signature Science and the internal FSC T&E group will analyze the post detonation debris for GVPs in skin proteins.

## Manchester Arena inquiry: Live exercise before bombing was 'catastrophic failure'

Source: https://news.sky.com/story/manchester-arena-inquiry-live-exercise-before-bombing-was-catastrophic-failure-12227854

Feb 24 – A live counter-terrorism exercise a year before the Manchester Arena bombing was a "catastrophic failure" and would have led to even more loss of life had it been real, the inquiry has heard.

Firefighters and paramedics did not turn up for more than two hours after the police failed to call them forward during the 2016 exercise - a situation replicated on the night of the bombing.

On the night of the attack in May 2017, firefighters did not deploy to the arena for more than two hours because they could not get through to police - and only one paramedic entered the scene of the explosion in the first 40 minutes.
The inquiry is investigating whether any of the 22 victims could have been saved if the emergency services had reacted faster.

Twenty-two people were killed in the bombing

During the training exercise, a police inspector refused to let the fire and ambulance services into the inner cordon and the exercise was packing up by the time they finally arrived, the inquiry was told.
Advertisement
June Roby was the police inspector responsible for Exercise Winchester Accord, which mocked up a terrorist firearms attack at the Trafford shopping centre in May 2016.
Pete Weatherby QC, for the Arena victims' families, asked: "Even in the context of a highly organised exercise with prompters in the wings, the exercise went catastrophically wrong in terms of the multi-agency response?"
"It would appear so, yes," Mr Roby said.
North West Ambulance Service said that "if it had been real life it would have led to further loss of life" and Ms Roby accepted: "I can't disagree with that."
Greater Manchester Fire and Rescue Service made the same point that the failure to call them up for 2 hours and 20 minutes was "likely to lead to the further loss of life". "That was a catastrophic failure?" Mr Weatherby asked. "Yes," the former inspector said.
Mr Weatherby suggested that the multi-agency aspect of the exercise was "not something taken particularly seriously by Greater Manchester Police". But Ms Roby insisted: "I disagree. If we weren't taking it seriously, we wouldn't have had any other agencies present." The inquiry continues.

## Bomb Blast Exposure May Raise Risk of Alzheimer's, Army-Funded Research Finds

Source: https://www.aviationpros.com/aircraft/defense/news/21212563/bomb-blast-exposure-may-raise-risk-of-alzheimers-armyfunded-research-finds

Mar 02—Troops exposed to shockwaves from bomb blasts may be at higher risk for developing Alzheimer's disease and other neurological issues, even if they haven't suffered a traumatic brain injury, recent Army-funded research suggests.

Researchers at the University of North Carolina at Pembroke found that even small explosions — ones unlikely to cause concussions or injuries — change the molecular structure of the brain, a study published last week in the journal Brain Pathology found.

"This finding may explain those many blast-exposed individuals returning from war zones with no detectable brain injury, but who still suffer from persistent neurological symptoms, including depression, headaches, irritability and memory problems," Ben Bahr, professor of molecular biology and biochemistry at UNC-Pembroke, said in an Army statement.

Explosions from roadside bombs, rockets and mortar rounds have affected many deployed troops in Afghanistan, Iraq and elsewhere in the past 20 years. Traumatic brain injuries and concussions from these blasts often lead to problems with sleep and memory, and sometimes to depression that leads to suicide.

Long-term issues can arise from blasts that troops might not recognize as harmful at the time, Bahr said.

"Our interest was focused on the effects of low-level blast waves that soldiers can experience during training and in war zones ... where nearby explosions can cause blast waves that can knock soldiers to their knees but they are able to get back up with no obvious injury to the body or brain," Bahr said in an email.

To test the impact of explosions on troops, researchers used slices of rat brains, specifically from the hippocampus, which plays an important role in learning and memory.

**They placed the brain tissue into a makeshift skull: an aquarium filled with warm water. Seven inches away from the aquarium was a 1.7-gram explosive charge, capable of a "seemingly innocuous level of blast wave intensity," Bahr said.**

**The explosion produced a blast wave that pulsed through the air, the tank and then through the water before reaching the brain tissue. The blast damaged the hippocampus and diminished electrical activity between neurons, said Frederick Gregory, program manager for the Army Research Office, which funded the research.**

"You start seeing the development of proteins associated with Alzheimer's plaque, as well as a loss in proteins you need to maintain your synaptic connections to your neurons," Gregory said in a phone call. These effects could be seen after only one blast, with further explosions showing cumulative damage, he said.

The research also involved the Development Command Army Research Laboratory and the National Institutes of Health.

Researchers said they plan to look at the effects of blasts on other parts of the brain.

"Early detection of this measurable deterioration could improve diagnoses and treatment of recurring neuropsychiatric impediments, and reduce the risk of developing dementia and Alzheimer's disease later in life," Bahr said in the Army statement.

## What do we know about unexploded WW2 bombs?

**By Charley Adams** (BBC South West)

Source: https://www.bbc.com/news/uk-england-devon-56243750

A bomb was detonated in a controlled explosion in Exeter

Mar 04 – Hundreds of thousands of bombs were dropped on Britain during World War Two, some of which never exploded, so perhaps it should not be a surprise that they are still being found more than 75 years after the end of the war. But how much do we know about them?

The discovery of an unexploded World War Two bomb in Exeter resulted in a military response, thousands of residents being evacuated from their homes and extensive damage to nearby properties.

After being discovered on an allotment due for development, the 2,200lb (1,000kg) German bomb was blown up on Saturday in a controlled explosion, leaving a crater the size of three double-decker buses.

Residents have all been allowed back into their homes but many of the properties are "uninhabitable" according to Exeter City Council. About 300 students are still waiting to be allowed back into their accommodation.

The BBC has spoken to a series of experts about the wider questions surrounding unexploded ordnance.

### How did the bomb get there?

Bombs created destruction around the city's cathedral in 1942

Exeter was the first victim of the Baedecker Raids on English cultural centres during World War Two, made in response to the British bombing of Lübeck.

The raids were named after the Baedeker guidebook used by the German military to select historic targets in England.

The Blitz of Exeter in April and May 1942 "was the single most destructive event in the city's history since at least the attack by the Vikings in 1003" said Dr Todd Gray.

The historian from the University of Exeter said the recently discovered bomb most likely fell during one of these attacks, when the city was targeted for morale rather than for strategic purposes.

Nearly 300 people died, more than 1,700 buildings were destroyed, 7,000 high explosives and incendiary bombs were dropped and 40 high explosive bombs did not detonate.

The 2,200lb (1,000kg) German bomb was discovered on an allotment due for development and blown up on Saturday

The sound of the bomb being exploded on Saturday was "ferocious", but Dr Gray said he felt "quite thankful" to have heard the noise as a reminder of what it would have been like at the time.

"That bomb going off reminds us what that generation in 1940s went through," said Dr Gray.

"It's sobering, but now and then something like this is good for us to think about."

The bomb was discovered near Exeter St David's railway station in an area not covered by a "bomb census".

"There's bound to be I would have thought one or two more somewhere," he added.

### Could there be more nearby?

Emily Charles, a World War Two curator at the Imperial War Museum said the exact number of bombs across the country was not known and it was "really hard" to work out where unexploded bombs could be.

The allies kept a detailed record of bomb damage inflicted on British cities during the war called the bomb census, said Ms Charles. They created maps to show the most damaged areas, which can give historians a "better picture" of where unexploded ordnance could be, she added.
The most common type of bomb used in the Blitz was about 500lb (226.8kg), meaning the 2,200lb (1,000kg) bomb detonated in Exeter was "particularly large" said Ms Charles.
However, she stressed it was "not uncommonly large" and bombs of this size had been found in recent years.

**Could they explode?**
A guide on managing the risk of unexploded devices was released by the Construction Industry Research and Information Association (CIRIA) in 2019.
The CIRIA guide said ordnance could be reactivated by either direct impact, vibration or heating.
The lack of fatalities in instances when construction teams discover unexploded devices "is particularly because of the Germans commonly using electrical fuses in WW2 that stopped functioning when the battery expired", said the guide.
"What makes unexploded bombs dangerous is their unpredictability," said Ms Charles.
She told the BBC there were "not huge scientific studies" on how explosives degraded or whether they got more deadly over time.
"So I think the best course of action is to treat them as if they are deadly."
That the bomb was detonated in a controlled explosion and houses suffered damage, proves they can still be dangerous, she said.
There are multiple reasons that bombs do not detonate upon landing, explained Ms Charles, such as faulty fuses, defects or the way they land.
She said people should call the police if they spot any suspected explosive devices.

**How much is there across the country?**

The explosion from the bomb being detonated was heard up to five miles away

The Ministry of Defence says since 2010 it has been involved with making safe 450 German WW2 bombs - about 60 a year, the BBC Reality Check team revealed in 2018.
However, these figures do not factor in the involvement of private companies that can also dispose of unexploded devices.
This can make it difficult to establish exact figures for how many are dealt with each year across the country.

A specialist from one such private company, Zetica UXO, told the BBC that since World War Two "45,000 unexploded bombs have been found and more are being found all the time".

Official records, which can often be understated, predicted around "200,000 plus bombs were detonated" during the war said Mike Sainsbury.

He said it was estimated that "another 10% or so" did not explode.

The CIRIA guide reveals an estimated 15,000 items of unexploded ordnance were removed from construction sites between 2006 and 2008 by three clearance firms.

Clearance efforts after World War Two were extensive, but some unexploded devices were "either deemed not to present a risk... or too inaccessible for practical removal", said the guide.

**How to detonate an unexploded bomb?**

The controlled explosion left a crater behind

Bomb disposal experts say they had no choice but to detonate the bomb because the fuse was so corroded they could not tell what type it was, or if it had been booby trapped.

A Ministry of Defence spokesperson said explosive ordnance teams from the Royal Navy and Army worked with local authorities to safely dispose of the bomb.

Military teams worked for 24 hours to build protective structures and trenches to minimise the impacts of the blast and used more than "400 tonnes of sand" to mitigate the explosion.

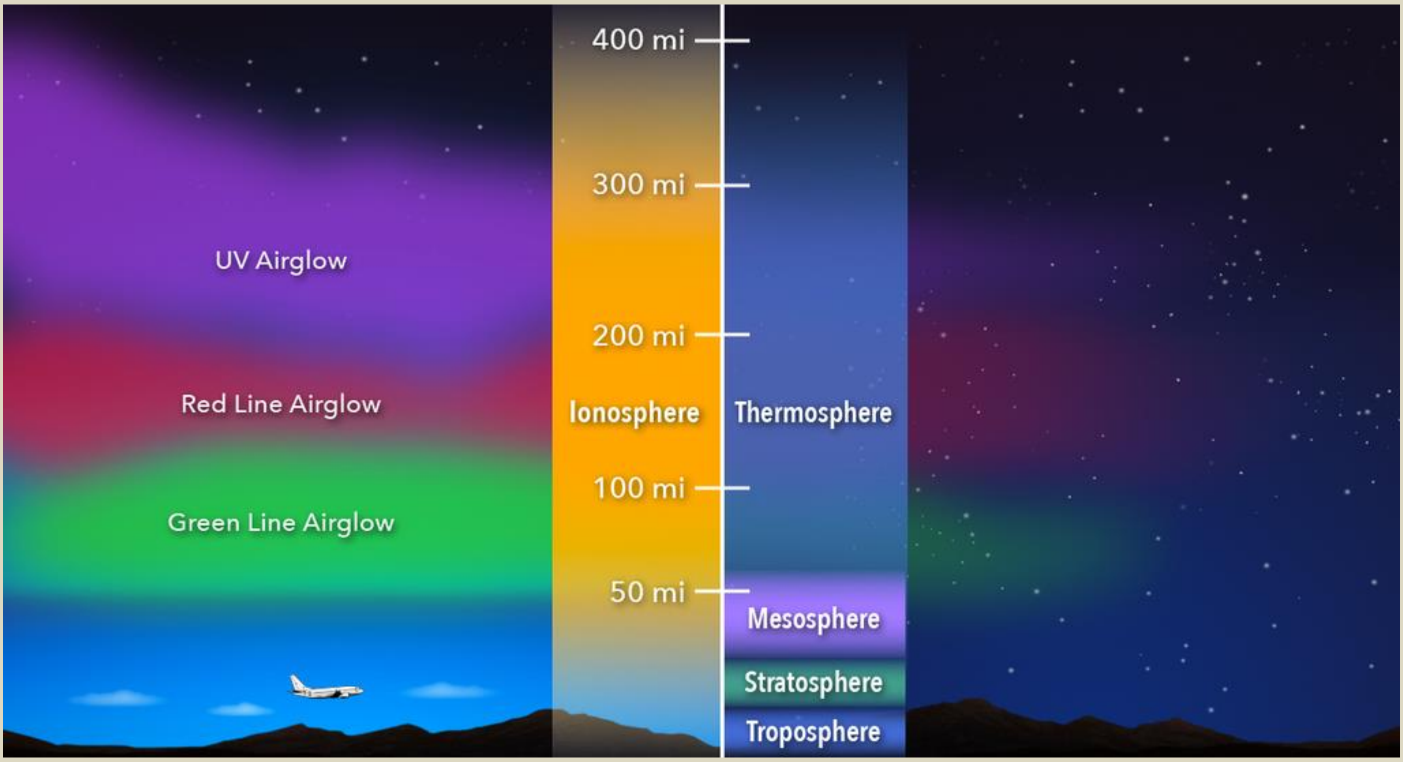
## The Tragic Beirut Explosion Was So Violent, It Disturbed Earth's Ionosphere

Source: https://www.sciencealert.com/last-year-s-blast-in-lebanon-was-so-violent-it-literally-shook-the-roof-of-the-world

Mar 19 – Early last August, residents near the Lebanese port of Beirut watched in horror as one of the largest non-nuclear, human-caused explosions on record tore a chunk out of their city, leaving hundreds dead, thousands injured, and hundreds of thousands homeless.

Its shock was felt around the globe - sensors as far away as Tunisia and Germany picked up the deep rumble, and seismic stations around 500 kilometers (just over 300 miles) away recorded its tremor.

Now it turns out the Beirut explosion caused the highest layers of the atmosphere to shake, and the resulting data could inform future efforts to keep an eye on weapons testing conducted by rogue states.



The ionosphere is the ionized part of Earth's upper atmosphere, from about 48 km (30 mi) to 965 km (600 mi) altitude, a region that includes the thermosphere and parts of the mesosphere and exosphere. The ionosphere is ionized by solar radiation.

Researchers from India's National Institute of Technology, Rourkela, and Hokkaido University in Japan measured electrical disturbances in the ionosphere, finding the blast was comparable to the impact of many volcanic eruptions.

"We found that the blast generated a wave that traveled in the ionosphere in a southwards direction at a velocity of around 0.8 kilometers per second," says Kosuke Heki, an Earth and planetary scientist from Hokkaido University.

Commencing around 50 kilometers (about 30 miles) overhead, and stretching into space hundreds of kilometers away, the ionosphere is characterized by high numbers of free-roaming electrons that get booted from gas molecules by solar radiation.

The team used variations in phases within microwave transmissions sent by the Global Navigation Satellite System (GNSS) on the day of the explosion to calculate changes in the distributions of the electrons, which in turn indicated the presence of acoustic waves through the gases.

It's a trick that scientists have used since the advent of such satellite networks in the 1990s, measuring ripples sweeping through the upper reaches of our atmosphere to note subtle signatures of anything from volcanoes to rogue nuclear testing.

One of the first experimental forays into using global positioning satellite (GPS) technology to measure surface explosions took place in the mid-1990s, with scientists taking advantage of three massive underground blasts at a coal mine in Wyoming, USA to study how the ionosphere responded.

Yet finding the faint traces of the Beirut explosion in this instance wasn't without a small amount of luck. With the event occurring early in the evening and close to sundown, ionosphere irregularities called equatorial plasma bubbles might have masked the signal altogether.

Fortunately, there were no signs of these bubbles at the time, giving the scientists a relatively clear image of the blast's wash slipping through the upper atmosphere at the speed of sound.

The researchers compared the impact of the Beirut explosion on the ionosphere with similar scars left by a number of recent volcanic eruptions in Japan, finding it more or less comparable. In the case of the eruption of Asama Volcano in central Japan in 2004, the Beirut blast was far more impactful.

Though slightly weaker than the 1.5 kiloton blasts studied all those decades ago in the Wyoming mine, the fact this explosion was exposed on Earth's surface gave it an unimpeded path towards the sky, with a release of energy clearly evident in the data.

Building a database of acoustic signatures that can be detected by the GNSS is providing scientists and authorities with a means to monitor not just the geological dynamics of our world, but its political friction as well.

We now know it took 2,700 tons of ammonium nitrate – a fertilizer also commonly used as an ingredient for explosives – to generate what's calculated to be equivalent to the detonation of 1.1 kilotons of TNT, putting it in the ballpark of a low-yield nuclear bomb.

The ability for states like Iran and North Korea to progress towards nuclear armament is still a concern for long-term global peace, so having a number of clever ways to keep an ear out for testing programs wouldn't go astray.

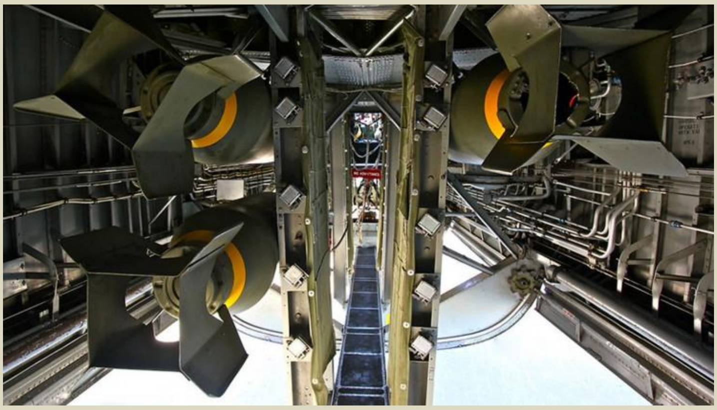
To the citizens of Beirut, the devastation of the 2020 port explosion is just one more insult piled on top of economic distress and the scourge of the coronavirus pandemic. It's not an event anybody would care to see repeated elsewhere; learning all we can about its impact can ensure it won't be.

▶▶ **This research was published in *Scientific Reports*.**

## E-Bombs: The Allure and Peril of High-Power Microwave Weapons

**By Christopher McFadden**

Source: https://interestingengineering.com/e-bomb-peril-high-power-microwave-weapons



Mar 20 – Good news! For those worried about the imminent take over of AI and robots, humans may have an "Ace card" up our sleeves — the E-bomb. These electronic weapons of mass destruction might just be the trick for knocking out any want-to-be Skynet in the near future.

Likely, these bombs may just represent one of the most serious threats to our modern tech-dominated lives after the nuclear bomb. Whether by belligerent nations or terrorists, such bombs could be used to wreak havoc without a bullet ever taking flight. Prepare to be shocked.

**What is an E-bomb?**

An electromagnetic bomb, or E-bomb for short, is a device that generates a high-power electromagnetic pulse and/or high-power microwave pulse, that is capable of severely damaging, or rendering completely useless, electronic devices within its pulse radius. Similar in concept to a conventional high-explosive bomb, the damage caused is not from the bomb's physical ability to destroy a target object, but rather its devastating effect on electronic devices and networks.

While few E-bombs currently exist (as far as we know) these kinds of bombs could prove devastating to nations that are heavily reliant on electrical and digital infrastructures. In fact, a form of NNEMP (non-nuclear E-bomb) was reportedly used to disable Saddam Hussein's propaganda network during the 2003 Invasion of Iraq.

Theoretically, such bombs could be used to disable a target nation's digital infrastructure and economy, potentially causing internal unrest, severely damaging their ability to wage war, and ultimately potentially create a societal collapse.

Similar EMP bursts are often observed during nuclear weapon detonations that propagate rapidly fluctuating electric and magnetic fields resulting in damaging current and voltage surges. Although, the term E-bomb often refers to non-nuclear EMP weapons (NNEMP).

EMP blasts can also be observed in nature, often associated with lightning storms and solar storm events. However, the impacts of the former tend to be more localized and small-scale. Solar storms, on the other hand, could arguably be more severe than a theoretical E-bomb attack.

These bombs potentially offer a greater threat to modern nations than atomic weapons, as digital hardware is now all-pervasive and increasingly critical to many developed economies. With drives for ever-more increased interconnectivity, like the Internet of Things, the potential threat these weapons would offer in the future is only set to increase exponentially.

With the increasing reliance on digital technology in military assets, such bombs could also prove devastating to naval, airborne, and ground-based military targets or communications.

While the threat these weapons pose might sound fanciful, some experts are so worried about them that they have been warning about the potential danger for many years. Unfortunately, these concerns have all-too-often fallen on deaf ears.

Some have even gone as far as to say that we may well see a real E-bomb attack within the next decade or so.

**How do E-bombs work?**

In our digitally-interconnected modern world, weapons like E-bombs could prove to be very dangerous indeed. One of the main reasons for this is the proliferation of electronic machinery and digital hardware around the world throughout the 20th and 21st centuries.

Digital infrastructure exists everywhere today in many nations, with applications varying from handheld devices, domestic or office equipment, transportation (like smart cars), production, health, to power plants. While the benefits of such digital integration are incalculable, the electronics used in any digital infrastructure could be a very serious chink in the armor of a nation's security with regards to E-bomb vulnerability. This could include infrastructure systems such as nuclear power plants, and water and sewer management plants.

Any exposure of these systems, be it to transient or radiant frequency, in excess of their specified voltage limit could result in very serious damage.

Not all EMp devices are hostile. This "friendly" EM Environment Simulator is used to test the effects of EMP pulses on electronic devices. *Source: Sandia Labs/Fliclr*

For example, most electronic devices will break down through a number of over-voltage-related mechanisms. An attack from a large enough E-bomb, or set of smaller ones could cause transient dropouts, lead to longer-term "wounds" in the system, or even end up with a complete electrical failure. A big enough surge could not only burn out semiconductor devices, but could melt wiring, fry batteries, and even explode transformers. All within the weapon's so-called "lethal footprint".

This is effectively the EMP "blast radius" of the E-bomb. EMP blasts tend to occur over three discrete phases. First seen in nuclear detonations, these are:

1. The initial near-instantaneous pulse (sometimes referred to as the "E1" phase).
2. A subsequent high-amplitude phase, aka the "E2" pulse.
3. And, the final lower-amplitude (but still damaging) "E3" pulse.

You can liken an E-bomb to a device that cracks a dyke or dam allowing an uncontrolled flood of electricity (the water being held back by the dyke) in its wake.

The first phase ("E1") causes most of the damage by inducing a voltage in electronic conductors beyond their safety tolerances (i.e. it cracks the dyke). The next phase ("E2") acts in a similar fashion to a lightning strike and would likely be the least damaging, assuming lighting protection is not compromised from the "E1" pulse.

The third, and final, "E3" pulse can last from seconds to minutes and occurs when the fireball (if explosively generated) from the initial blast temporarily warps the Earth's magnetic field. This is the phase that could cause the highly damaging cascading damage to digital infrastructures (more on this later).

Exposure to massive bursts of EM energy can cause dielectric insulators (like MOSFETs, which are metal-oxide-semiconductor field-effect transistors) to break down or leak, and reverse-biased junctions can suffer avalanche breakdowns. Once things like MOSFETs are compromised, they are no longer able to switch/control current flow and electrons are able to freely move between the source (power supply) and drain.

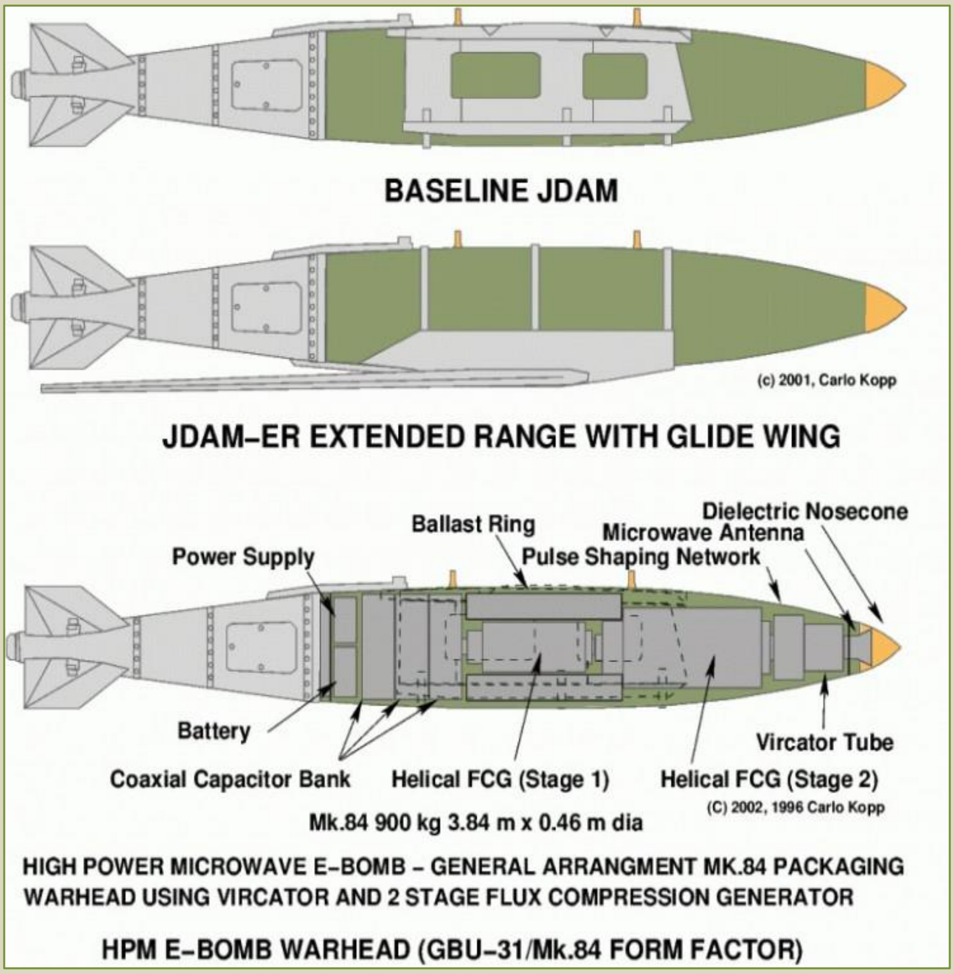
Another problem is the consequential build-up of heat in electronics too. According to Ohm's law, higher voltages tend to increase the amount of current in electrical circuits leading to a chain reaction in heat generation because of a semiconductor's negative temperature coefficient. This heat, while likely not high enough to melt the semiconductors, will probably be enough to melt thin metal wires and epoxy, resulting in burnouts.

Grid or battery-powered devices often require very little energy to actually initiate this kind of catastrophic failure.

After the initial EMP pulse and with insulators damaged, the power supply (be it battery or mains), can flow unimpeded wreaking havoc in electrical circuitry.

For this reason, one of the most important potential impacts from E-bomb attacks is the cascading damage caused within a nation's digital infrastructure. The failure of one device in the system, could, potentially, trigger an overload in another, and then another, so on and so forth all the way along the network.

For large interconnected systems, like those in developed nations, E-bomb attacks could lead to a total power grid, and/or digital network, collapse.


BASELINE JDAM
(c) 2001, Carlo Kopp
JDAM–ER EXTENDED RANGE WITH GLIDE WING
Dielectric Nosecone
Ballast Ring
Microwave Antenna
Power Supply
Pulse Shaping Network
Battery
Vircator Tube
Coaxial Capacitor Bank
Helical FCG (Stage 1)
Helical FCG (Stage 2)
(C) 2002, 1996 Carlo Kopp
Mk.84 900 kg 3.84 m x 0.46 m dia
HIGH POWER MICROWAVE E–BOMB – GENERAL ARRANGMENT MK.84 PACKAGING
WARHEAD USING VIRCATOR AND 2 STAGE FLUX COMPRESSION GENERATOR
HPM E–BOMB WARHEAD (GBU–31/Mk.84 FORM FACTOR)

Examples of theorized E-bombs. *Source: ausairpower*

This kind of cascading effect would lead to things like switch mode power supply (SMPS) blowouts that will, in turn, produce electrical spikes in the power grid. This could conceivably cause hundreds of thousands of these to fail near-simultaneously within the peripheral areas to the E-bombs initial "lethal footprint".

As you can imagine, this would be devastating and potentially a very efficient way to severely cripple an enemy nation.

**Which countries have E-bombs?**

The short answer is that we don't really know. While it is known that countries like the US, Russia, EU member states, China, and possibly North Korea have been conducting research into the weaponization of such technology, we can not be entirely sure how much progress has been made.

That being said, and as we previously mentioned, the US appears to have a working example, if reports of their use during the 2003 Invasion of Iraq are correct.

One disconcerting thing to note is that anyone with sufficient knowledge of how a nuclear or conventional bomb works, and access to the required materials, could conceivably make one relatively easily.

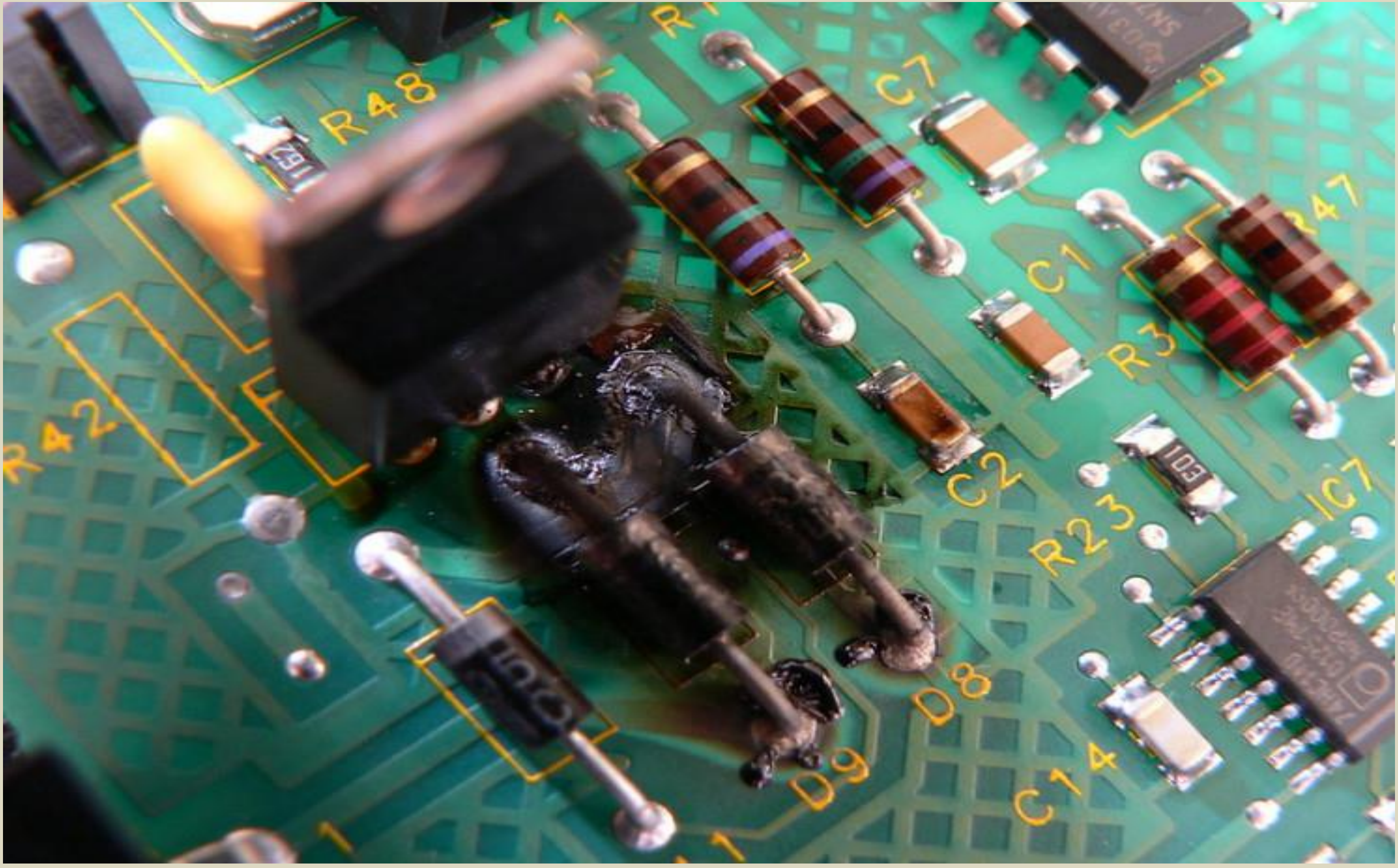
However, this should also bring some form of comfort, as any research team would need to have sufficient physicists with a working knowledge of how to make FCGs (flux compression generators) and vircators (VIRtual CAthode oscillaTOR).

With regards to the equipment and components needed, much of what would be required have existed since the 1950s or so. If someone could get accurate enough schematics, or devise their own, a working E-Bomb could be built for a few hundred to a couple of thousand dollars in uncontrolled materials.

For example, such devices often require access to C4, Semtex, or other high-velocity castable explosives that are readily available.

**What kind of electromagnetic weapons are there?**

You might be surprised to hear that there are actually quite a few of them. However, most generally tend to fall into several types depending on their means of deployment and spectral coverage.



E-bomb attacks would seriously damage electronic circuits and networks. *Source: Rick Kimpel/Flickr*

It is important to note, that various electromagnetic pulse generating equipment is also used for scientific and more benign purposes also.

For their effect, be it steady-state or transient effect, the former tends to consist of things like beam weapons, with the latter one-shot devices like E-bombs. Once activated, or detonated, the spectral coverage released then tends to fall into either wideband or narrowband, high or low frequency, and emitted power.

According to one expert, Carlo Kopp, "a wideband low-frequency low power one-shot weapon might be a submunition for a cluster bomb using a rare earth magnet with a high explosive jacket, while a wideband high-frequency high power repetitively pulsed weapon might be a Marx bank driven Landecker Ring mounted in the focal area of a parabolic dish antenna."

Kopp also happens to be the person who first coined the term "E-bomb" back in the 1990s.

This term has been used to describe both something like a high-altitude, nuclear Electro-Magnetic Pulse (EMP) bomb and has been applied to smaller, non-nuclear devices based on something called a Flux Compression Generator (FCG).

This device, first demonstrated by Max Fowler in the 1940s, uses a fast explosive to rapidly compress a magnetic field, transferring energy from the explosive into the magnetic field. During operation, the FGC would be destroyed, but it would emit enormous amounts of electrical current in the process. If enough of them were detonated in sequence, this current can be amplified into peak power levels of the order of TeraWatts to tens of TeraWatts.

These devices would produce a direct low-frequency wideband effect or could be used as a one-shot pulse power supply for a High Power Microwave (HPM) tube such as a Virtual Cathode Oscillator (Vircator). A vircator is a device used to focus the energy released from an FGC over hundreds of meters, or more, away a bit like the reflector on a torch or car headlight.

**What are the limitations of E-bombs?**

The main limitation of E-bombs, like any other conventional bomb, is their means of delivery to a target. If launched from an aircraft, their effectiveness is completely reliant on the delivery platform's ability to reach and deploy the weapon.

If intended to be delivered by smaller fighter-bomber jets, for example, the size of the E-bomb will be limited. Delivery by larger intercontinental ballistic missiles (ICBM) would offer the potential for higher payloads, but would also drastically increase the cost per unit.

Interestingly, another limitation of E-bombs is also their intended target. If older electronics are used, for example, thermionic technology rather than solid-state, the target would have some resilience to an E-bomb attack.

Some other targets, like radar installations, may also appear to have been unaffected if they continue to radiate radar signals after an attack. While receiving equipment will likely have been knocked out of action, this would not be obvious to an observer. Shutting off such systems prior to an attack could also be used to "fool" attacking forces into thinking an attack has been successful too.

**Can digital infrastructure be protected from E-bombs?**

Are you scared yet? The good news is that while E-bombs are potentially incredibly destructive devices, there are things that can be done to protect against them — electromagnetic hardening of digital infrastructure.

This process involves the "hardening" of digital equipment and power supplies. One example is to replace all metallic cabling (especially old copper wiring) with optical fiber alternatives in networks. Others include installing protection devices into antenna feeds, and grid power interfaces.

Other options include enclosing critical electronic systems within conductive enclosures, like a Faraday cage. However, systems inside the cage would still need connectivity or power from outside it, which can still present a vulnerability.

Under such circumstances, electromagnetic arresting devices could prove incredibly useful.

While homeowners can do this to their own homes to some extent, it is important to note it is more critical to protect the main grid and telecom networks. A protected, working computer will be practically useless with no grid power or internet connection should an E-bomb be detonated.

Retroactive hardening of this kind would be costly, and time-consuming, for most developed nations, but if experts in the field are correct, E-bombs are quite literally, a ticking time bomb. It is not a matter of if, but when, an E-bomb attack is seen.

If decision-makers in governments can be convinced to take the problem seriously, rather than treat it as an esoteric or ethereal fantasy, only then can nations fortify their electronic defenses. Even if they are never needed.

If newer devices and installations could be "hardened" from the outset, this will save time and shouldn't add that much extra cost (estimates range from 10 to 20%) at the point of purchase or commission.

Even if E-bombs never really materialize as a potential national security threat in the near term, the hardening of our digital infrastructures might be a good idea anyway. After all, concerns about acts of nature like Coronal Mass Ejections, and other solar events, have been shown to disable electrical systems here on Earth.

Two birds with one stone, if you like. So far, we've been lucky, but large future solar storm events are an inevitability.

***Christopher McFadden** graduated from Cardiff University in 2004 with a Masters Degree in Geology. Since then, he has worked exclusively within the Built Environment, Occupational Health and Safety and Environmental Consultancy industries. He is a qualified and accredited Energy Consultant, Green Deal Assessor and Practitioner member of IEMA. Chris's main interests range from Science and Engineering, Military and Ancient History to Politics and Philosophy.*

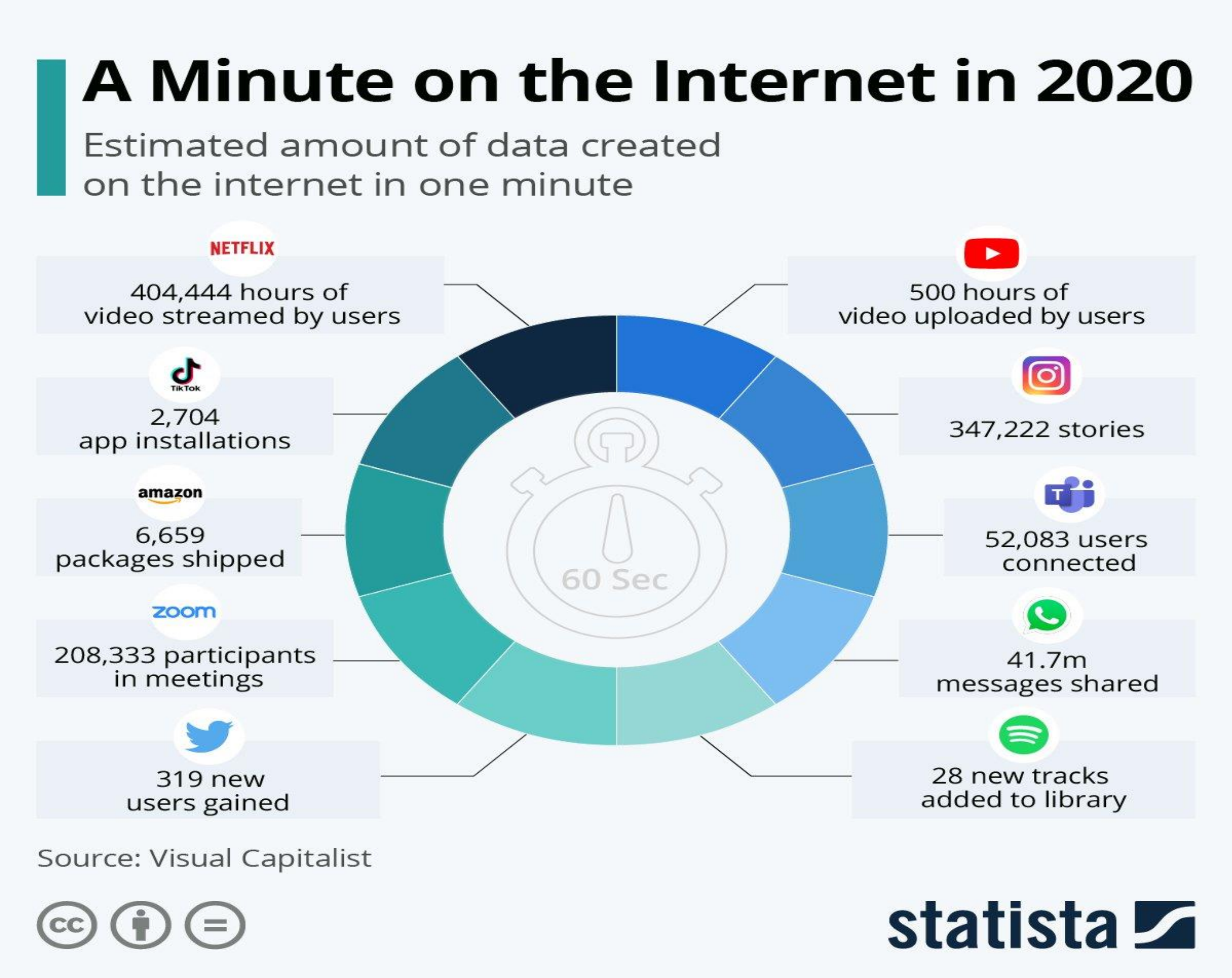
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C$^2$BRNE DIARY

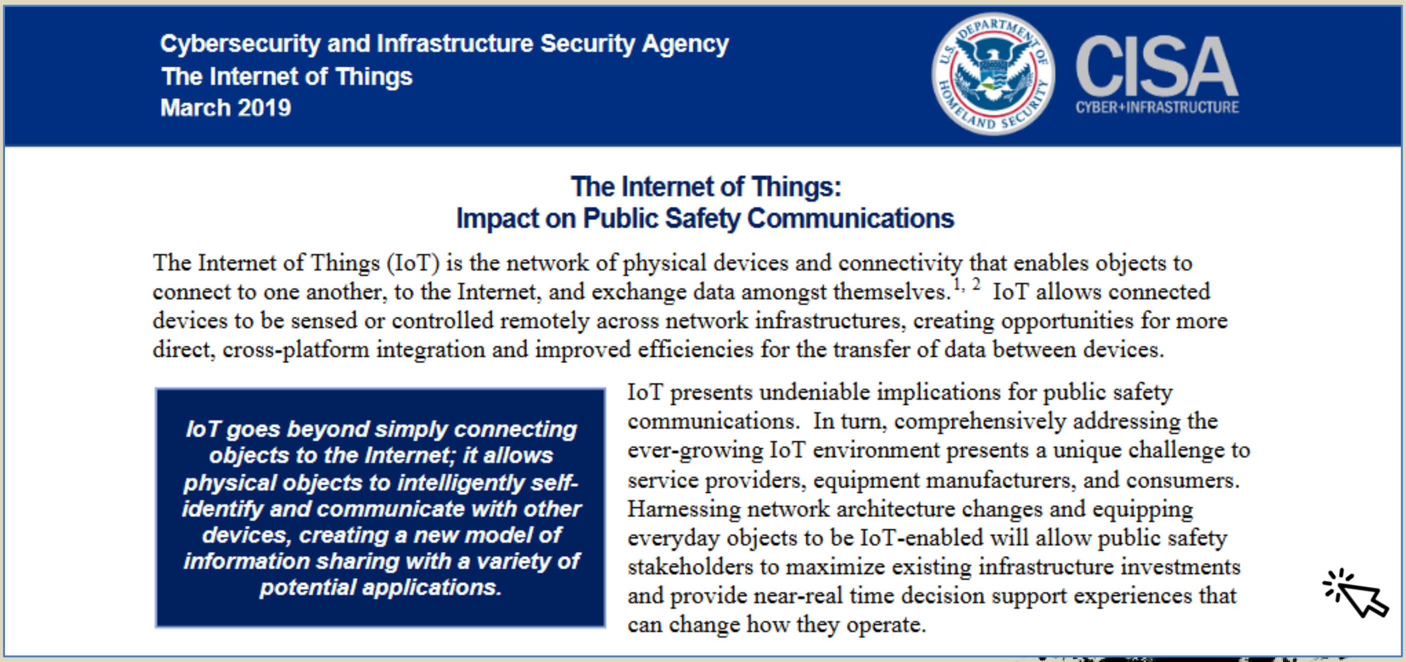
# CYBER NEWS



## A Minute on the Internet in 2020

Estimated amount of data created on the internet in one minute

Source: Visual Capitalist



Cybersecurity and Infrastructure Security Agency
The Internet of Things
March 2019

CISA
CYBER+INFRASTRUCTURE

### The Internet of Things: Impact on Public Safety Communications

The Internet of Things (IoT) is the network of physical devices and connectivity that enables objects to connect to one another, to the Internet, and exchange data amongst themselves.[1, 2] IoT allows connected devices to be sensed or controlled remotely across network infrastructures, creating opportunities for more direct, cross-platform integration and improved efficiencies for the transfer of data between devices.

*IoT goes beyond simply connecting objects to the Internet; it allows physical objects to intelligently self-identify and communicate with other devices, creating a new model of information sharing with a variety of potential applications.*

IoT presents undeniable implications for public safety communications. In turn, comprehensively addressing the ever-growing IoT environment presents a unique challenge to service providers, equipment manufacturers, and consumers. Harnessing network architecture changes and equipping everyday objects to be IoT-enabled will allow public safety stakeholders to maximize existing infrastructure investments and provide near-real time decision support experiences that can change how they operate.

# IBM Report: Attacks on Healthcare, Manufacturing and Energy Doubled in 2020

Source: https://www.hstoday.us/industry/ibm-report-attacks-on-healthcare-manufacturing-and-energy-doubled-in-2020/

Mar 02 – IBM Security has released the **2021 X-Force Threat Intelligence Index** highlighting how cyberattacks evolved in 2020 as threat actors sought to profit from the unprecedented socioeconomic, business and political challenges brought on by the COVID-19 pandemic.

In 2020, IBM Security X-Force observed attackers pivoting their attacks to businesses for which global COVID-19 response efforts heavily relied, such as hospitals, medical and pharmaceutical manufacturers, as well as energy companies powering the COVID-19 supply chain.

According to the new report, cyberattacks on healthcare, manufacturing, and energy doubled from the year prior, with threat actors targeting organizations that could not afford downtime due to risks of disrupting medical efforts or critical supply chains. In fact, manufacturing and energy were the most attacked industries in 2020, second only to the finance and insurance sector. Contributing to this was attackers taking advantage of the nearly 50% increase in vulnerabilities in industrial control systems (ICS), which manufacturing and energy both strongly depend on.

“In essence, the pandemic reshaped what is considered critical infrastructure today, and attackers took note. Many organizations were pushed to the front lines of response efforts for the first time – whether to support COVID-19 research, uphold vaccine and food supply chains, or produce personal protective equipment,” said Nick Rossmann, Global Threat Intelligence Lead, IBM Security X-Force. “Attackers’ victimology shifted as the COVID-19 timeline of events unfolded, indicating yet again, the adaptability, resourcefulness and persistence of cyber adversaries.”

The X-Force Threat Intelligence Index is based on insights and observations from monitoring over 150 billion security events per day in more than 130 countries. In addition, data is gathered and analyzed from multiple sources within IBM, including IBM Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services, and data provided by Quad9 and Intezer, both of which contributed to the 2021 report.

Some of the report’s key highlights include:

- Cybercriminals Accelerate Use of Linux Malware – With a 40% increase in Linux-related malware families in the past year, according to Intezer, and a 500% increase in Go-written malware in the first six months of 2020, attackers are accelerating a migration to Linux malware, that can more easily run on various platforms, including cloud environments.
- Pandemic Drives Top Spoofed Brands – Amid a year of social distancing and remote work, brands offering collaboration tools such as Google, Dropbox and Microsoft, or online shopping brands such as Amazon and PayPal, made the top 10 spoofed brands in 2020. YouTube and Facebook, which consumers relied on more for news digestion last year, also topped the list. Surprisingly, making an inaugural debut as the seventh most commonly impersonated brand in 2020 was Adidas, likely driven by demand for the Yeezy and Superstar sneaker lines.
- Ransomware Groups Cash In On Profitable Business Model – Ransomware was the cause of nearly one in four attacks that X-Force responded to in 2020, with attacks aggressively evolving to include double extortion tactics. Using this model, X-Force assesses Sodinokibi – the most commonly observed ransomware group in 2020 – had a very profitable year. X-Force estimates that the group made a conservative estimate of over $123 million in the past year, with approximately two-thirds of its victims paying a ransom, according to the report.

Amid the COVID-19 pandemic, many businesses sought to accelerate their cloud adoption. “In fact, a recent Gartner survey found that almost 70% of organizations using cloud services today plan to increase their cloud spending in the wake of the disruption caused by COVID-19.” But with Linux currently powering 90% of cloud workloads and the X-Force report detailing a 500% increase in Linux-related malware families in the past decade, cloud environments can become a prime attack vector for threat actors.

With the rise in open-source malware, IBM assesses that attackers may be looking for ways to improve their profit margins – possibly reducing costs, increasing effectiveness and creating opportunities to scale more profitable attacks. The report highlights various threat groups such as APT28, APT29 and Carbanak turning to open-source malware, indicating that this trend will be an accelerator for more cloud attacks in the coming year.

The report also suggests that attackers are exploiting the expandable processing power that cloud environments provide, passing along heavy cloud usage charges on victim organizations, as Intezer observed more than 13% new, previously unobserved code in Linux cryptomining malware in 2020.

With attackers' sights set on clouds, X-Force recommends that organizations should consider a zero-trust approach to their security strategy. Businesses should also make confidential computing a core component of their security infrastructure to help protect their most sensitive data – by encrypting data in use, organizations can help reduce the risk of exploitability from a malicious actor, even if they're able to access their sensitive environments.

The 2021 report highlights that cybercriminals opted to disguise themselves most often as brands that consumers trust. Considered one of the most influential brands in the world, Adidas appeared attractive to cybercriminals attempting to exploit consumer demand to drive those looking for coveted sneakers to malicious websites designed to look like legitimate sites. Once a user visited these legitimate-looking domains, cybercriminals would either seek to carry out online payment scams, steal users' financial information, harvest user credentials, or infect victims' devices with malware.

The report indicates that the majority of Adidas spoofing is associated with the Yeezy and Superstar sneaker lines. The Yeezy line alone reportedly pulled in $1.3 billion in 2019 and was one of the top selling sneakers for the sportswear manufacturing giant. It's likely that, with the hype for the next sneaker release in early 2020, attackers leveraged the demand of the money-making brand to make their own profit.

According to the report, in 2020 the world experienced more ransomware attacks compared to 2019, with nearly 60% of ransomware attacks that X-Force responded to using a double extortion strategy whereby attackers encrypted, stole and then threatened to leak data, if the ransom wasn't paid. In fact, in 2020, 36% of the data breaches that X-Force tracked came from ransomware attacks that also involved alleged data theft, suggesting that data breaches and ransomware attacks are beginning to collide.

The most active ransomware group reported in 2020 was Sodinokibi (also known as REvil), accounting for 22% of all ransomware incidents that X-Force observed. X-Force estimates that Sodinokibi stole approximately 21.6 terabytes of data from its victims, that nearly two-thirds of Sodinokibi victims paid ransom, and approximately 43% had their data leaked – which X-Force estimates resulted in the group making over $123 million in the past year.

Like Sodinokibi, the report found that the most successful ransomware groups in 2020 were focused on also stealing and leaking data, as well as creating ransomware-as-a-service cartels and outsourcing key aspects of their operations to cybercriminals that specialize in different aspects of an attack. In response to these more aggressive ransomware attacks, X-Force recommends that organizations limit access to sensitive data and protect highly privileged accounts with privileged access management (PAM) and identity and access management (IAM).

Additional key findings in the report include:

- Vulnerabilities Surpass Phishing as Most Common Infection Vector – The 2021 report reveals that the most successful way victim environments were accessed last year was scanning and exploiting for vulnerabilities (35%), surpassing phishing (31%) for the first time in years.
- Europe Felt the Brunt of 2020 Attacks – Accounting for 31% of attacks X-Force responded to in 2020, per the report, Europe experienced more attacks than any other region, with ransomware rising as the top culprit. In addition, Europe saw more insider threat attacks than any other region, seeing twice as many such attacks as North America and Asia combined.

## Cyber Mercenaries in Demand as Organizations Hire Their Services

Source: https://www.hstoday.us/industry/cyber-mercenaries-in-demand-as-organizations-hire-their-services/

Mar 01 – **BlackBerry Limited has released its 2021 Threat Report**, detailing a sharp rise in cyberthreats facing organizations since the onset of COVID-19. The research shows a cybercrime industry which not only adapted to new digital habits, but also became increasingly successful in finding and targeting vulnerable organizations. The research also highlights a dangerous new shift in the cybercrime world, one where mercenaries and crimeware-as-a-service models have become increasingly accessible.

At the outset of the pandemic, countless organizations suddenly had to support a large proportion of their workforce remotely, with many forced to digitize various parts of their infrastructure overnight. This evolution and adoption of digital offerings exposed companies to inadequate protections for employees and customers amongst an ever-growing and under-secured attack surface. There was also a greater merging of cyber and physical threats, with cybercriminals increasingly targeting healthcare organizations or using the pandemic to trick already vulnerable populations.

“The cybersecurity industry becomes more complex each passing year as new technologies, devices and innovations emerge – and at no time was that truer than in 2020, which witnessed everything from a global pandemic to the U.S. election,” said Eric Milam, Vice President of Research and Intelligence, BlackBerry. “As the world becomes more interconnected and as new dimensions to cybercrime continue to rise, preparation will become a key factor in successful threat prevention in 2021.”

The report highlights a burgeoning crimeware-as-a-service business model as well as the increasing sophistication and collaboration of these hacker-for-hire groups. Not only was the ransomware-as-a-service model highly successful – especially as more non-digital natives transacted online – but the additional research into threat actors such as BAHAMUT and CostaRicto shows that these groups possess the tools once thought to be solely the domain of nation-state attackers. This presents a new danger for companies, one where attacks can be more frequent, skillful and targeted.

**Key findings in the report include:**

- Ransomware attacks shifted from performing indiscriminate targeting to conducting highly focused campaigns deployed via compromised MSSPs
- Elections remained vulnerable to cyber attacks through unsecured mobile technology, insufficient DMARC email protection, and over-exposure of personal information on social media
- Global automakers faced new regulations to protect connected vehicles from cyber attacks and data theft
- Numerous phishing campaigns targeted critical infrastructure systems across manufacturing, healthcare, energy services and food supply sectors
- Mercenary threat groups experienced a year of growth as unscrupulous actors and organizations outsourced their cyber attacks
- Ransomware-as-a-service offerings grew in popularity, replacing traditional off-the-shelf ransomware with ready-made exploit kits, malspam campaigns and threat emulation software
- Newer APT groups like CostaRicto targeted disparate victims worldwide with their customized backdoors and tooling
- Emotet, the banking trojan turned attack platform, received new upgrades and capabilities, including a flaw that allowed BlackBerry researchers to easily identify and prevent it from installing on systems

“As both public and private organizations work to meet cyber espionage groups at ground zero, the foundation for robust security practices remains unchanged. From round-the-clock monitoring to AI-driven security tools and insider threat detection, the same time-tested security fundamentals – and an understanding of how current events impact an organization’s attack surface – can make the difference between a data breach and a successful cyber defense,” Milam said.

▶▶ Download the report at BlackBerry

## Why Cybersecurity is Becoming a Top Priority for Drug Makers

**By Sonit Jain** (CEO, GajShield Infotech)
Source: https://www.expresscomputer.in/industries/pharma/why-cybersecurity-is-becoming-a-top-priority-for-drug-makers/73680/

Mar 09 – In the last ten years, we’ve witnessed a dramatic rise in the number of novel disease outbreaks globally. Leading pharmaceutical companies have been working rigorously to develop newer drugs to effectively counter these threats. The relentless pressure to innovate and produce medicines has pushed major drug companies to embrace digital technology. And as the pharma industry moves towards complete digitalisation, the shadow of cyber threats now looms larger than ever. This is evident from the startling levels of sophistication in cybercrimes this millennium has seen already.

Pharmaceutical companies need to be vigilant and proactive to prevent the security breaches caused by external as well as internal actors. A failure to keep data security measures updated can prove disastrous for drug companies in several ways. The issues that can stem from weak or incoherent cyber protection include:

### Patient Data Leaks

Pharmaceutical companies are gradually moving towards becoming more patient-centric. They store information about individual customers to serve them in a more personalised way. A Cambridge-based biotech company offers a good example of deploying a more patient-centric approach towards drug formulation. The biotech company had collaborated with Parent Project Muscular Dystrophy (PPMD), an advocacy group, and had used the latter’s patient preference study to get faster approval for the first disease-modifying therapy for the Duchenne muscular dystrophy. A compromise in the confidential data can be dangerous for the customer. Moreover, a data leak will end up having legal ramifications for the pharmaceutical company.

The pharma company must, therefore, be extra careful with this data to maintain consumer relationships and avoid litigation.

### Pharmacovigilance Audit Issues

Pharmacovigilance is the science related to collection, detection, monitoring, assessment, and prevention of adverse effects with pharmaceutical products. The pharmacovigilance audits are used to verify the quality of manufactured drugs for mass usage. Pharmaceutical companies are obligated to provide information about new drugs to regulatory bodies. From a security perspective, the sensitive and confidential data present in these audits is vulnerable to tampering by cybercriminals. It is important for the designated cybersecurity agency to make sure that the information from the pharmacovigilance audits is prevented from unauthorised alterations. Any tampering of data present in the audit reports poses significant threats to the company in a few ways. For instance, medicines not approved for commercial use by regulatory bodies pose health risks for potential consumers if they are greenlit for production.

### Data Compromise by Employees

There is always a chance of employees becoming disillusioned with company management for some reason or another. Employees who are discontent with the way they are treated in the organisation could negatively impact the company from within. Pharmaceutical companies, especially, have a lot to lose if their confidential medicinal ingredients and formulation processes are exposed in the public domain. To sort this out, a few measures could be taken by the management. Firstly, the higher-level employees at any organisation must know about the prevailing issues within their subordinate ranks. The data leaks can happen by an employee's negligence too. It is vital for the pharmaceutical company to play safe with regards to keeping their secret details hidden from the public view. It is the job of the cybersecurity team to ensure that the confidential details of the drug manufacturer are protected at all times.

### Problems with Internet of Things

The Internet of Things could cause issues such as AI-driven security threats, cloud attacks, issues related to a lack of knowledge regarding it amongst others. The team responsible for installing such complex and synchronised systems must also undertake the training of the employees to ensure that malfunctions are avoided. Moreover, the cybersecurity team must ensure that data leaks and attacks from external sources are prevented. As mentioned earlier, pharmaceutical companies stand to lose much more than most regular companies when a data leak occurs.

### Chemical Terrorism

Chemical terrorism is the utilisation of harmful chemicals to cause widespread damage. The emission of dangerous chemicals at any location can have adverse effects on biological and environmental levels. Drug-making companies utilise several elements to manufacture proprietary drugs. These companies store large amounts of confidential data related to pharmaceutical formulation in their databases. Modern cybercriminals possess the knowhow to breach security protocols and gain access to this data. Certain standalone elements in these drugs are extremely dangerous in an open environment. If they end up in the wrong hands, the perpetrators could use the elements to wreak havoc on large swathes of people and the environment. Although extreme to an extent, the possibility of such an attack cannot be overlooked by pharmaceutical companies. They must make sure to safeguard the formulation data by using the services of experienced and reputed cyber protection agencies.

The ongoing COVID-19 pandemic and other health-related issues have resulted in pharmaceutical companies being a hot topic of discussion globally. These drug makers possess vast amounts of essential information which is critical in the current scenario. As specified earlier, technology plays a big part in the drug producers' operations. The threat of cyber-attacks makes it vital for such companies to adopt extensive

## When Does a Cyber Attack Become an 'Act of War'?

**By Karan Tripathi**

Source: https://www.thequint.com/news/law/is-cyber-attack-an-act-of-war

Mar 07 – Recorded Future, a US-based firm, has reported that Chinese state-sponsored actors may have used malware to target India's power grid system and seaports. According to the New York Times, which broke this story, Recorded Future has claimed in its report that the 12 October 2020 grid failure in Mumbai, may have been caused by this malware.

This report has come in the backdrop of escalating border tensions between India and China, which actually led to a deadly skirmish at the Line of Actual Control (LOAC) in June 2020.

As there's a history of hostility between the two nations, the legality of such cyberattacks becomes a serious question. Are these cyberattacks a part of a larger armed conflict or a means to unleash an armed attack? Can these cyberattacks be attributed to the ongoing conflict between the two sovereign nations?

Most importantly, can India interpret Chinese hacking as an attack on its 'political independence or sovereignty'? Does the international law on armed conflict describe such cyber attacks as an 'armed attack'? Can India retaliate? If yes, then in what manner? These questions can be answered by looking at cyber attacks through the lens of the law on wars.

### 1. Cyberspace: A New Battlefield

Almost every country is now using computer systems for their civil, security, and military infrastructure. This has made cyberspace attractive to both, state and non-state actors, to target the 'vulnerable' systems of rival countries to cause significant disruption at a far lower cost, in money and manpower, than conventional and mainly military options.

Countries with advanced cyber capabilities have shown keen interest in targeting cyberspace for strategic interventions in other countries.

1. In 2020, both Iranian and the American governments acknowledged cyber-attacks as central to their strategies.
2. In 2010, Stuxnet, which some consider India's first genuine cyber weapon, reportedly destroyed a fifth of Iran's nuclear centrifuges.
3. Russia has consistently targeted the critical civil infrastructure of Ukraine, leading to a large-scale disruption to the internet as pro-Russian rebels took control of Crimea (2014), taking down the election commission 3 days before Ukraine's Presidential elections (2014), and cutting off the power supply to around 250,000 people in western Ukraine.
4. In 2007, a major cyber-attack on Estonia's banking and communications system led to 22 days of civil unrest.

USA has established 'cyber commands' as part of its Air Force and Navy. There is a consensus among NATO member-nations to invoke the principle of 'collective self-defence' when faced with complex cyber-attacks. South Korea and Saudi Arabia are also developing systems to "retaliate" when faced with "coordinated" and "sophisticated" cyber-attacks.

### 2. Not Every Attack Is War

While experts are divided on whether the existing framework of the law on armed conflict (LOAC) should be extended to cyber-attacks or not, there is broad agreement on distinguishing different kinds of cyber aggression.

Every act of cyberspace targeting won't amount to an 'attack' so as to invoke laws governing war. Centre for Strategic and International Studies, an American think-tank, argues that merely a violation of sovereignty is not enough. To invoke the right to self-defence under international law, an aggrieved nation will have to show that a cyber attack led to 'substantial death' or 'physical destruction' so as to qualify as an 'armed attack'.

**The Tallinn Manual, a leading document on legality of cyber-warfare prepared by 19 international law scholars, recognise only those cyber attacks as part of armed conflict which "are reasonably expected to cause injury or death to persons or damage or destruction to objects".**

Therefore, the threshold is understandably high. Instances of cyber espionage or data theft would ordinarily not justify action or retaliation under the law on armed conflict.

### 3. How Can Law of War Apply to Cyber Warfare?

The law on armed conflict consists of rules and state practices governing decisions to go to war and how to fight a war. Over the decades, the Geneva Convention, The Hague Convention, and the UN Charter, have been used to determine what amounts to 'war' and what kind of retaliation can be justified.

The existing framework for law on armed conflict doesn't envisage cyber warfare. While some experts say that cyber warfare can be read into the existing legal framework, others argue that it is inadequate and a new legal framework is required. However, there is a consensus on the threshold of 'substantial damage' that every cyber-attack will have to meet to qualify as an act of war.

**The Tallin Manual uses the definition provided in Article 2(4) of the UN Charter to argue that any cyber operation that "constitutes a threat or use of force against the territorial integrity or political independence of any state, or that in other manner is inconsistent with the purposes of United Nations is unlawful". Such a cyber operation could trigger a response under the law on armed conflict.**

### 4. Who's the Enemy: The Problem of Fixing Blame

Unlike conventional warfare, it is extremely difficult to conclusively identify the source of a transnational cyber attack. For instance, the Stuxnet attack against Iran is largely attributed to the US and Israel, but there's no conclusive evidence for it. Similarly, while Germany

blames Russia for hacking the computer systems of its Bundestag (Parliament), Russia is able to deny it, as there isn't sufficient proof.

**Another issue is the involvement of anonymous non-state actors. Most malware that has attacked critical civil infrastructure, including the recent Chinese malware in the Indian power system, has been attributed to private players. These non-state actors may very well be state-sponsored, but without conclusive evidence establishing a direct link, accusing another state of 'an act of war' would be diplomatically foolhardy.**

Then there's a problem of 'spoofing'. Persons initiating a cyber attack can resort to 'spoofing', which is falsify the identity of their server. For instance, a cyber system in Russia can initiate an attack, but while doing so, can falsify the identity of its server to suggest that the attack was routed through China. This further complicates the problem of attribution in cyber warfare.

Some scholars, however, have suggested that states can act under the laws of armed conflict, even against non-state actors. They cite post 9/11 cyber operations of the US as a 'state practice' that has validated the use of retaliatory force against non-state actors as well.

The Tallinn Manual puts an obligation on states to not allow their cyber-infrastructure to be used for unlawful activities against other states. This obligation applies regardless of whether an attack is attributable to a state actor or not.

**A state shall not knowingly allow the cyber infrastructure located in its territory or under its control to be used for acts that adversely and unlawfully affect other states. [Tallinn Manual]**

Scott J. Shackelford, an expert on the law of cyber warfare, argues that there's no need to prove complete state control to attribute a cyber attack. Even if the state had an 'operational control' on the cyber-infrastructure used to target other states, the attack can be attributed to it.

### 5. How Can 'Attacked' States Retaliate?

Once the issue of attribution is resolved, or largely agreed upon, the next step would be to assess what level of cyber counter operation would be permissible under the law of armed conflict.

**Rule 13 of the Tallinn Manual states that a state targeted by a cyber operation that "rises to a level of an armed attack" would be allowed to exercise its "inherent right of self-defence" as enshrined under Article 51 of the UN Charter and customary international law. However, the force used by a state in its self-defence cyber operation should be proportionate and necessary.**

Mike Schmitt, an authority on cyber warfare and international law, argues that a state can still respond to a cyber operation that doesn't meet the threshold of 'armed conflict' if the said cyber operation is part of an overall operation culminating in an armed attack or is an "irrevocable step in an imminent (near-term) and probably unavoidable attack".

### 6. Pre-emptive Measures for A Potential War?

Experts are divided over treating cyber warfare and conventional warfare as the same under international law. But they all recognise the potential threats that cyber warfare can pose in the future, including the prospect of what Barack Obama called the 'cyber arms race'.

The Weapons Review of the International Committee of the Red Cross (ICRC) has asked all states to ensure that the means of cyber warfare that they acquire or use comply with the rules of LOAC that bind all states.

Vincent Boulanin and Maaike Verbruggen of the Stockholm International Peace Research Institute (SIPRI) have argued for subjecting 'cyber capabilities' or 'cyber weapons' of states to a process that periodically reviews their compliance with the law on armed conflict. Such a legal review should address the following critical aspects of a state's cyber capabilities:

1. Is it, in its normal and intended circumstances of use, likely to cause superfluous injury or would it lead to unnecessary suffering?
2. Is it by nature indiscriminate? Under International Humanitarian Law, indiscriminate attacks are prohibited.
3. Would its use be intended to, or be expected to, breach LOAC rules? The LOAC prohibits the use of certain kinds of weapons in warfare.
4. Is there any provision of a treaty or customary international law that directly addresses it?

**Chatham House, a British think tank, has mooted an arms treaty comparable to the Chemical Weapons Convention, to regulate the cyber warfare. Such a treaty will also provide a framework for distinguishing offensive and defensive cyber weapons, while subjecting the former to prohibition.**

# The Future of Cyberwarfare

**By Shomiron Dasgupta**

Source: https://securityboulevard.com/2021/03/hack/

Mar 11 – Over the years, we have seen an escalation in the series of hacks on health care services, power grids, nuclear plants and our privacy, with no respite. The threat is not just from China alone. It could be from North Korea or, as a matter of fact, from any state or non-state actor. This intent is to destabilize a country.

Cybersecurity is critical for national security and requires indigenization, and the cybersecurity framework of a nation should aim to provide a safe, secure and resilient system for the country's prosperity. Cybersecurity is not the responsibility of an individual or an organization, but of the country as a whole. It is a culture that has to be inculcated. Furthermore, government ministries should be cognizant of the latent threat of cyberwarfare and not behave like an ostrich!

This article walks you through the possible cyberwarfare tactics that could be the knockout blow for democracies around the globe.

## The Future of Cyberwarfare

### Interconnected Lives

We live in a highly connected world. Most of the cities across the globe are connected to computerized systems that connect vehicles, traffic, utility services, people and the government to one another. These connections are themselves connected to grids that manage the networks efficiently; be it the energy grid, the finance grid or the transportation grid, all are connected, interdependent and, sometimes, connected to a super grid.

However, a super-connected smart nation also means security threats that have the potential to destabilize, or at least disrupt, the country. A potential vulnerability on one grid can have a multiplier effect that impacts them all.

### The Cost of Deterrence

Most countries are substantially equipped with weapons of mass destruction. The Federation of American Scientists estimates that Russia possesses 6,800 nuclear weapons, while the United States has 6,185, India has 150 nuclear warheads, while China and Pakistan have 320 and 160, respectively. Certain countries have significant military advantages, with thousands of troops and an advanced infantry, and also are armed with possible allies.

India's latest – and one of the most advanced – medium range artillery guns, the ATAGS Howitzer, comes at a price of USD $3 million; each artillery shell costs USD $14,000. On the other hand, developing a cyber weapon is quite cheap and easy. The Top 10 VPN Hacking Tools Price Index found malware that can be bought for $45, while tutorials on building an attack are available for a mere $5. Considering the fact that, if a nation-state sponsors such attacks and bears the cost, $1,000 to buy a single component for a zero-day exploit or $28,000 for a cell tower simulator kit to intercept call data seems insignificant.

## Cyberwarfare

Cyberwarfare is unlike any war we have witnessed, and will almost certainly be a tragic part of our future. In fact, it has already begun. Cyberwarfare, put simply, will include fighting enemies remotely using new classes of weapons such as computer viruses, malware and programs that alter a system's operability or initiate a complete system shutdown. Cyberattacks will be the new battlefield — unseen, invisible and unpredictable, where hackers from various nations will compete to disrupt economies and lives.

Although there are legal frameworks in place for prosecuting cybercrimes, incidents are exponentially rising — warfare that lets nations or individuals take down organizations and economies without guns and bombs. As the cybercrime statistics of 2020 prove, the most significant threats we face today are threat actors operating from their home desktops with an intent to propagate harm.

The future seems grim, as recent reports reveal state-sponsored cyberwarfare tactics. According to the 2020 Verizon Data Breach Investigation Report ("DBIR"), there's been an increase in state-sponsored espionage-related incidents, ranking only second after organized crime. What's more, Google's Threat Analysis Group (TAG) revealed in October 2020 that it had managed to absorb one of the biggest DDoS attacks in 2017 – a massive bandwidth attack of 2.5 TB per second over six months. In a separate report, Google TAG also revealed that the attack was state-sponsored, wherein the researchers could connect the dots to internet service providers in China.

The list goes on. In February 2020, Iran announced that it faced and eliminated a DDoS against its communications infrastructure that disrupted the internet. In the same month, Chinese hackers tried to steal confidential information on Malaysian government-backed projects through its officials. As reported by the DHS and the FBI, the Russian government has deliberately intruded into the U.S. CI since 2011.

Although the recent power grid failure in Mumbai was the result of human error, the power ministry confirmed cyberattacks happened on their SCADA system. The malware was unable to hit the operating systems, which is a wakeup call to strengthen our cyberfront further. Even the possibility that such a massive power outage could be a result of a state-sponsored attack was enough to send a shiver down a nation's spine, especially during the pandemic.

These attacks are not only limited to data theft, impersonation, malware and viruses. Social engineering attacks that target a specific group are rampant, as well. For instance, in April 2020, it was found that a Russian hacking group forged diplomatic cables and planted articles on social media to turn the masses against the governments of Estonia and the Republic of Georgia.

In 2010, a virus named Stuxnet demolished a secret Iranian nuclear weapons plant. Hackers at Symantec Corporation unraveled its mysteries – what made Stuxnet different was that it impacted the cyber world and caused real-world kinetic damage, which baffled cybersecurity experts. Although Stuxnet's threat actors are still unknown, it was clear from the objective that it was a nation-state that wanted to perpetuate damage in Iran.

## The Cause and Effect

As cybersecurity experts expect more attacks that exploit how "hackable" humans are, it is prudent for countries to be prepared for strategic destabilization from an indirect cyberattack.

Cyberwarfare is a huge challenge, considering the widespread and long-lasting impact an attack can have. Such attacks have penetrated every aspect of our being — call logs, geolocation data and text messages across domains such as manufacturing, media, health care and non-profit sectors.

Cyberweapons have potential to inflict damage that is the equivalent to any other weapon. They can shut down the power grid of an entire city; for example, if the financial capital is out of power, banks can no longer operate or carry out transactions after backup generators fail, the stock exchange will be shut down, and consumers won't be able to withdraw money, as ATMs won't work. A well-orchestrated attack could lead to nationwide panic, as people try to stock up on cash and essentials as soon as possible.

What's more, the ripples of the attack will be felt in other industries — for example, essential utilities such as water treatment plants and waste management will come to a screeching halt. Stores will run out of stock and credit cards won't work, leading to absolute mass panic. An attack on the power grid would also mean blinding the armed forces by shutting down GPS and computer networks. It may take days or weeks for the systems to recover from a strategic cyberattack and return to normalcy.

## Building Cyberresilience

It is estimated that by 2025, cybercrime will cost global economies over $10.5 trillion.

This represents the greatest peril for economic wealth in history, risks the incentives for innovation and investment, and dwarfs the damage inflicted from natural disasters and illegal drugs, combined, in a year.

Fighting the ongoing cyberwar is not going to be easy. Unlike traditional scenarios, where we could trace an IP and threat actor to eliminate both, in the cyber world, the very existence of a malicious module means that several mirrored, infected modules have already been propagated throughout the networks.

What makes threat detection even more difficult is that state-sponsored threat actors rarely draw attention to themselves. They reportedly use limited malware and generic administrator tools to unravel layers of security. They also have been reported to linger in the network for a long time, going undetected for days or months.

These threat actors are motivated by their own sense of nationalism, and are aware of the consequences of their actions. Their attacks may be a type of hacktivism, financially motivated or opportunistic. They may be part of a larger army of cybercriminals available for hire, and some often have close links to the military, intelligence or state administration of their country.

The objective of the undeclared cyberwar is to place persistent mechanisms on networks that may stay dormant for years. Their methodologies also exploit the industry-wide perception that the third party holding one's data is not as vulnerable. Similarly, a company that doesn't consider its data highly confidential or itself a prime target doesn't tend to have appropriate measures in place for threat detection and response.

As a closing note, state-sponsored attacks are highly incentivized and relatively easy to carry out and get away with. It is also increasingly difficult to trace an incident back to a specific country. Thus, countries are now collaborating and innovating to counter such attacks. India, for instance, for the most part a silent observer, is now diving into cyberwarfare to protect

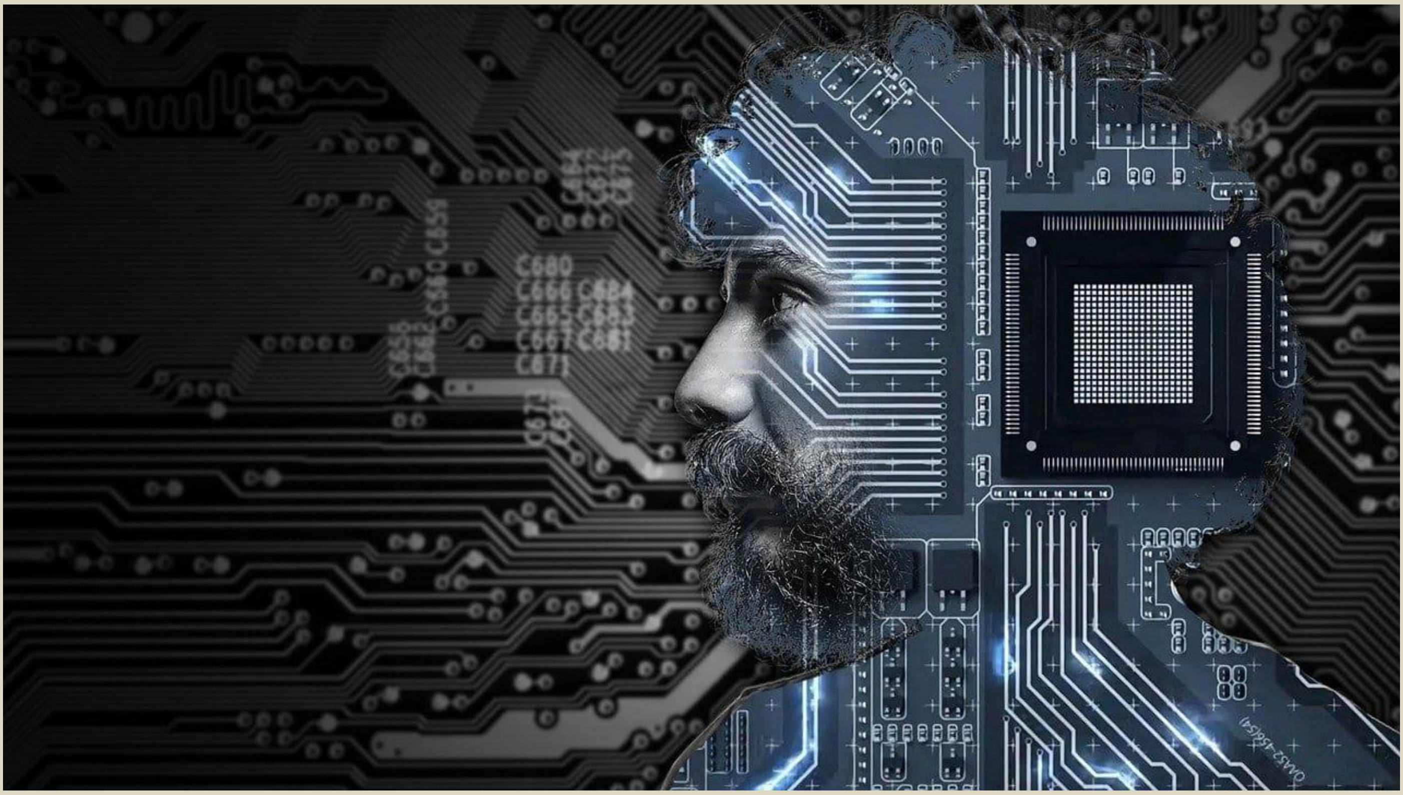
assets, as well. The inherent lack of international norms in this domain will always be a gray area, until addressed seriously. The future may see a full-blown cyberwar if the uncertainty around global cybersecurity regulations persists.

*With his extraordinary skillset as an intrusion analyst and immense passion for tech advancements, **Shomiron Dasgupta** has been building threat detection systems for close to two decades and has established partners in 14 countries across several industries like healthcare, insurance, transport, banking, and media. Prior to founding and developing DNIF, a product that delivers quality attack detection products and services to its customers, he worked with ICICI Infotech Ltd. as a Senior Consultant, where his core responsibility was to solve critical cybersecurity challenges faced by customers. Shomiron, a TedX speaker, is also an eminent speaker at many industry events including DSCI (Data Security Council of India) and SACON (Sálim Ali Centre for Ornithology and Natural History). He is an alumnus of St. Xavier's college. Outside the tech world, he is a trained mountaineer with expedition experience in the high Himalayas.*

## How Predictive AI Will Change Cybersecurity in 2021

**By Dr. Igor Mezić**

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-how-predictive-ai-will-change-cybersecurity-in-2021/



Mar 16 – AI-enhanced cybersecurity is a must in 2021 and beyond. Clearly, the industry agrees – you'll find an endless list of AI security platforms in the marketplace. What do vendors really mean when they use the term "artificial intelligence?" AI can be a fluid term, and sometimes mean different things to different people, and although marketing teams at cyber companies are using this ambiguity to their advantage, too often when it comes to the actual implementation and use of these platforms, the technology and promise fall short of AI in its true scientific sense.

But this isn't always the case. Some artificial intelligence is and will be groundbreaking for the cybersecurity industry. For example, predictive "Third-Wave AI," which is a term originally coined by DARPA to mean contextual and self-adaptable without the need for human training and tuning, can empower organizations to shut down threats before they happen, free from the restrictions and encumbrances of rules-based platforms like SIEM and other legacy AI-enhanced options.

Before you invest in a cybersecurity platform upgrade, carefully consider your options. Second-wave AI solutions may work in the short term, but modern cyber criminals have devised countless ways to break these platforms and programs. To fend off data breaches, malware, ransom attacks and other cyber crimes, SOCs will need more robust, third-wave AI solutions.

### What is Third-Wave AI?

Predictive AI has been a part of cybersecurity for several years now, to varying degrees. The biggest distinction between legacy solutions and modern AI is that third-wave, predictive AI **detects and surfaces threats in real time.**

The U.S. Defense Advanced Research Projects Agency (DARPA) outlines three eras of AI:

- First-wave, rules-based AI enabled "reasoning over narrowly defined problems" with a reduced level of certainty, like early computer chess matches or tax prep software.
- Second-wave, or machine-learning AI, is based on "training statistical models on big data," with minimal capacity for reasoning.
- Third-wave, or unsupervised-learning AI, is context-aware. Machines with third-wave AI "adapt to changing situations."

Predictive AI is a type of machine learning that automatically collects, analyzes and tests data. As it relates to cybersecurity, this technology is often seen in applications like anomaly detection platforms, threat detection and cybercrime prevention.

Predictive AI is patterned on the human brain but powered by the immense power and speed made possible only through computing processes. Today's strongest systems are powered by quantum computing.

### What's Wrong with Second-Wave AI?

Until fairly recently, enterprises and medium-size organizations tended to work with traditional cybersecurity platforms based on first- and second-wave AI. One particularly popular choice has been SIEM (Security Information and Event Management) systems, which rely on a set of rules that "train" AI to detect network anomalies based on expected behavior.

SIEM looks promising on paper, but as many organizations soon became aware, the approach is fundamentally flawed. One overarching issue is the ongoing costs created by SIEM. Basic log storage, incremental analytics and maintenance are all quite costly (and unavoidable).

Security analyst talent is often wasted by SIEM platform functions, as well, due to an overabundance of false positives created in response to context limitations. There are only so many rules the human team can create, and since modern networks rely on constantly evolving baseline behavior, it would be impossible to keep up with all the necessary rules, anyway.

### How Predictive AI Bolsters Network Security

Predictive AI can power modern, responsive cybersecurity platforms, outperforming previous-generation solutions in several key areas.

*Data Overload*

Because third-wave AI-enabled security monitoring detects and surfaces threats in real time, before they can compromise your network, there's no need to accumulate and store massive amounts of data. Best-in-class AI can identify patterns and develop a humanlike understanding of what normal traffic looks like, even within constantly changing conditions.

*Approach to Expected Baseline Network Activity*

Free from human tuning, self-supervised (third-wave) AI learns over time how to identify and fix issues that traditional solutions can't solve. When there is a deviation from expected baseline behavior, predictive AI quickly finds it and alerts security.

Rules-based SIEM platforms operate on a similar principle – detecting anomalous behavior by comparing activity to expected behavior. In the real world, any SOC will likely attest that "expected" behavior can change on a dime.

For example, when the world's workforce abruptly shifted to work-from-home models en masse, any notion of "expected" or "normal" went right out the window. Millions of new, remote connections, all at once, were certainly unexpected by most security platforms, but these connections weren't really abnormal. Associated behaviors were not actually anomalous. Still, security analysts working for organizations relying on SIEM faced a growing mountain of false positives they had to sort through. In the meantime, cyber criminals who had been waiting for a moment like this for years swooped right in. Not only did bad actors seek out network vulnerabilities opened up by these SIEM and similar issues, but they wasted no time unleashing phishing schemes while they knew security teams would be busy addressing immediate network issues. On the flip side, organizations that had invested in third-wave AI solutions experienced far fewer issues. These systems create an ***evolving*** baseline of normal network behavior. As a "new normal" took hold for these organizations, their third-wave AI solutions were able to adjust on the fly.

*Zero Day Attack Capabilities*

Zero-day attacks like the Solarwinds attack on U.S. federal agencies, which made headlines at the end of 2020, can be devastating to an organization. Within minutes, an entire network

can become compromised, after hackers have been inside the network for months or years, completely undetected.
Third-wave AI helps to stave off zero day attacks the instant bad actors make their move. Real-time threat detection means just that. In a rules-based system, there's a much higher risk of losing precious response time. By the time a security analyst figures out what's happening, the damage may well be done.

**Looking Ahead: Predictive AI in 2021… and Beyond**

To keep ahead of the current crop (and tomorrow's crop) of tech-savvy cybercriminals, organizations will need to invest in cybersecurity solutions that are streamlined, powerful and powered by predictive AI.
For too long, modern SOCs have dumped millions of dollars into solutions that are failing at increasing rates. Enterprises and organizations of every size are losing revenue, constantly dealing with the financial and operational impacts of data loss while failing to address the fundamental issues with their security solutions, all the same.
Unsupervised, predictive AI is the best path forward for modern SOCs. These systems offer a centralized solution that addresses the functional requirements of anomaly detection platforms, SIEM and UBA with the added benefits of predictive, self-learning AI. Third-wave AI delivers true, real-time protection for networks assets on-prem, in the cloud, and across connected devices.

***Dr. Igor Mezić** is Chief Technology Officer and Chief Scientist at MixMode AI. Mezic works on operator-theoretic methods in nonlinear dynamical systems and control theory and their applications in fluid dynamics, energy efficient design and operations and complex systems dynamics. He did his Dipl. Ing. in Mechanical Engineering in 1990 at the University of Rijeka, Croatia and his Ph. D. in Applied Mechanics at the California Institute of Technology. Dr. Mezic was a postdoctoral researcher at the Mathematics Institute, University of Warwick, UK in 1994-95. From 1995 to 1999 he was a member of Mechanical Engineering Department at the University of California, Santa Barbara where he is currently a Professor. In 2000-2001 he worked as an Associate Professor at Harvard University in the Division of Engineering and Applied Sciences. He won the Alfred P. Sloan Fellowship, NSF CAREER Award from NSF and the George S. Axelby Outstanding Paper Award on "Control of Mixing" from IEEE. He also won the United Technologies Senior Vice President award for Science and Technology Special Achievement Prize in 2007. He was an Editor of Physica D: Nonlinear Phenomena and an Associate Editor of the Journal of Applied Mechanics and SIAM Journal on Control and Optimization. Dr. Mezic is a Fellow of the American Physical Society (APS), Fellow of Society of Industrial and Applied Mathematics (SIAM), the Director of the Center for Energy Efficient Design and Head of Buildings and Design Solutions Group at the Institute for Energy Efficiency at the University of California, Santa Barbara.*

## 2020 Cibercrime Losses Exceeded $4.2 Billion: FBI

Source: http://www.homelandsecuritynewswire.com/dr20210318-2020-cibercrime-losses-exceeded-4-2-billion-fbi

Mar 18 – The FBI's Internet Crime Complaint Center has released its annual report. The *2020 Internet Crime Report* includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. State-specific statistics have also been released and can be found within the *2020 Internet Crime Report* and in the accompanying *2020 State Reports*.
**The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion.** Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.
In addition to statistics, the IC3's *2020 Internet Crime Report* contains information about the most prevalent internet scams affecting the public and offers guidance for prevention and protection. It also highlights the FBI's work combating internet crime, including recent case examples. Finally, the *2020 Internet Crime Report* explains the IC3, its mission, and functions.
The IC3 gives the public a reliable and convenient mechanism to report suspected internet crime to the FBI. The FBI analyzes and shares information from submitted complaints for investigative and intelligence purposes, for law enforcement, and for public awareness.
With the release of the *2020 Internet Crime Report*, the FBI wants to remind the public to immediately report suspected criminal internet activity to the IC3 at ic3.gov. By reporting internet crime, victims are not only alerting law enforcement to the activity, but aiding in the overall fight against cybercrime.

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

# DRONE NEWS

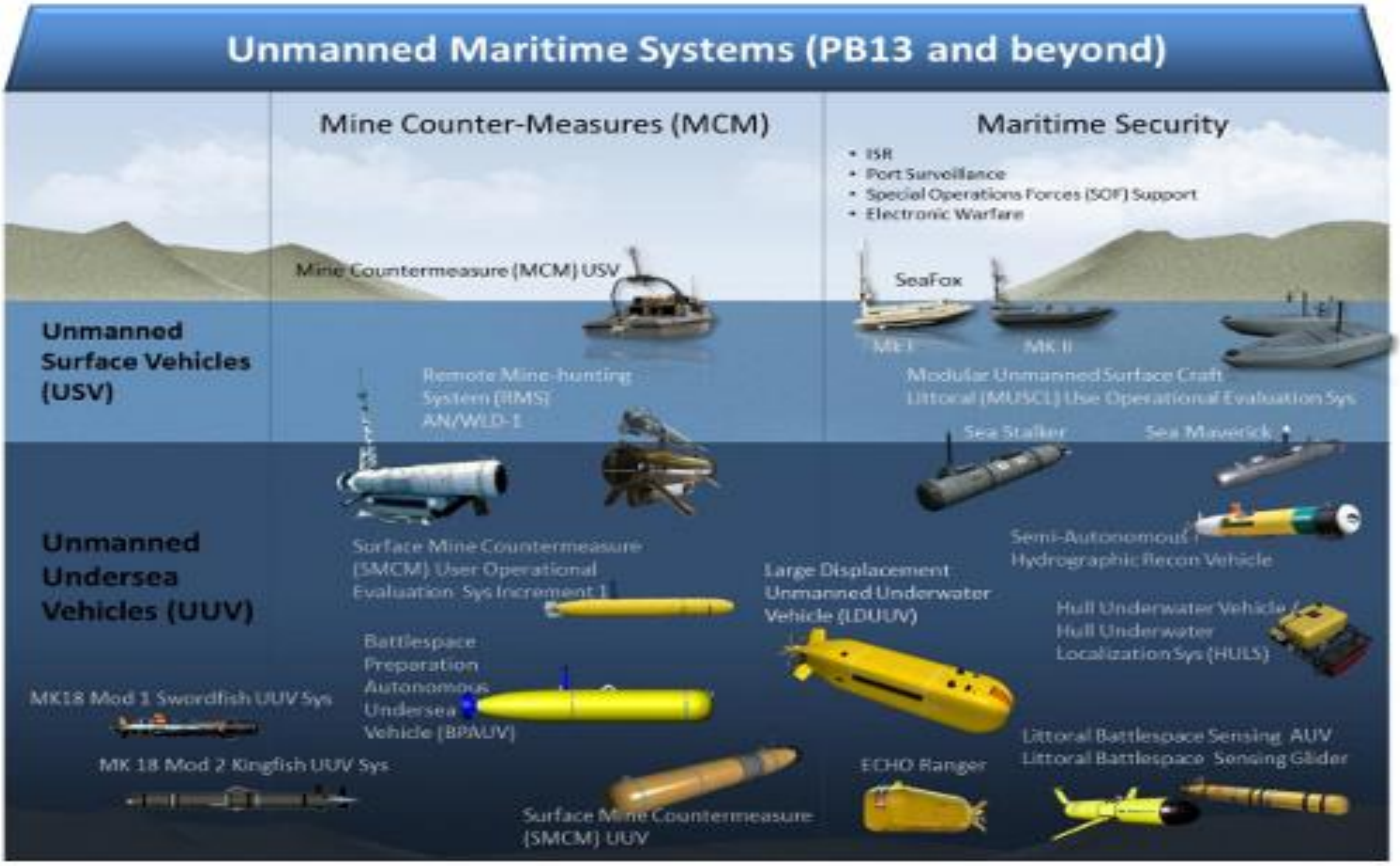
## Inexpensive Drones: Using Technological Innovation to Eradicate Landmines

60 states and other areas, e.g., North Atlantic and the Baltic Sea (where naval mines from World War II can still be found from time to time), are still contaminated by antipersonnel mines. The dilemma: progress in demining is highly dependent on technical developments in the field as well as new policy-challenges. In parallel, removing landmines is difficult and massively time-consuming. What would be the best solution? - countering the problem remotely on the ground and from the air with robotics! Read this article...

## Turkey-Hamas unleash hell in the Mediterranean: An Israeli warship was attacked on turkish orders

Source: https://www.pentapostagma.gr/kosmos/mesi-anatoli/6992287_turkey-hamas-unleash-hell-mediterranean-israeli-warship-was-attacked

Feb 24 – New kind of war in the Mediterranean - A submarine unmanned vehicle of Hamas attacked an Israeli warship
We have a new unexpected development since according to foreign sources, the Israeli navy was attacked by an unmanned submarine on the shores of the Gaza Strip. The attack was neutralized in time by its weapon systems.


Unmanned Maritime Systems (PB13 and beyond)
Mine Counter-Measures (MCM)
Maritime Security
• ISR
• Port Surveillance
• Special Operations Forces (SOF) Support
• Electronic Warfare
Unmanned Surface Vehicles (USV)
Unmanned Undersea Vehicles (UUV)
Mine Countermeasure (MCM) USV
SeaFox
MK I
MK II
Modular Unmanned Surface Craft Littoral (MUSCL) Use Operational Evaluation Sys
Remote Mine-hunting System (RMS) AN/WLD-1
Sea Stalker
Sea Maverick
Semi-Autonomous Hydrographic Recon Vehicle
Surface Mine Countermeasure (SMCM) User Operational Evaluation Sys Increment 1
Large Displacement Unmanned Underwater Vehicle (LDUUV)
Hull Underwater Vehicle / Hull Underwater Localization Sys (HULS)
Battlespace Preparation Autonomous Undersea Vehicle (BPAUV)
MK18 Mod 1 Swordfish UUV Sys
MK 18 Mod 2 Kingfish UUV Sys
ECHO Ranger
Littoral Battlespace Sensing AUV
Littoral Battlespace Sensing Glider
Surface Mine Countermeasure (SMCM) UUV

As the ship approached the port, it exploded and its neutralization caused relatively little material damage to the Israeli warship.
Russian sources, judging by the explosion that took place, emphasize that there were enough explosives in the unknown submarine remote-controlled yacht that was moving at high speed to hit (unsuccessfully) the Israeli warship, with the aim of causing great damage.
Who exactly is behind the attack on the Israeli warship remains unknown at this time. However, all indications are that Palestinian radical groups (Hamas) have already declared their readiness to attack Israeli targets at sea.

Israel, for its part, has not yet revealed all the details of the incident, noting only that the threat was eliminated immediately. To date, no group has claimed responsibility for the attack on the Israeli warship.

However, the Islamist terrorist organization Hamas owns remote-controlled submarines. Unmanned submarines could be used to attack any number of Israeli targets at sea, including gas drilling rigs, merchant ships and warships, as in this case.

The Israeli military said Hamas' naval arsenal contained "advanced naval weapons capable of infiltrating and carrying out terrorist attacks."

The same sources estimate that Hamas has expanded its naval capabilities, both in terms of advanced technology and in terms of training frogmen, so that they can penetrate Israeli territory from the sea to attack Israeli ships.

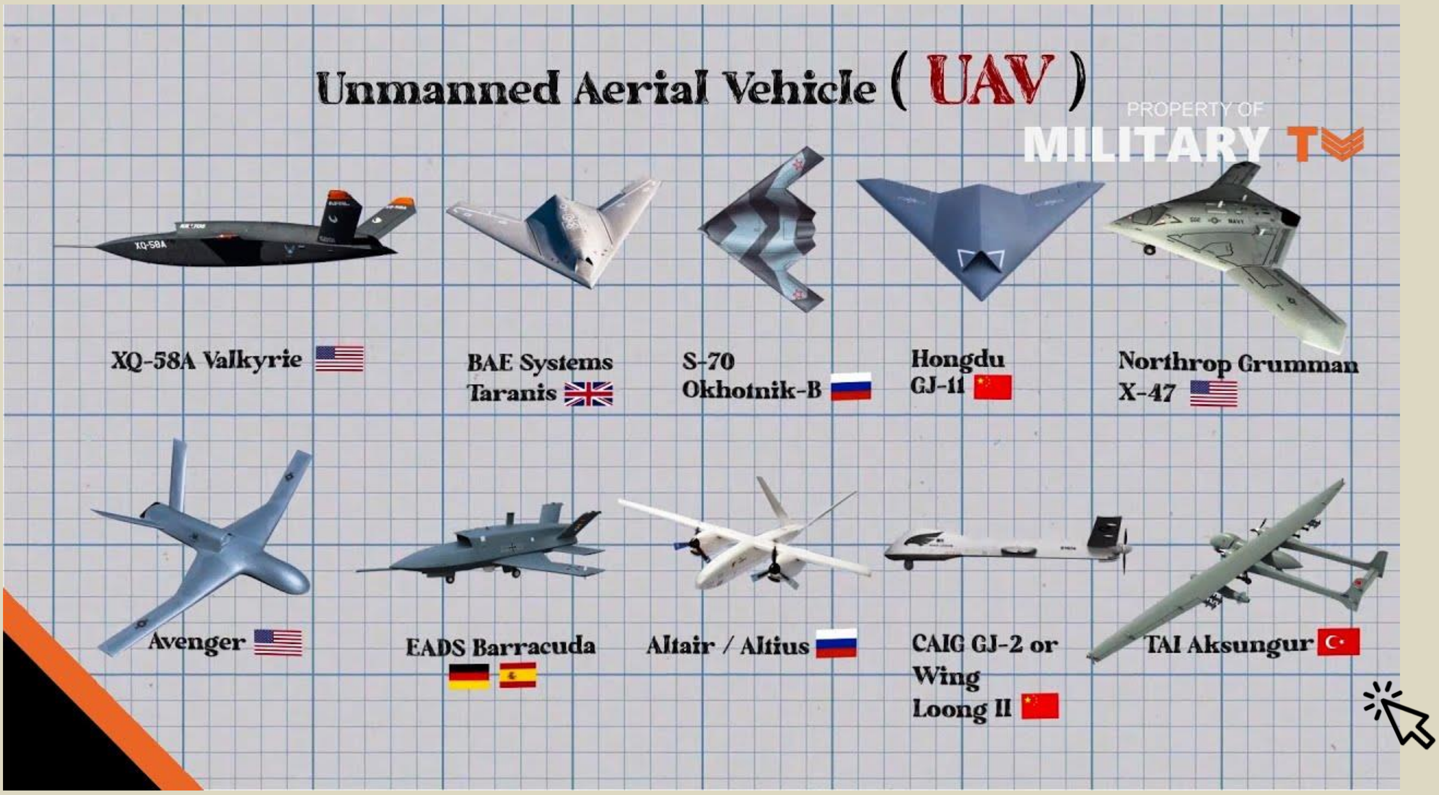
Behind everything, however, are probably two countries, one is Turkey and the other is Iran, according to the same sources.

The Americans estimate that over the next decade, submarine drones will become the worst nightmare of surface units and submarines. Mohammed al-Zoari, a Tunisian expert in unmanned vehicles, was said to be constructing small, remote-controlled submarine drones for the terrorist group when he was killed by gunmen in December 2016. (The Mossad was blamed for the killing; Israel would not comment on the allegation.)

Aerial unmanned vehicles will be called upon to locate and neutralize manned and non-submarine vehicles. In fact, they are expected to develop the well-known detection methods which are active and passive sonar. They will locate torpedoes and turn themselves into torpedoes to destroy enemy warships.

The Mediterranean countries in combination with the major energy projects in the region will be called first of all, as everything shows, to respond very soon to this huge, insidious danger under water.

## Top 10 combat drones in the world 2021



## nEUROn

Source: https://www.dassault-aviation.com/en/defense/neuron/introduction/

For the coming twenty years, the European combat aircraft industry will face three main challenges:

- the need to develop strategic technologies,
- the necessity to uphold skills of excellences in areas in which the European industry has gained technical competences and fields of excellence,

- the goal to provide workload to the European design offices.

Facing such a situation, the French government took the initiative by launching in 2003 a project for a technological demonstrator of an Unmanned Combat Air Vehicle (UCAV), elaborated in the frame of a European cooperation scheme.

The aim of the nEUROn demonstrator is to provide the European design offices with a project allowing them to develop know-how and to maintain their technological capabilities in the coming years.

This project has gone far beyond the theoretical studies that had been conducted until now, as it plans the building and the flight demonstration of an unmanned aircraft.

nEUROn and Rafale M in flight over the Charles de Gaulle aircraft carrier.

It is also a way to implement an innovative process in terms of management and organisation of a European cooperative programme. To be fully effective, a single point of decision, the French Defence Procurement Agency (DGA – Délégation Générale pour l'Armement), and a single point of implementation, Dassault Aviation company as prime contractor, were settled to manage the nEUROn programme.

The Italian, Swedish, Spanish, Greek and Swiss governments acting together with their related industrial teams, Alenia, SAAB, EADS-CASA, Hellenic Aerospace Industry (HAI) and RUAG, have joined the French initiative.

### An effective European cooperation scheme

In accordance with the guidelines defined by the French DGA, Dassault Aviation has entrusted about 50% of the work value to European partners, elected after a scrutinized evaluation based on:

- **Experience and excellence:** the objective of this project was not to create new technological capabilities everywhere in Europe, but to take the full benefit of the already existing technological niches.
- **Competitiveness:** this project had the ambition to find new ways for costs reduction. Each partner, in addition to their technical excellences, was invited to apply for the most efficient "value for money".
- **State budget allocation:** it was a condition imposed by the French DGA that each country having the ambition to participate to the nEUROn programme shall

contribute to its financing. For more flexibility, no constraint in term of "geographical return" was assigned to this project, as already dealt with at governmental level.

**Related industrial team**

The industrial team of the nEUROn programme is composed of 6 companies.

**Dassault Aviation (France)**

in addition to being the design authority, has taken care of the general design and architecture of the system, the flight control system, the implementation of low observable devices, the final assembly, the systems integration on the "global integration tests rig", the ground tests, and the flight tests,

**Alenia Aermacchi (now Leonardo, Italy)**

has contributed to the project with a new concept of internal weapon bay ("Smart Integrated Weapon Bay" – SIWB), an internal EO/IR sensor, the bay doors and their operating mechanisms, the electrical power and distribution system, and the air data system,

**SAAB (Sweden)**

was entrusted with the general design of the main fuselage, the landing gear doors, the avionics and the fuel system,

**EADS-CASA (now Airbus Defence & Space, Spain)**

brought its experience for the wings, the ground station, and the data link integration,

**Hellenic Aerospace Industry – HAI (Greece)**

was responsible for the rear fuselage, the exhaust pipe, and the supply of racks of the "global integration tests rig",

**RUAG (Switzerland)**

was taking care of the low-speed wind tunnel tests, and the weapon interfaces between the aircraft and the armaments.

## Drones deliver COVID-19 vaccines to remote African regions

Source [+video]: https://newatlas.com/drones/coronavirus-vaccine-drone-delivery-zipline-ghana-covax/

When the drone reaches its destination, its payload is released over a predetermined area and is (paper) parachuted down to the ground

Mar 08 – Early in March the world's first COVID-19 vaccine drone deliveries began in the African nation of Ghana. The drone dropped 250 vaccine doses by parachute to a rural health center, one of 36 deliveries completed on the first day.

US medical drone delivery company Zipline has been working for several years in various African countries, building drone delivery infrastructure to help transport vital medical supplies to remote regions. Blood deliveries by drone kicked off in 2016 in Rwanda, and rapidly spread to countries including Tanzania.

The company's custom-designed drone technology offers a round-trip range of 160 km (99 miles) with up to 1.75 kg (3.8 lb) of cargo. The fixed-wing drones can reach a top speed of 128 km/h (80 mph) and a have a cruising speed of 101 km/h (63 mph).

The latest Zipline drone deliveries encompass the first COVID-19 vaccines to be distributed in Africa as part of the global COVAX agreement, an international initiative working to aid equitable access to vaccines. After months of planning things swiftly kicked into gear when 600,000 doses of the Oxford/AstraZeneca vaccine landed in Ghana's capital.

On the 2nd of March the first drone was launched from Mpanya, in the southern-central Ghana region of Ashanti. After 34 minutes of flying the drone arrived in Asuofua, around 70 km (43 miles) away. A small insulted box containing 25 vials of vaccine parachuted down and within five hours 250 people had been vaccinated. By the end of the day another 35 drone deliveries to the Asuofua Health Center had been completed.

With the support of several stakeholders, including the UPS Foundation, the Ghana government and Gavi - the Vaccine Alliance, several Zipline hubs have been established across the country. It's estimated around 1,000 health centers in the country are now served by the drone delivery service.

Caitlin Burton, from Zipline, suggests this distribution system allows for precise and fast deliveries of vaccines to remote areas. “Being able to use every point of care in the health system to get people vaccinated – that’s the strategy here,” says Burton. “We’ll be sending exactly the number of doses needed – the chain of custody is very short, and the cold chain is one hundred percent guaranteed.”

## Drones in Dubai drop seeds from sky in tree planting drive

**Video:** https://www.thenationalnews.com/uae/environment/watch-drones-in-dubai-drop-seeds-from-sky-in-tree-planting-drive-1.1185495

One of the drones being used by Cafu to plant one million ghaf tree seeds across the UAE over the next two years. Pawan Singh / The National

Mar 17 – A Dubai company has launched an ambitious project to use drone technology to plant one million ghaf tree seeds across the UAE in an effort to combat climate change.

Fuel-delivery company Cafu is behind the project that will send out drones to plant the ghaf tree seeds by firing them into the ground at a speed of 288 kilometres per hour.

A senior figure from the company said the two-year strategy would involve swarms of drones launching the seeds into the ground from a height of 10 metres.

We want to show that planting seeds by drone technology is a much more efficient method than using hundreds of people

The company has already completed the first two rounds of the programme with drone seeding taking place in the Mleiha Desert, Sharjah.

“The key benefit we hope to create is to discover a new way to plant trees in a cost-effective way,” said Cafu general manager Antonio Al Asmar.

“We want to show that planting seeds by drone technology is a much more efficient method than using hundreds of people to do the same task.”

The drones fire a custom-made “seedball” into the surface of the desert, using pneumatic power to ensure they are embedded at least 1 centimetre in the ground.

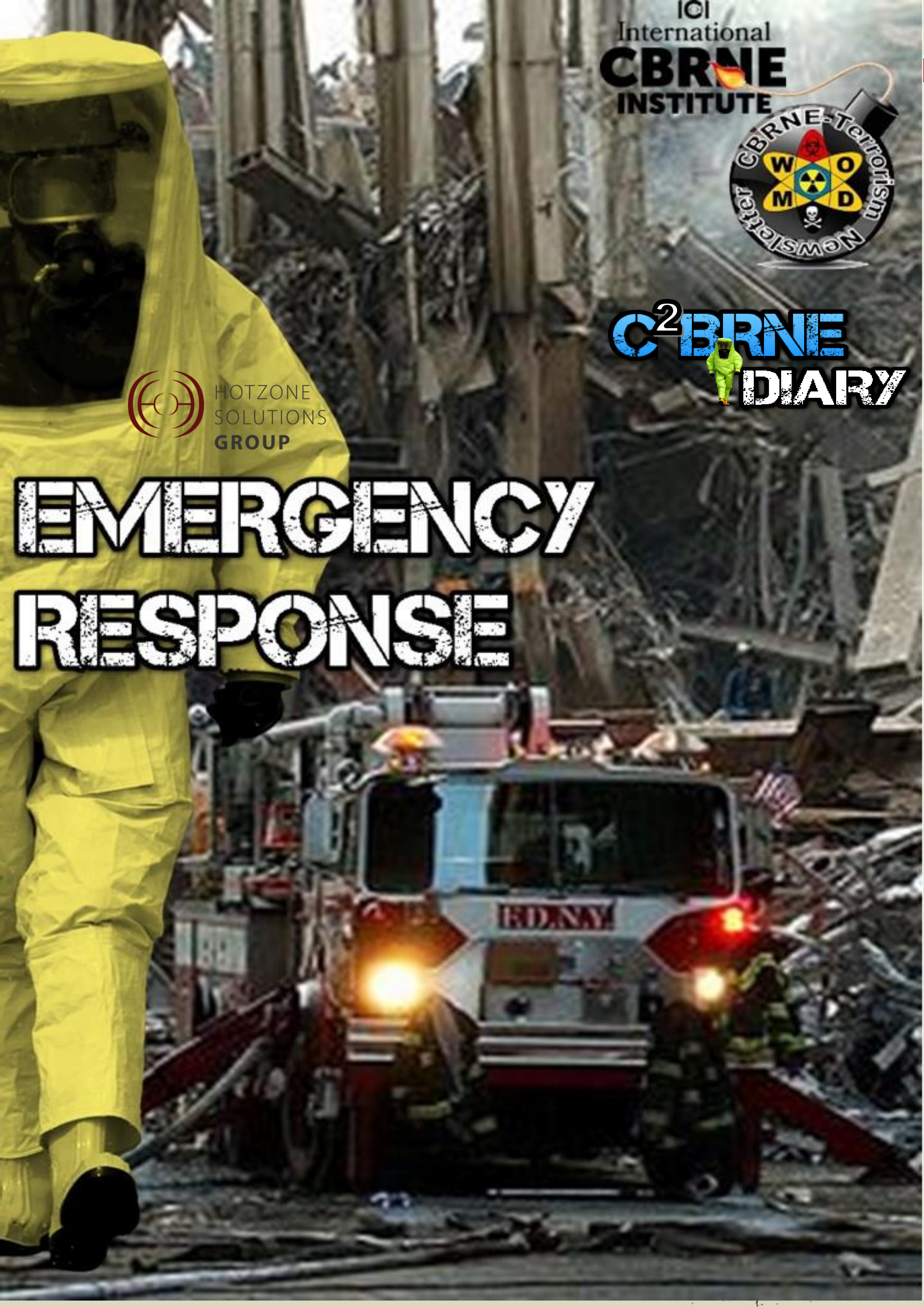
Mr Al Asmar said he hoped the project could be adopted by other countries over time, if successful.
He was unable to give an exact cost of the project but estimated it would run to "hundreds of thousands of dirhams" at the very least.
"If we can make it work here in the desert environment, there is no limit to where we can make it work," said Mr Al Asmar.
"For now, though, we want to prove it works here and then take it to other areas. I see a lot of potential for it. There is a lot of time-consuming manual labour involved in the agricultural industry that could be made much more efficient."

**A commitment to combating climate change**

The native ghaf tree. Randi Sokoloff / The National

Mr Al Asmar said it was right that, as a fossil fuel company, it works to negate the impact of its industry on the environment.
"We are absolutely committed to tackling climate change and this is our way of contributing," he said.
"People might see the Cafu project as being cynical when we are delivering fuel in a truck but what we offer actually helps the environment.
"Our model is more efficient than cars going to the gas station: one vehicle filling 200 cars is better than 200 cars going and filling at the gas station."
The company's founder and chief executive said the drone project was in keeping with its ethos to promote sustainable practices.
"Our motivation, since the time we launched in 2018, has been to set convenience in motion to make life better for our customers and residents, not just through our services, but through our ethos and values," said Rashid Al Ghurair, founder of Cafu.
"The Ghaf Tree Project, which forms the central pillar of our sustainability deal, is very close to my heart and I am happy to see the impact we are making on the UAE through this project."

**EDITOR'S COMMENT:** Clever and interesting! But keep in mind the dual use of innovations like this.



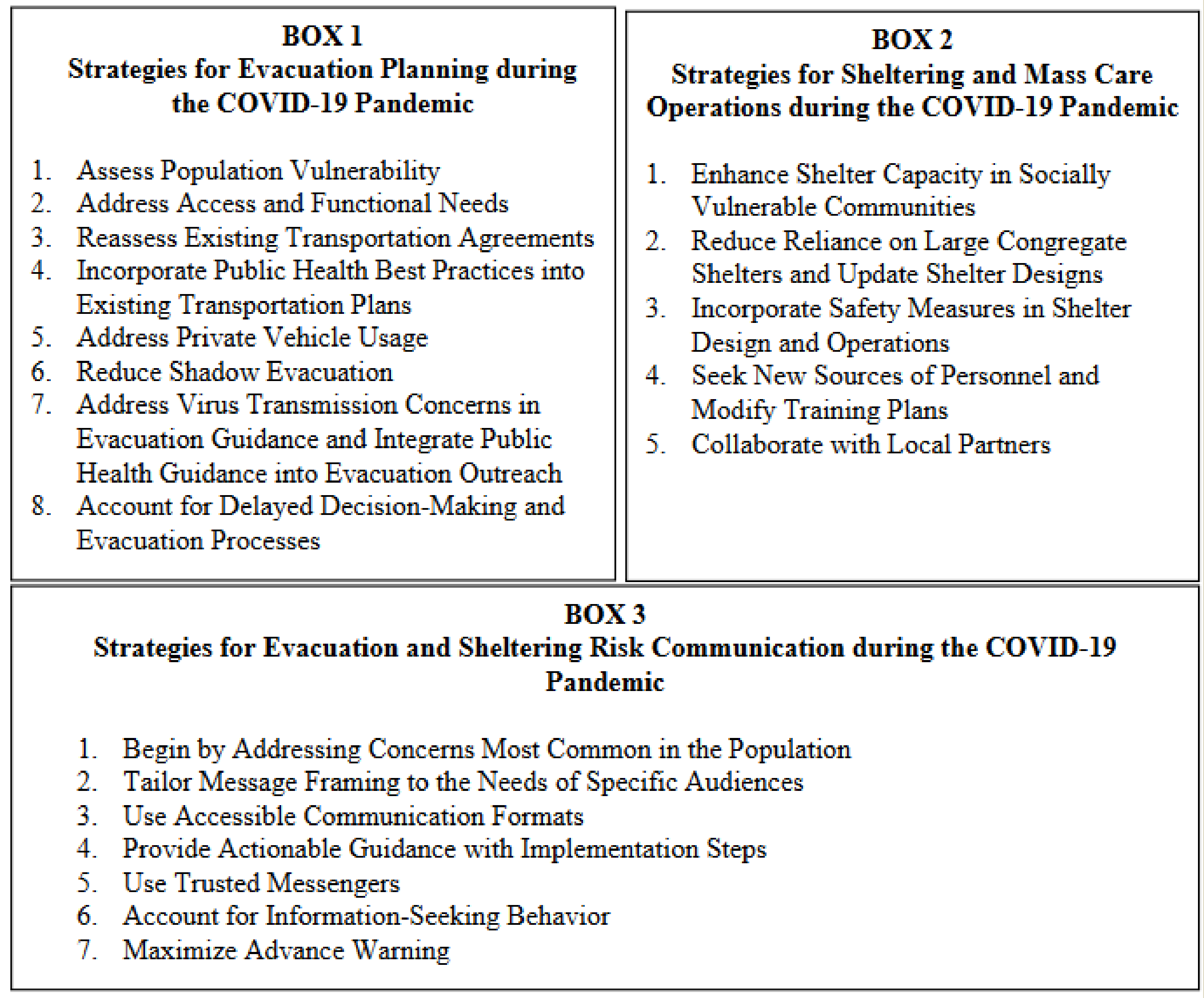
# EMERGENCY RESPONSE

## Emergency Evacuation and Sheltering During the COVID-19 Pandemic

Source: https://www.nap.edu/read/26084/chapter/1

Feb 2021 – Fundamental shifts in preparedness planning are needed to ensure health, safety, and smooth operations during emergencies in the context of the COVID-19 pandemic. To prepare for emergency events requiring evacuation, it is necessary to revise shelter planning and mass care operations, shelter staffing, and shelter design and operations with a focus on reducing virus transmission and ensuring safety. Developing effective public messaging is also critical during the pandemic and requires advance planning and familiarity with the needs and characteristics of the communities being served.

This rapid expert consultation details what is known from research on evacuation behavior, social responses to disaster, and risk communication, as well as lessons learned from emergency managers, public health departments, local officials, and human service providers, as the second year of the pandemic unfolds. It includes strategies for (1) evacuation plans, (2) sheltering operations, and (3) risk communication best practices for public officials confronting hazards and disasters.



**BOX 1**

**Strategies for Evacuation Planning during the COVID-19 Pandemic**

1. Assess Population Vulnerability
2. Address Access and Functional Needs
3. Reassess Existing Transportation Agreements
4. Incorporate Public Health Best Practices into Existing Transportation Plans
5. Address Private Vehicle Usage
6. Reduce Shadow Evacuation
7. Address Virus Transmission Concerns in Evacuation Guidance and Integrate Public Health Guidance into Evacuation Outreach
8. Account for Delayed Decision-Making and Evacuation Processes

**BOX 2**

**Strategies for Sheltering and Mass Care Operations during the COVID-19 Pandemic**

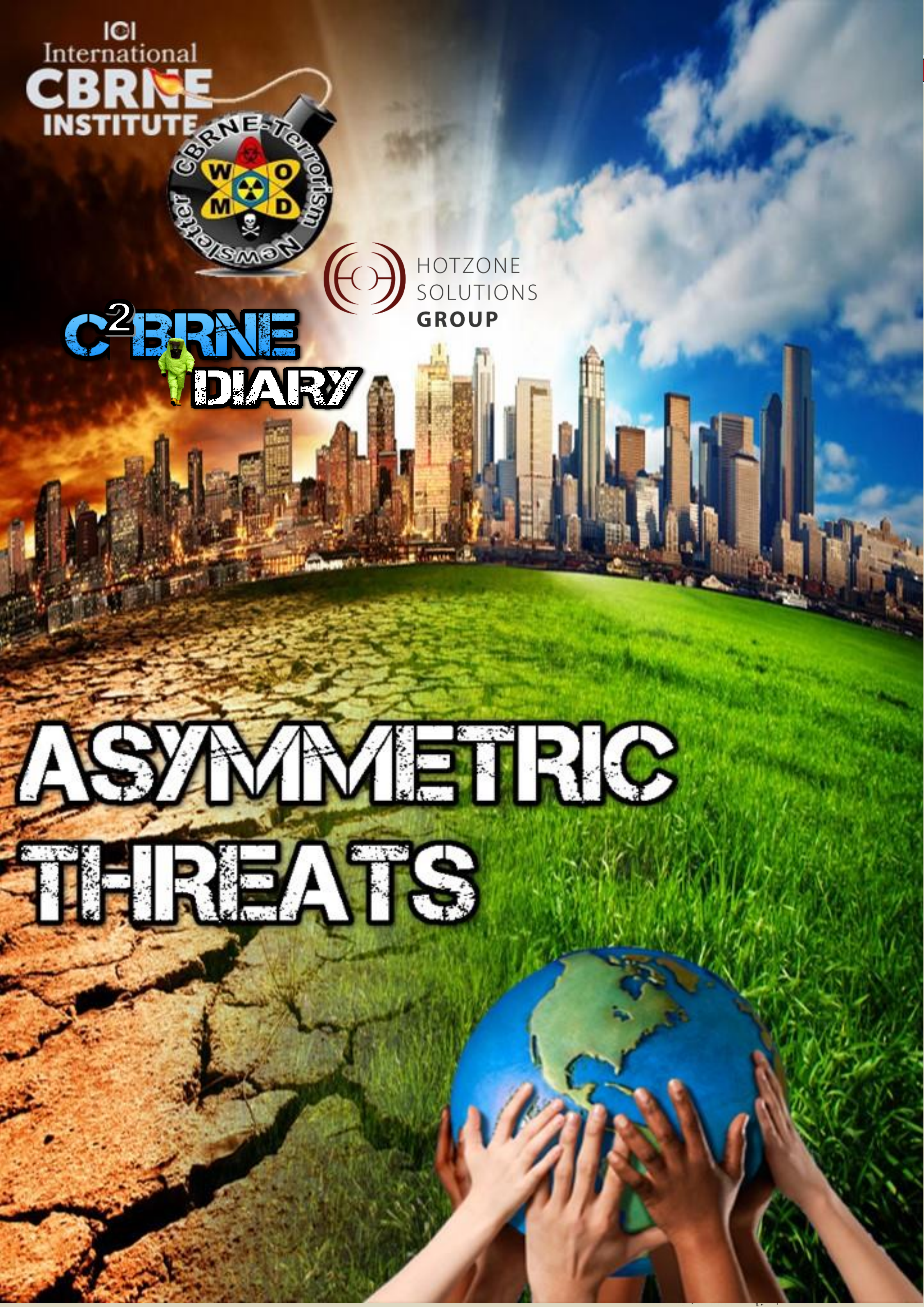
1. Enhance Shelter Capacity in Socially Vulnerable Communities
2. Reduce Reliance on Large Congregate Shelters and Update Shelter Designs
3. Incorporate Safety Measures in Shelter Design and Operations
4. Seek New Sources of Personnel and Modify Training Plans
5. Collaborate with Local Partners

**BOX 3**

**Strategies for Evacuation and Sheltering Risk Communication during the COVID-19 Pandemic**

1. Begin by Addressing Concerns Most Common in the Population
2. Tailor Message Framing to the Needs of Specific Audiences
3. Use Accessible Communication Formats
4. Provide Actionable Guidance with Implementation Steps
5. Use Trusted Messengers
6. Account for Information-Seeking Behavior
7. Maximize Advance Warning

The Societal Experts Action Network (SEAN) is an activity of the National Academies of Sciences, Engineering, and Medicine that is sponsored by the National Science Foundation. SEAN links researchers in the social, behavioral, and economic sciences with decision makers to respond to policy questions arising from the COVID-19 pandemic. This project is affiliated with the National Academies' Standing Committee on Emerging Infectious Diseases and 21st Century Health Threats.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

# ASYMMETRIC THREATS

# Unravelling the When, Where and How of Volcanic Eruptions

**By Sandrine Ceurstemont**
Source: http://www.homelandsecuritynewswire.com/dr20210304-unravelling-the-when-where-and-how-of-volcanic-eruptions

Mar 04 – There are about 1,500 potentially active volcanoes worldwide and about 50 eruptions occur each year. But it's still difficult to predict when and how these eruptions will happen or how they'll unfold. Now, new insight into the physical processes inside volcanoes are giving scientists a better understanding of their behavior, which could help protect the 1 billion people who live close to volcanoes.

Dome-building volcanoes, which are frequently active, are among the most dangerous types of volcanoes since they are known for their explosive activity. This type of volcano often erupts by first quietly producing a dome-shaped extrusion of thick lava at its summit which is too viscous to flow. When it eventually becomes destabilized, it breaks off and produces fast-moving currents of hot gas, solidified lava pieces and volcanic ash, called pyroclastic clouds, that flow down the sides of the volcano at the speed of a fast train.

"The hazards associated with them can be very spontaneous and hard to predict," said Professor Thomas Walter, a professor of volcanology and geohazards at the University of Potsdam in Germany. "That's why it's so important to understand this phenomenon of lava domes."

Little is known about the behavior of lava domes, partly because there isn't much data available. Prof. Walter and his colleagues want to better understand how they form, whether they can vary significantly in shape and what their internal structure is like. Over the last five years, through a project called VOLCAPSE, they have been using innovative techniques to monitor lava domes by using high resolution radar data captured by satellites as well as close-up views from cameras set up near volcanoes.

"Pixel by pixel, we could determine how the shape, morphology and structure of these lava domes changed," said Prof. Walter. "We compared (the webcam images) to satellite radar observations."

### Time-lapse

The project focused on a few dome-building volcanoes such as Colima in Mexico, Mount Merapi in Indonesia, Bezymianny in Russia, and Mount Lascar and Lastarria in Chile. It partly involved visiting them and installing instruments such as time-lapse cameras powered by solar panels that could be controlled remotely. If a lava dome started to form, for example, the team could tweak the settings so that it captured higher resolution images more often.

Due to high altitudes and harsh weather conditions, setting up the cameras was more challenging than expected. "It was a sharp learning curve, but also trial and error, because nobody could tell us what to expect at these volcanoes since it was never done before," said Prof. Walter.

During their visits, the team also used drones. These would fly over a lava dome and capture high resolution images from different perspectives, which could be used to create detailed 3D models. Temperature and gas sensors on the drones provided additional information.

Prof. Walter and his colleagues used the data to create computer simulations, such as how the growth of lava domes changes from eruption to eruption. They found that new lava domes don't always form in the same location: a lava dome may form at the summit of a volcano during one eruption while the next time it builds up on one of its flanks. The team was puzzled, since a conduit inside a volcano brings magma to the surface during an eruption, which would mean that it changes its orientation between one eruption and the next. "That was very surprising for us," said Prof. Walter.

### Stress field

They were able to explain how this happens by examining the distribution of internal forces – or stress field - in a volcano. When magma is expelled during an eruption, it changes how the forces are distributed inside and causes a reorientation of the conduit.

The team also found that there was a systematic pattern to how the stress field changed, meaning that by studying the position of lava domes they could estimate where they had formed in the past and where they would appear in the future. This could help determine which areas near a volcano are likely to be most affected by eruptions yet to come.

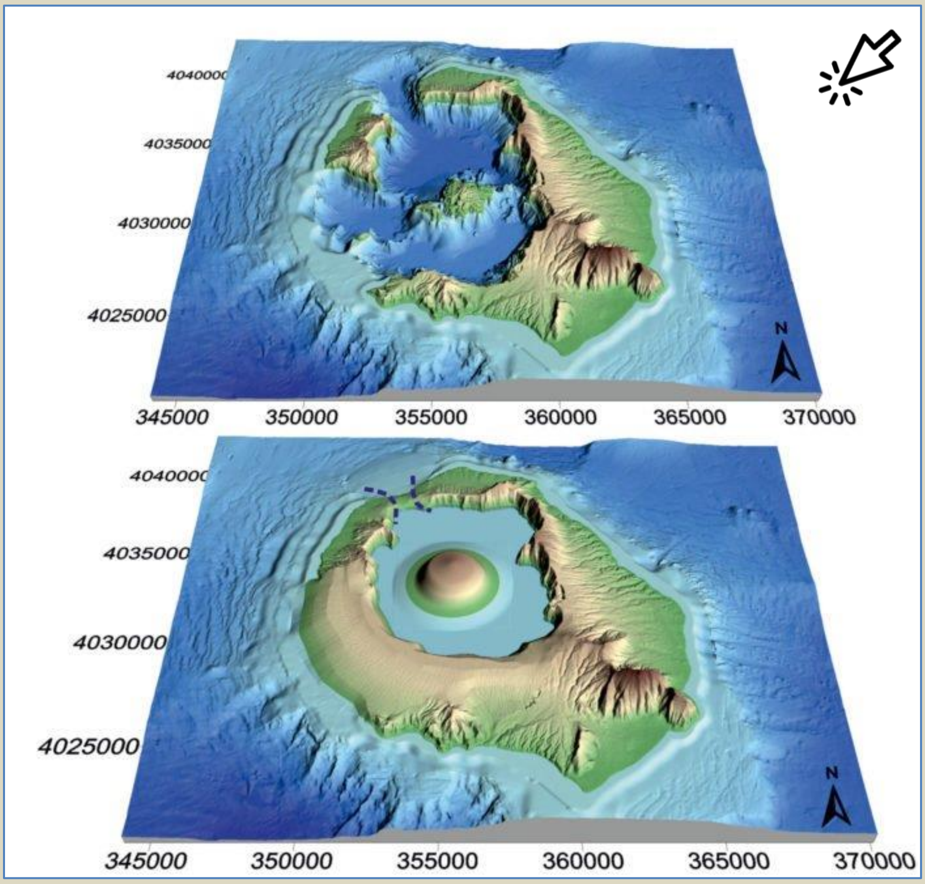
"This is a very cool result for predictive research if you want to understand where the lava dome is going to extrude (or collapse) from in the future," he said.

Knowing where a volcano will erupt from is one thing, but knowing when it will do so is a different matter and the physical factors that govern this are also not well understood. Although there is a relationship between how often eruptions occur and their size, with big eruptions occurring very rarely compared to smaller ones, a lack of reliable data makes it hard to examine the processes that control eruption frequency and magnitude.

"When you go back in the geological record, (the traces of) many eruptions disappear because of erosion," said Professor Luca Caricchi, a professor of petrology and volcanology at the University of Geneva in Switzerland.

Furthermore, it's not possible to access these processes directly since they occur deep down beneath a volcano, at depths of 5 to 60 kilometers. Measuring the chemistry and textures of magma expelled during an eruption can provide some clues about the internal processes that led to the event. And magma chambers can sometimes be investigated when they pop up at the surface of the Earth due to tectonic processes. Extracting information from specific time periods is still difficult though since the "picture" you get is like a movie where all the frames are collapsed into a single shot. "It's complicated to retrieve the evolution in time – what really happened during the movie," said Prof. Caricchi.

Prof. Caricchi and his colleagues are using a novel approach to forecast the recurrence rate of eruptions. Previous predictions were typically based on statistical analyses of the geological records of a volcano. But through a project called FEVER the team is aiming to combine this method with physical modelling of the processes responsible for the frequency and size of eruptions. A similar approach has been used to estimate when earthquakes and floods will occur again.



Santorini Island Volcano – Greece: Above: The island after the volcanic eruption of 1613 BC. Below: The island as it was before the eruption. – Karatson et al., 2018

Using physical models should especially be useful to make predictions for volcanoes where there is little data available. "To extrapolate our findings from a place where we know a lot, like in Japan, you need a physical model that tells you why the frequency-magnitude relationship changes," said Prof. Caricchi.

Santorini Island

To create their model, the team have incorporated variables that affect pressure in the magma reservoir or the rate of accumulation of magma at depth below the volcano. The viscosity of the crust under the volcano and the size of the magma reservoir, for example, play a role. They have performed over a million simulations using all the possible combinations of values that can occur. The relationship between frequency and magnitude they obtained from their model was similar to what was estimated by using volcanic records so they think they were able to capture the fundamental processes involved.

"It's sort of a fight between the amount of magma and the properties of the crust," said Prof. Caricchi. "They are the two big players that fight each other to finally lead to this relationship."

**Tectonic plates**

However, the team also found that the relationship between the size and frequency of changes across volcanoes in different regions. Prof. Caricchi thinks this is due to differences in the geometry of tectonic plates in each area. "We can see that the rate at which a plate subducts below another, and also the angle of subduction, seem to play an important role in defining the frequency and magnitude of a resulting eruption," he said. The team is now starting to incorporate this new information into their model.

Being able to predict the frequency and magnitude of future eruptions using a model could help better assess hazards. In Japan, for example, one of the countries with the most active volcanoes, knowing the probability of future eruptions of various sizes is important when deciding where to build infrastructure such as nuclear power plants.

It's also invaluable in densely populated areas, such as in Mexico City, which is surrounded by active volcanoes, including Nevado de Toluca. Prof. Caricchi and his colleagues studied this volcano, which hasn't erupted for about 3,000 years. They found that once magmatic activity restarts, it would take about 10 years before a large eruption could potentially occur. This knowledge would prevent Mexico City from being evacuated if initial signs of activity are spotted.

"Once the activity restarts, you know you have ten years to follow the evolution of the situation," said Prof. Caricchi. "(People) will now know a little bit more about what to expect."

***Sandrine Ceurstemont** is a freelance science writer based in London.*

## Does the US Military "Own the Weather"? "Weaponizing the Weather" as an Instrument of Modern Warfare?

**By Prof Michel Chossudovsky**

Source: https://www.globalresearch.ca/does-the-us-military-own-the-weather-weaponizing-the-weather-as-an-instrument-of-modern-warfare/5608728

*"Weather modification will become a part of domestic and international security and could be done unilaterally… It could have offensive and defensive applications and even be used for deterrence purposes. The ability to generate precipitation, fog and storms on earth or to modify space weather… and the production of artificial weather all are a part of an integrated set of [military] technologies." (Study Commissioned by the US Air Force: Weather as a Force Multiplier, Owning the Weather in 2025, August 1996)*

*Environmental modification techniques have been available to the US military for more than half a century.*

*The issue has been amply documented and should be part of the climate change debate.*

The U.N. Climate Conference (COP 25) met in Madrid with Delegates from nearly 200 countries. The focus was on Greenhouse gas emissions. Under the 1992 United Nations Framework Convention on Climate Change, "every country on earth is treaty-bound to "avoid dangerous climate change", and find ways to reduce greenhouse gas emissions globally in an equitable way.": A narrow consensus which focusses on the nefarious impacts of CO2 emissions (from fossil fuel) on World temperature.

What has casually been omitted from the COP debate is the manipulation of climate for military use.

The broader issue of **environmental modification techniques** (ENMOD) must be addressed and carefully analyzed. It should also be understood that the instruments of weather warfare are part of the US arsenal of weapons of mass destruction (WMD) and their proposed use by the US military against "enemies" constitutes not only a crime against humanity but to put it mildly **a threat to planet earth.**

In this essay I am providing the reader with direct quotes from a publicly available 1996 US Air Force document on the use of environmental modification techniques which indelibly provide evidence that the threats are real and must be addressed.

It should be noted that the US is in violation of a historic 1977 international Convention ratified by the UN General Assembly which banned "military or other hostile use of environmental modification techniques having widespread, long-lasting or severe effects." (AP, 18 May 1977). Both the US and the Soviet Union were signatories to the Convention.

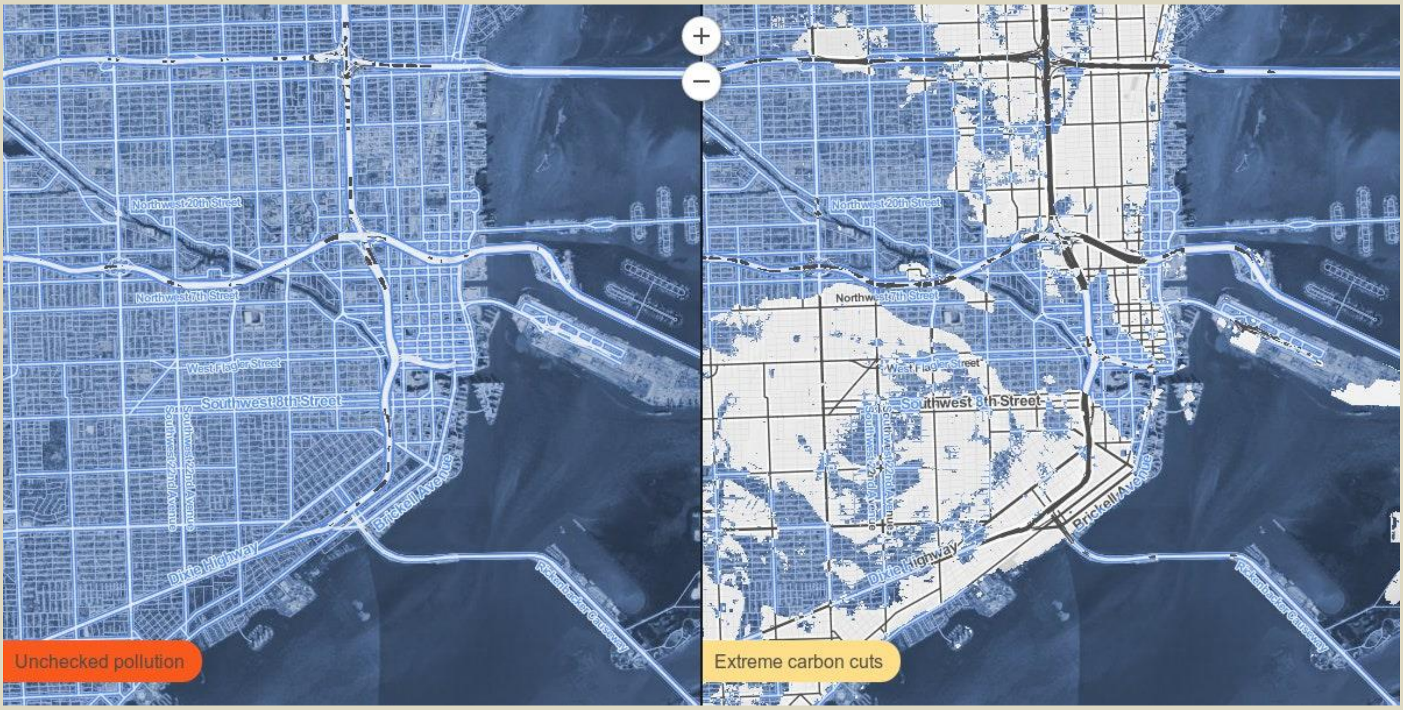
▶▶ **Read the full text at source's URL.**

***Michel Chossudovsky** is an award-winning author, Professor of Economics (emeritus) at the University of Ottawa, Founder and Director of the Centre for Research on Globalization (CRG), Montreal, Editor of Global Research. He has taught as visiting professor in Western Europe, Southeast Asia, the Pacific and Latin America. He has served as economic adviser to governments of developing countries and has acted as a consultant for several international organizations. He is the author of eleven books including The Globalization of Poverty and The New World Order (2003), America's "War on Terrorism" (2005), The Global Economic Crisis, The Great Depression of the Twenty-first Century (2009) (Editor), Towards a World War III Scenario: The Dangers of Nuclear War (2011), The Globalization of War, America's Long War against Humanity (2015).*

## Sea-Level Rise Affects Coastal Areas 4 Times Faster Than We Thought. Here's Why

Source: https://www.sciencealert.com/sea-level-rise-at-the-coast-is-happening-up-to-4-times-faster-than-we-thought

Mar 09 – The sea is rising, but that's not all. Scientists say current assessments of global sea-level rise have disregarded an important phenomenon affecting coastal regions – an oversight that means the ongoing specter of sea-level rise is even more ominous than we knew.



While the global average of sea-level rise attributable to melting ice masses in our warming world equates to about 2.6 millimetres per year over the last two decades, that measurement ignores a simultaneous and widespread occurrence where sea-level rise is at its most threatening: subsidence along the world's coastlines, often the result of human activity.

Less than a month ago, scientists explored the same issue within the limited context of the San Francisco Bay Area, highlighting how the colossal weight of the region was making it sink progressively lower, even while water levels along the shoreline are steadily moving in the other direction.

Unfortunately, this same issue is happening in coastal regions all over the world, and it's something that vastly alters the outlook of what 2.6 millimetres of annual sea-level rise actually means where it matters most.

"Rapid rates of subsidence in deltas and especially cities on deltas are also human-caused, mostly due to groundwater pumping, also oil and gas extraction, and sediment resupply prevented by upstream dams, flood defenses, sand extraction or mining," says coastal engineer Robert Nicholls from the University of East Anglia in the UK.

"About 58 percent of the world's coastal population lives on deltas where land is subsiding."

In a new study, Nicholls and his team quantified what sea-level rise actually looks like in coastal areas, once subsidence – both natural and human-caused – is taken into account.

According to their calculations, relative sea-level rise in affected regions is effectively happening up to four times faster than the global average otherwise suggests: representing between 7.8 to 9.9 mm per year.

That's a dramatically different rate of ongoing sea-level rise lapping at the world's coastlines, and it's something that's already affecting the majority of humans living on the planet, given our species' tendency to congregate in urbanized coastal areas – vulnerable, sinking cities that are the most exposed to rising tides.

"These findings have important implications for coastal management, climate action and sustainability goals," the researchers explain in their paper.

"For climate mitigation, they mean that contemporary and future global sea-level rise risks and adaptation needs are much higher than previously assessed."

To adapt to the newly identified pace of the threat, the researchers say we need to look into ways to reduce human-induced subsidence, alongside existing policies working to mitigate the climate crisis, chiefly by reducing heat-trapping emissions caused by burning fossil fuels.

In the longer term, climate change mitigation strategies are the more important, the researchers say, but previous efforts to reduce subsidence in the Netherlands, Japan, and China have shown that we can slow down sinking rates when responsible groundwater management policies are put in place in coastal cities.

As always, it's important to think positively and act decisively. Still, there's no denying the drastic implications if we don't address these findings now – and start to take local subsidence effects into consideration whenever we think and talk about sea-level rise.

It's not a far-off problem, either. Relative sea-level rise is already affecting millions of people living in the world today.

"The impacts of sea-level rise being experienced today are much larger than the global numbers being reported by the Intergovernmental Panel on Climate Change (IPCC)," Nicholls says.

"One of the main reasons that Jakarta, the capital city of Indonesia, is being moved to Borneo is because the city is sinking due to groundwater extraction from shallow wells… Jakarta might be just the beginning."

▶▶ **The findings are reported in** *Nature Climate Change*.

## Water Wars Are Here

**By Ben Frankel**

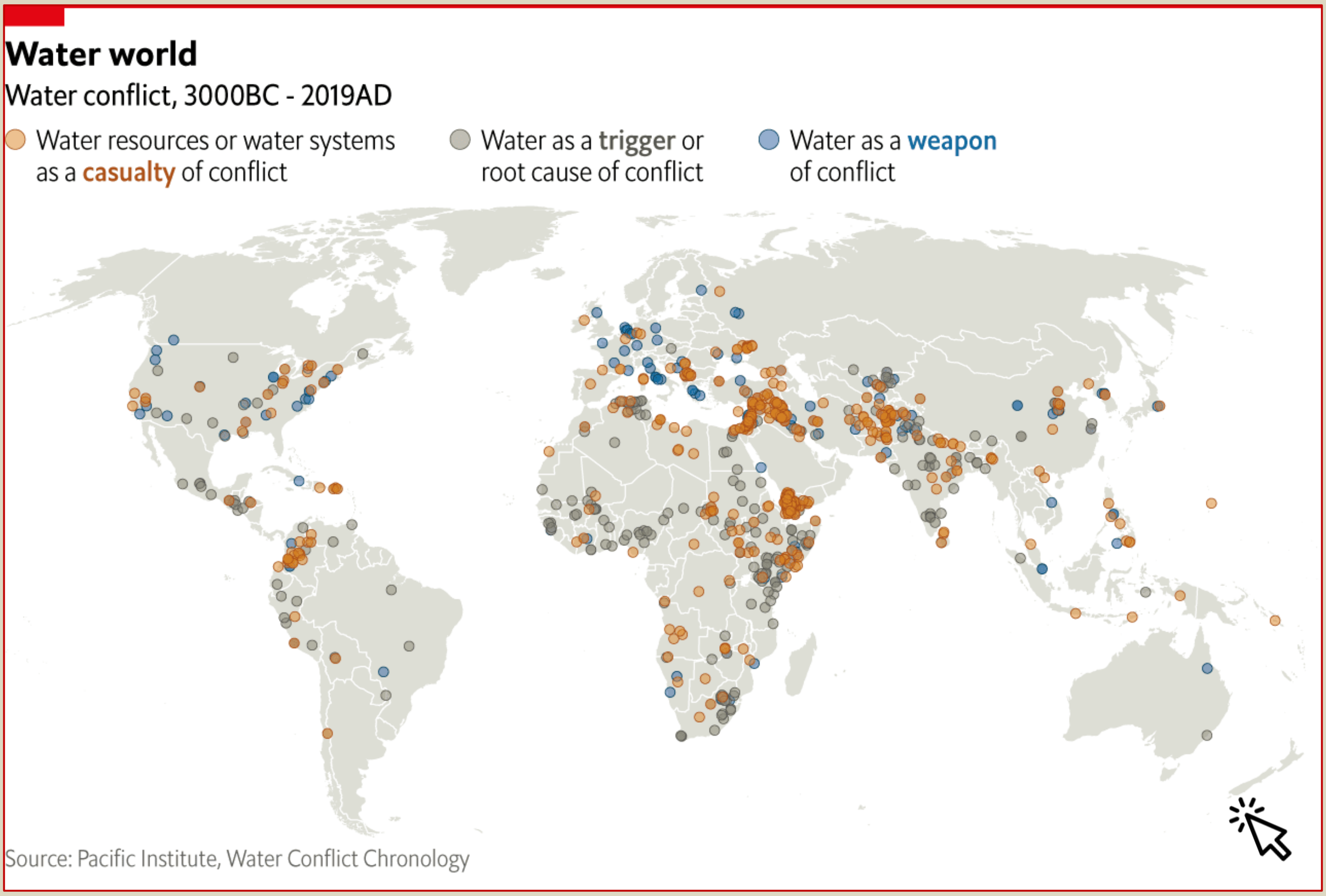
Source: http://www.homelandsecuritynewswire.com/dr20210319-water-wars-are-here

Mar 19 – In 2009, the U.K. intelligence services submitted their annual intelligence report to then-Prime Minister Gordon Brown, warning of the coming threat of "water wars" between states vying for diminishing fresh-water resources.

In the last decades, few regions have become water hot spots:

- The British intelligence services' report pointed out that the Asian subcontinent will likely be the theater of the first such war. In 2011, the *Nation*, a Pakistani newspaper, charged that India was engaging in "water terrorism." India is "rapidly moving towards its target of making Pakistan totally barren," the paper said, by building dams on three major rivers including Chenab, Jhelum, and Indus flowing into Pakistan from the Indian side of the border. The paper said that the dams were being built in violation of international laws and Indus Water Treaty signed between the two countries to ensure equitable distribution of water resources.
- Over the last five years, tensions have been rising between Ethiopia, on the hand, and Egypt, Sudan, South Sudan, and Eritrea, on the other hand, over the massive Grand Ethiopian Renaissance Dam which Ethiopia has been building on the Blue Nile River. Its neighbors worry that Ethiopia will use the dam to deny them essential water from the Nile, on which their economies depend. Egypt has publicly said it would resort to military action to prevent this eventuality.

- Iraq and Syria have voiced similar concerns over the twenty-two dams Turkey has been building on the Tigris and the Euphrates as part of its ambitious Southeastern Anatolia Project.



Water world

Water conflict, 3000BC - 2019AD

● Water resources or water systems as a casualty of conflict
● Water as a trigger or root cause of conflict
● Water as a weapon of conflict

Source: Pacific Institute, Water Conflict Chronology

It appears that Turkey has began to use its dam system to deny water to the Kurdish region in northern Syria (see "Kurds in Northern Syria Warn of Water Crisis," HSNW, 19 March 2021), but observers note that the Turkish move will lead to water shortages throughout Syria, increasing tensions and instability in the region.

***Ben Frankel** is the editor of the Homeland Security News Wire*

HOTZONE
SOLUTIONS
**GROUP**

## The world's most practice oriented provider of Hazardous Substances Management Solutions

Consultation

Products

Training

Belgium
The Netherlands (HQ)
Serbia
USA
China
Middle East
India
Latin America
Australia and New Zealand

**https://hotzonesolutions.org**