# 2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

November 2019

## A new threat?

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

# CBRNE DIARY

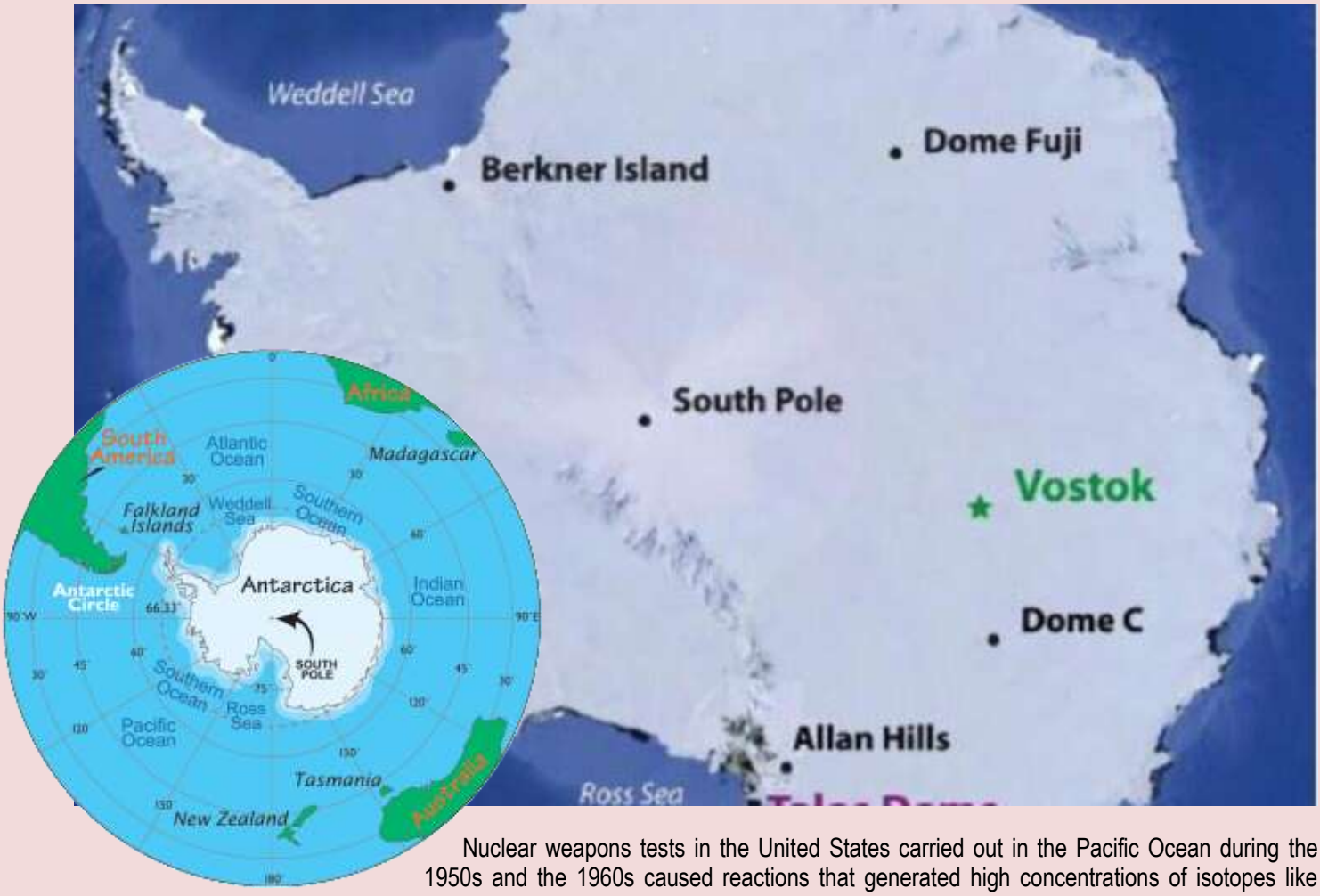
# DIRTY R-NEWS

# Radioactive chlorine from nuclear bomb tests still present in Antarctica

Source: https://phys.org/news/2019-10-radioactive-chlorine-nuclear-antarctica.html

Oct 16 – Antarctica's ice sheets are still releasing radioactive chlorine from marine nuclear weapons tests in the 1950s, a new study finds. This suggests regions in Antarctica store and vent the radioactive element differently than previously thought. The results also improve scientists' ability to use chlorine to learn more about Earth's atmosphere.

Scientists commonly use the radioactive isotopes chlorine-36 and beryllium-10 to determine the ages of ice in ice cores, which are barrels of ice obtained by drilling into ice sheets. Chlorine-36 is a naturally occurring radioactive isotope, meaning it has a different atomic mass than regular chlorine. Some chlorine-36 forms naturally when argon gas reacts with cosmic rays in Earth's atmosphere, but it can also be produced during nuclear explosions when neutrons react with chlorine in seawater.




Nuclear weapons tests in the United States carried out in the Pacific Ocean during the 1950s and the 1960s caused reactions that generated high concentrations of isotopes like chlorine-36. The radioactive isotope reached the stratosphere, where it traveled around the globe. Some of the gas made it to Antarctica, where it was deposited on Antarctica's ice and has remained ever since.

Other isotopes produced by marine nuclear bomb testing have mostly returned to pre-bomb levels in recent years. Scientists expected chlorine-36 from the nuclear bomb tests to have also rebounded. But new research in AGU's *Journal of Geophysical Research: Atmospheres* finds the Vostok region of Antarctica is continuing to release radioactive chlorine into the atmosphere. Since naturally produced chlorine-36 is stored permanently in layers of Antarctica's snow, the results indicate the site surprisingly still has manmade chlorine produced by bomb tests in the 1950s and in the 1960s.

"There is no more nuclear chlorine-36 in the global atmosphere. That is… why we should observe natural chlorine-36 levels everywhere," said Mélanie Baroni, a geoscientist at the European Centre for Research and Teaching in Geosciences and the Environment in Aix-en-Provence, France, and co-author of the new study.

Studying the chlorine's behavior in Antarctica can improve ice dating technology, helping scientists better understand how Earth's climate evolved over time, according to the study's authors.
Vostok and Talos Dome are both shown on this map of Antarctica. Vostok is still releasing anthropogenic chlorine-36 into the atmosphere. Credit: AGU
In the new study, Baroni and her colleagues examined chlorine emissions in different parts of Antarctica to better understand how chlorine behaves over time in areas where annual snowfall is high versus areas where snowfall is low. The researchers took ice samples from a snow pit at Vostok, a Russian research station in East Antarctica that receives little snow accumulation, and compared them to ice samples from Talos Dome, a large ice dome roughly 1400 kilometers (870 miles) away that receives a lot of snow accumulation every year.
The researchers tested samples from both sites for concentrations of chlorine-36 and determined how much chlorine was present in Vostok's ice from 1949 to 2007 and how much was in Talos Dome's ice from 1910 to 1980.
The results showed chlorine-36 in Talos Dome ice has gradually decreased over time, holding only four times the level of natural chlorine-36 level, in 1980. However, the Vostok ice showed very high levels of chlorine-36, with the top of the snow pit reaching levels of 10 times the expected natural concentration in 2008.
The consistently higher levels suggest the Vostok snowpack is still releasing radioactive chlorine from the 1950s and 1960s marine nuclear bomb tests. The amount of radioactivity is too small to have an effect on the environment, but the results are surprising because a different radioactive isotope produced by nuclear tests had already returned to prebomb levels in Vostok, according to the study's authors. They had hypothesized chlorine-36 would behave similarly.
They also compared the Vostok ice samples with samples from the same site taken in 1998. Measuring the depth of each sample, they found chlorine-36 had moved closer to the surface of the snowpack, which was surprising, according to Baroni. The chlorine was not only spreading to the atmosphere from the firn surface of the snowpack, but moving up from the snowpack's depths, meaning the chlorine is more mobile scientists previously thought.
Scientists are currently planning to drill for a 1.5 million-year-old ice core in the Antarctic and understanding how Vostok releases manmade chlorine-36 could improve how scientists use the isotope to glean data from the ancient ice core, Baroni said.
Determining how manmade nuclear chlorine-36 moves in low snow accumulation zones over the last century could serve as a microcosmic example for how natural chlorine-36 has built up in snowpacks over the last 1 million years, according to the study authors. The results give more information to future scientists using the isotope to date ancient ice and uncover Earth's past climate, according to the study.

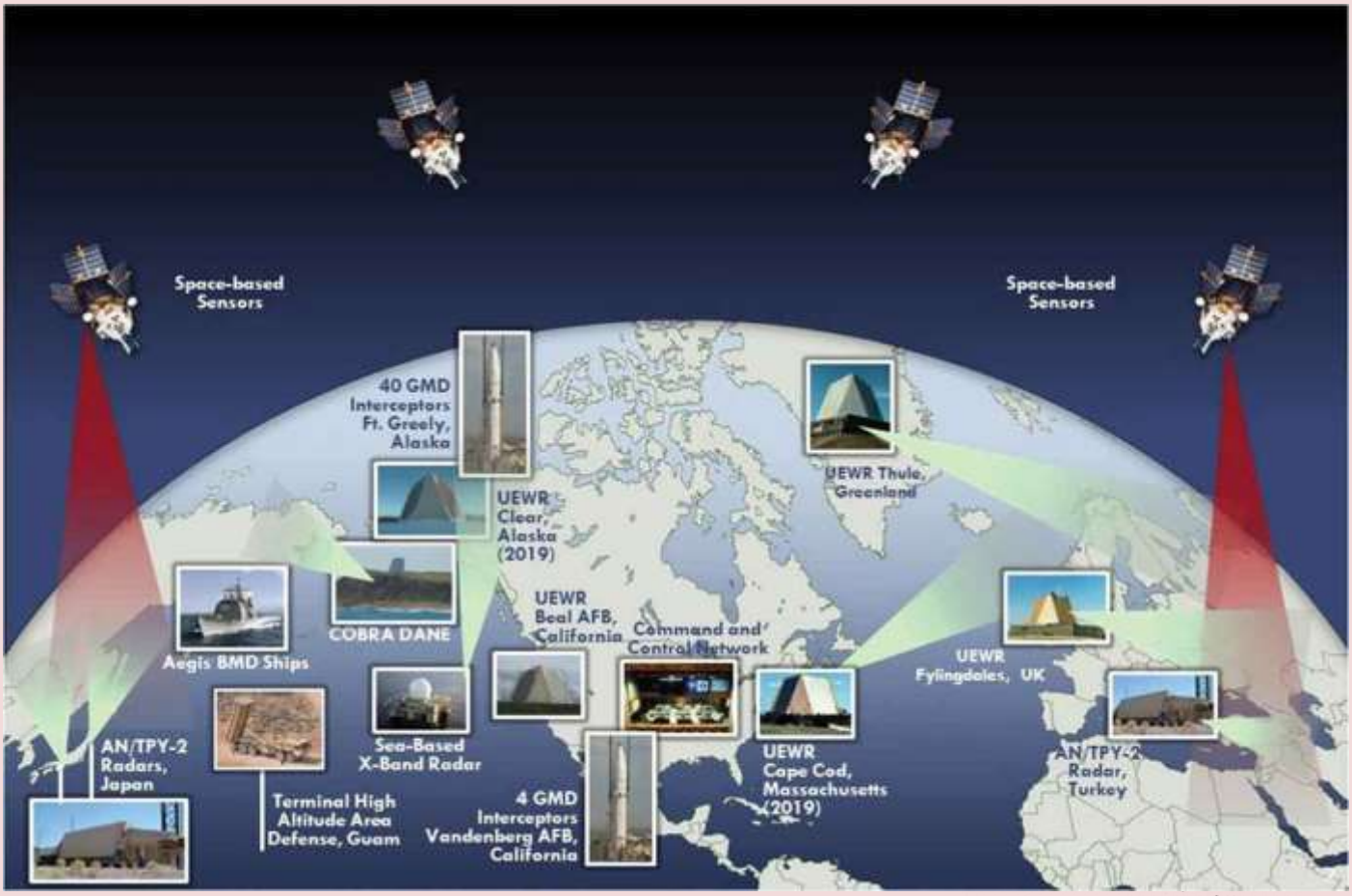
# US ballistic missile defenses, 2019

**By Matt Korda and Hans M. Kristensen**
Source: https://tandfonline.com/doi/full/10.1080/00963402.2019.1680055

Oct 24 – The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Matt Korda, a research associate with the project. The Nuclear Notebook column has been published in the Bulletin of the Atomic Scientists since 1987. This issue examines the status of US missile defense, a key driver of the global nuclear arms race. According to the latest Missile Defense Review, the United States will continue to enhance its four primary missile defense systems – one for homeland defense and three for regional defense – without "any limitation or constraint."

| System | Theater | Designed to Counter | Warhead | Speed (km/s) | Deployment | Performance Record |
|---|---|---|---|---|---|---|
| Ground-based Midcourse Defense | Homeland | Strategic ballistic missiles in midcourse phase of flight. | Hit-to-kill | 7.6 | 40 interceptors at Ft. Greely, AK<br>4 interceptors at Vandenburg AFB, CA.<br>By 2023: 20 additional interceptors at Ft. Greely, AK. | 11 successes in 19 attempts. |

| System | Theater | Designed to Counter | Warhead | Speed (km/s) | Deployment | Performance Record |
|---|---|---|---|---|---|---|
| THAAD | Regional | Short- and medium-range ballistic missiles in exo- or endo-atmospheric terminal phase of flight. | Hit-to-kill | 2.8 | 7 batteries, many deployed abroad, including in Guam and South Korea. Additionally purchased by UAE and Saudi Arabia. | Pre-2006: 2 successes in 8 attempts. Post-2006: 16 successes in 16 attempts. |
| Aegis SM-3 | Regional | Block IA and IB: Short-, medium-, and intermediate-range ballistic missiles during their midcourse and terminal phases of flight. (Block IIA: rudimentary ICBMs) | Hit-to-kill | SM-3 Block IA and IB: 3.0 SM-3 Block IIA: 4.5 | Aegis ships: Five Ticonderoga (CG-47) class cruisers and 33 Arleigh Burke (DDG-51) class destroyers. Aegis Ashore: Romania (2016) and Poland (2020). | 34 successes in 43 attempts. |
| PAC-3 | Regional | Short- and medium-range ballistic missiles during their terminal phase of flight, in addition to aircraft. | Hit-to-kill | 1.4 | Bahrain, Germany, Greece, Israel, Japan, Kuwait, the Netherlands, Poland, Qatar, Romania, Saudi Arabia, South Korea, Spain, Sweden, Taiwan, and the United Arab Emirates. | Very poor success rate during Gulf wars, likely only a few isolated intercepts. |




Doing so is likely to be destabilizing, as potential adversaries will attempt to build offensive systems to offset the United States' defensive systems. This dynamic is currently on display with Russia and China, both of which are developing missiles that are specifically designed to counter US missile defenses.

# UAE's first nuclear plant to begin major testing on third reactor

Source: https://www.thenational.ae/uae/government/uae-s-first-nuclear-plant-to-begin-major-testing-on-third-reactor-1.900569

Aug 20 – The opening of the UAE's first nuclear power plant has moved a step closer.

Operators on Tuesday said the plant's third nuclear reactor – unit three – had been connected to the country's electricity grid.
The significant development allows for major tests of the reactor to take place and, over the next few months, at least 200 assessments will be carried out on the reactor's systems. Unit three will also undergo what is known as "hot functional testing" which assesses its cooling and safety systems before nuclear fuel is added.
"I am proud of the continued progress being made at unit three of the Barakah Nuclear Energy Plant," said Mohamed Al Hammadi, chief executive of Emirates Nuclear Energy Corporation.
"We have maintained our track record of safety and efficiency with the successful energisation [the formal term for connection to the grid] of the unit's transformers and we continue to establish Barakah as the benchmark for new nuclear construction projects worldwide."
Construction of the **Barakah Nuclear Energy Plant in Al Dhafra is now about 93 per cent complete** and, when all four reactors are working, it will provide **close to 25 per cent of the UAE's electricity needs.**
Operators did not reveal an opening date for the plant. Construction of the $25 billion (Dh91bn) facility began in 2011, with electricity generation set for 2017.
But it is now thought the reactors will not start producing electricity until late this year or early next.
To begin generating power, the reactors must be loaded with uranium pellets and these generate heat through a controlled nuclear reaction. This heat is transferred to water which creates steam to drive the turbines.
Barakah is being built in co-operation with the Korea Electric Power Corporation and to begin working, it must get a licence from the Federal Authority for Nuclear Regulation. The authority regulates the industry according to international standards.
**The Barakah plant's workforce is about 60 per cent Emirati, a quarter of whom are women.** This figure is believed to be the highest for any nuclear power company in the world.

# The Next Nuclear Weapons State: Australia?

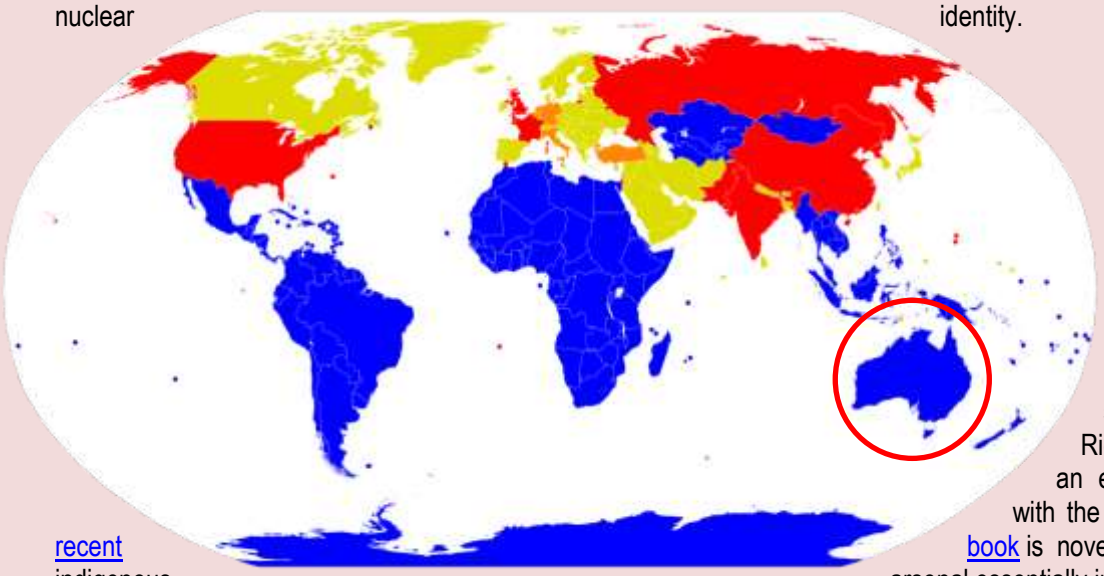
**By Rod Lyon**

Source: https://nationalinterest.org/blog/buzz/next-nuclear-weapons-state-australia-90661

Oct 27 – ASPI releases today the second issue of its Strategist Selections series, pulling together a collection of 36 of my *Strategist* posts on nuclear strategy. I'm honoured to follow in the footsteps of Kim Beazley, whose collected posts formed the first issue, and hope that readers find value in the latest publication. *The Strategist*, ASPI's commentary and analysis site, is now over seven years old, and a vast archive of more than 6,000 articles is there for the mining. I do not think the latest volume in the series could be timelier.
In recent months the question of whether Australia should build its own nuclear arsenal has received considerable attention. It's a question that demands careful handling, not least because it's an invitation to the incautious respondent to take a length of rope and hang themselves in the corner. And all too often, respondents do exactly that, burdening the

argument for a domestic nuclear arsenal with poor judgement, strategic paranoia and moral insensibilities.

For many years the simple, formal answer to the question has always been the same: Australia is a party to the Nuclear Non-Proliferation Treaty, and it is not a repentant state. (Repentant states are those that signed the treaty but later came to regret their own hastiness.) That's because the NPT generally represents the last major occasion on which states were asked to choose their nuclear identity.




The strategic commentariat has, over the years, been reluctant to challenge the choice Canberra made then. For good reason: Australia hasn't confronted a serious strategic challenge since Richard Nixon's opening to China, an event almost contemporaneous with the NPT. That's why Hugh White's recent book is novel. It explores the option of an indigenous arsenal essentially in 21st-century strategic terms.

**So, should Australia build its own nuclear arsenal?** I think the answer is, 'Yes, if it needs to.' That's a big 'if'—indeed, a series of big 'ifs': if the regional strategic environment becomes appreciably darker; if US extended nuclear deterrence is no longer available, or patently incredible; and, perhaps just as importantly, if there's bipartisan Australian acceptance of the need for an indigenous arsenal.

**The first 'if'** poses a major challenge of assessment: how dark does the regional strategic environment need to be? The fact that the Australian mainstream is already broken over the 'China threat', despite China's recent blatantly coercive behaviour, doesn't bode well for its ability to reach a consensus on what might constitute the grounds for initiating a nuclear-weapons program.

I'd venture one, imperfect, benchmark: the environment would need to be sufficiently dark that an Australian nuclear-weapons program would be seen (by some countries at least) as a positive contribution to regional stability. It certainly would have to be dark enough for us to satisfy the 'supreme national interests' test of Article X of the NPT—the article covering withdrawal from the treaty.

**The second 'if'**—extended deterrence—is already encountering some choppy waters, waters which Donald Trump's presidency has roiled rather than calmed. True, the administration's 2018 nuclear posture review comes closer to underlining the specific provision of a US nuclear umbrella to Australia than any of its predecessors. On page 22 of the main text, there's a sentence that reads: 'The United States has extended nuclear deterrence commitments that assure European, Asian, and Pacific allies.' That's an interesting separation of America's usually hyphenated Asian and Pacific allies, and may reflect a deliberate attempt by Washington to reinforce its assurance to Australia.

Still, US extended nuclear deterrence was a doctrine invented for a different era; it faces genuine credibility issues in a more risk-tolerant world, especially if themes of nationalism and buck-passing continue to resonate in US strategic policy.

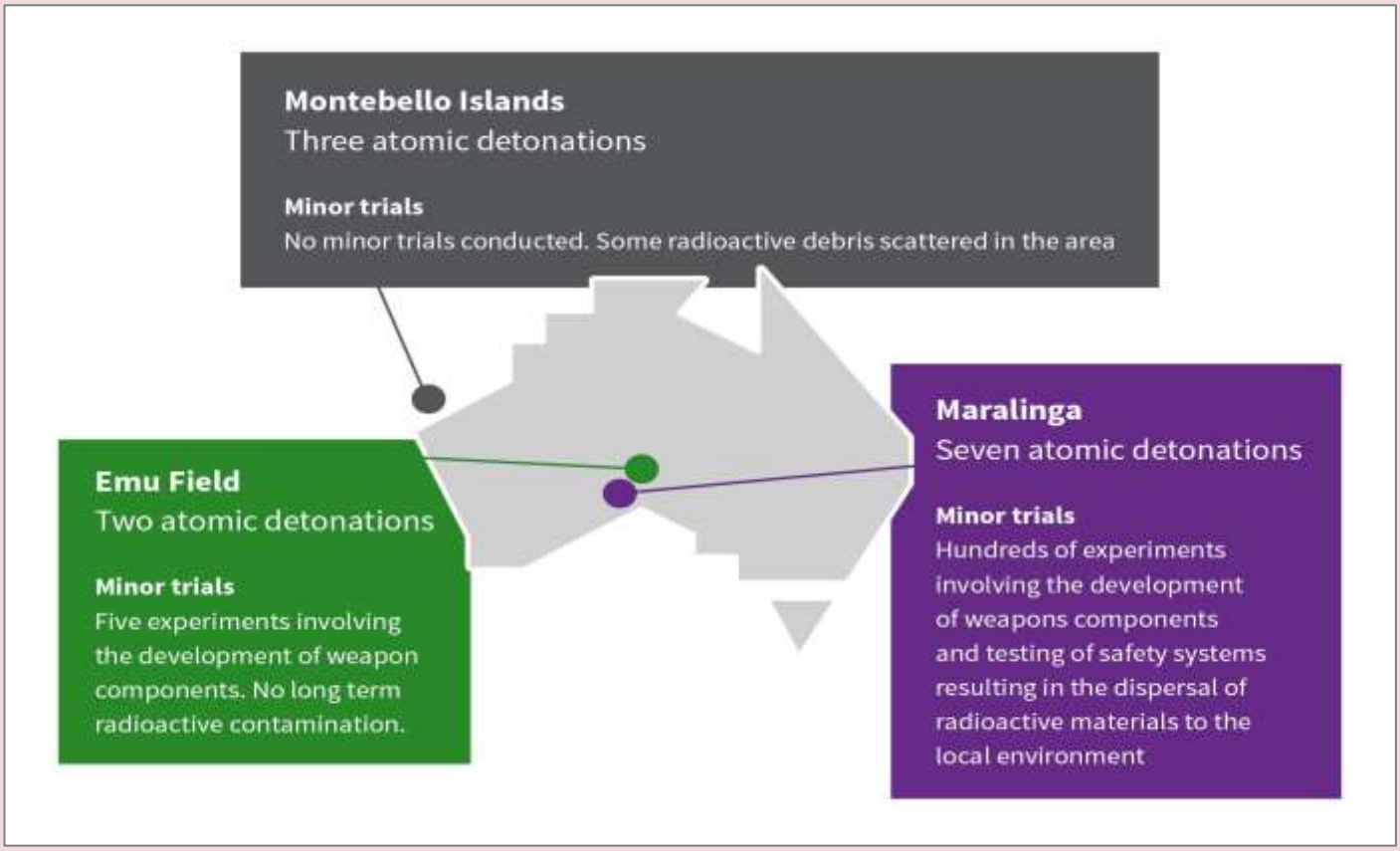
**The third 'if'** is just as awkward, and often overlooked. Australia, to use a rowing metaphor, hasn't got its head in the boat in relation to an indigenous nuclear-weapons program. For Australian thinking about nuclear weapons to change, we'd probably have to be facing an existential threat. Only such a condition could generate the level of bipartisan agreement necessary to develop, build and deploy a serious nuclear force.

But, of course, if we were staring down the barrel of an existential threat, we'd probably want to have a nuclear arsenal to hand relatively quickly. And there's the problem. Nuclear-weapons programs take time. In wintertime, many Canberrans are acutely conscious of how far their most remote hot-water tap is from their hot-water system, and the amount of time it takes for hot water to move through the house. But pursuing an indigenous nuclear-weapons program in Australia's current circumstances would be worse: it would be the equivalent of turning on a tap in a house to which no hot-water system had ever been fitted.

It would be easier to build nuclear weapons if we had in place a stronger core of nuclear skills in our workforce, some capacity to produce fissionable materials, and a suitable delivery vehicle. (More 'ifs'.) Australia has few of those assets. We have one research reactor at Lucas Heights. We have neither an enrichment capability for uranium nor a reprocessing

facility for plutonium. And our best delivery vehicle, the F-111, has long since faded into history. If Australia was to attempt to proliferate, using only national resources, we'd likely face a 15-year-plus haul.
Working in partnership with others would allow us to shorten that timeframe. Indeed, in a post-NPT world we might even be able to buy an arsenal, or critical parts thereof, off the shelf—our usual path to acquiring high-technology military weaponry. But that seems an unlikely scenario.
Nuclear weapons cast long political shadows—which, indeed, is their primary purpose. But they're also weapons of mass destruction, meaning a decision to proliferate should never be taken lightly.
Personally, I think there are enough large strategic variables already at play that we should be thinking now about an indigenous nuclear-weapons program in much the same way that we did between the 1950s and 1970s. That is, we should be acting to minimise the lead time required for us to have such a capability, just in case we decide we do need it.

▶▶ **Read also:** https://en.wikipedia.org/wiki/Nuclear_weapons_tests_in_Australia




***Rod Lyon*** *is a fellow at ASPI and executive editor of The Strategist.*

# An update from Fukushima, and the challenges that remain there

**By Tatsujiro Suzuki**
Source: https://thebulletin.org/2019/11/an-update-from-fukushima-and-the-challenges-that-remain-there/

Nov 11 – After more than eight years, Japan is still struggling with aftermath of the 2011 Fukushima nuclear disaster. The Japanese government and nuclear industry have not solved the many technical, economic, and socio-political challenges brought on by the accident. More worrying, they continue to put special interests ahead of the public interest, exacerbating the challenges and squandering public trust. The longer these issues remain unsolved, the more difficult it will be to restore this trust.

**Technical challenges**
The most difficult challenge is, of course, the decommissioning of the Fukushima Daiichi reactors. It would take too long to describe all of the technical challenges of the decommissioning operations, but two recent events are instructive of the overall difficulties.

The first is the dismantlement of the joint exhaust stack for units one and two. This stack stands 120 meters tall and is at risk of collapse because of fractures in its pillars. It was also heavily contaminated by the venting of radioactive gases during the accident. So, the stack must come down, and the operation to deconstruct it must be done remotely from the stack itself to avoid exposing workers to dangerous radiation. According to the Tokyo Electric Power Company (TEPCO), the operation was supposed to be simple: cut down the top of the tower using special remote-controlled equipment, slicing pieces from the top of the chimney one by one and guiding them down by crane. Originally, the operation was supposed to start in March 2019, but TEPCO deployed an operation tower that was about three meters too short for the task, meaning it needed to rebuild the tower before starting. The cutting operation began on August 1, but the project has already faced numerous additional delays because of technical difficulties that include malfunctions of the crane, the camera on the cutting machine (which is needed to monitor the operation), the saws of the cutting machine, and both the main generator and sub-generators. The operation was supposed to finish by the end of 2019 but will now drag on until at least March 2020.

Workers stack bags of soil collected during Fukushima decontamination and cleanup operations, 2011. Photo credit Ricardo Herrgott for Global 2000.

The second technical problem, which is much more serious than the first, is the management of contaminated water. The water is continuously injected into the reactors to cool the fuel debris, and then treated to remove most—though not all—of the radioactive materials. The so-called "treated water" is being stored on site and amounts to about 1.1 million tons, with several hundred tons being added every day. According to TEPCO, the total tank capacity to store treated water will be approximately 1.37 million tons by the end of 2020, but the volume of treated water will exceed storage capacity by 2022. A subcommittee of the Ministry of Economy, Trade, and Industry recommended that the treated water, which still contains tritium, should be released into the sea once the radioactive concentration is below the standard agreed beforehand. The agreed standard between TEPCO and the local fishing industry association is 1,500 becquerels per liter (Bq/l), which is far below the drinking water standard for tritium water of 10,000 Bq/l set by the World Health Organization. An additional condition of release, however, is that all other radioactive substances besides tritium must be removed below a detectable limit or in line with regulatory standards. Unfortunately, in

August 2019 news outlets reported that some radioactive materials such as iodine 129 were not completely removed and that their concentration levels were above the regulatory standards.
Most recently, the super typhoon Hagibis hit the eastern part of Japan, which includes Fukushima prefecture and the area affected by the nuclear accident. TEPCO reported irregular readings from sensors monitoring water at the Fukushima Daiichi plant but did not confirm whether any radioactive water leaked into the sea. In addition, according to the Tamura city government, some bulk bags filled with soil collected from decontamination operations were swept into a river during the typhoon on October 12. The bags were among 2,667 that have been temporarily stored at a site in the city. The Ministry of the Environment later confirmed that total of 11 bags were swept away and found downstream. Thankfully, there was no evidence that any of the contaminated soil leaked out. But this wasn't the first time an incident like this has happened. In September 2015, several hundred bags were swept downstream during flooding caused by tropical storm Etau. The recurring close calls reveal the ongoing vulnerabilities of the Fukushima and associated sites. The contaminated soil will need to be stored for at least 30 years, and the risk of possible leakage remains if a larger and stronger typhoon, or a tsunami, hits the region again.

**Economic challenges**

In December 2016, the Ministry of Trade, Economy, and Industry's committee for reforming TEPCO published its latest estimate for total accident costs, including decommissioning the reactors, compensation, and decontamination of the land. The total cost was estimated at almost 22 trillion yen ($188 billion), which was twice as much as the previous estimate of 11 trillion yen ($96 billion). More recent estimates have put the figure even higher—up to 80 trillion yen ($736 billion) over 40 years.
According to the legal scheme established by the ministry, TEPCO and other nuclear utilities will pay about 20 trillion yen of the total accident costs. But now the rest (2 trillion yen) will be footed by Japanese taxpayers. The 2016 report was the first time that the Japanese government admitted that tax money would be spent for the Fukushima accident costs.
The government's lack of transparency in agreeing to this scheme is a source of ongoing concern, not least because the taxpayer burden could balloon if total costs go up, or if the nuclear utilities cannot pay off the debt. The government has given no clear explanation why and how much tax money will be spent to cover the total accident costs. To make matters worse, the power utilities are passing on part of the accident cleanup costs to customers by increasing their electricity rates, but without disclosing the amount. This exceptionally high cost may have influenced the future economic competitiveness of nuclear power. At present, no utility has announced plans to build new reactors or to replace existing reactors.

**Socio-political challenges**

On September 19, 2019, three former top executives of TEPCO were found not guilty of criminal negligence for their roles in the disaster, which resulted in the death of 44 and the injury of 13 others. The Tokyo district court ruled that it was not realistic for the former executives to have prevented the triple core meltdown because they were not able to predict all possible tsunami scenarios. This was the only criminal case so far involving TEPCO officials and, although they were found not guilty, the case revealed new facts regarding the tsunami predictions. A 2008 TEPCO internal study, based on a 2002 report by a government panel, concluded that a wave of up to 15.7 meters could hit the plant after a magnitude 8.3 earthquake, overwhelming the Fukushima site, which sits 10 meters above sea level. The findings were reported to the TEPCO executives, but they did not act to take measures against such high-tsunami scenarios. The court decision was totally unsatisfactory to the public, especially for the victims in Fukushima who were forced to leave their homes. For them, it is now clear that the accident was preventable and that no one at TEPCO will be held accountable for their lack of action to prevent it.
Although the criminal case was highly symbolic, it is not the only legal one involving TEPCO and Fukushima. More than 100,000 evacuees have filed about 30 different civil lawsuits seeking compensation from TEPCO and the government. Several district courts have ruled that TEPCO could have predicted and prevented the nuclear crisis and have awarded millions of dollars in damages to the evacuees.
TEPCO isn't the only utility with a public relations problem. On September 27, 2019, the Kansai Electric Power Company held a press conference to disclose that 20 of its employees, including top executives, received inappropriate payments and gifts worth a total of $2.9 million from a senior local government official in Takahama, a town that hosts one of the company's four nuclear power plants. This has become the biggest scandal since the 2011 Fukushima accident and has exposed the collusive relationship between the utility companies and local public officials as well as the connection between the utilities and local construction companies, which may have benefited from favorable contracts for necessary safety upgrades at the nuclear plants. In October, the chairman, executive vice president, and three executive directors resigned, while the president of the company stepped down from his position as the head of the powerful Federation of Electric Power Companies of Japan. Although Kansai Electric Power Company planned to restart units one and two of its Takahama nuclear plant earlier this year, that plan is now on hold indefinitely.

These two recent events show that social and political problems persist even eight years after the Fukushima accident. According to the latest public polling conducted in 2018 by Japan Atomic Energy Relations Organization, a utility-sponsored pro-nuclear organization, only 6.7 percent of the public think nuclear industry organizations are trustworthy or somewhat trustworthy (a decline from 7 percent in 2017), and only 7.9 percent of the public think the government is trustworthy or somewhat trustworthy (a decline from 9.2 percent in 2017).

**Lessons not learned**

The ongoing technical, economic, and socio-political problems demonstrate that the nuclear power industry and the Japanese government haven't learned their lesson from the Fukushima accident, which is that **transparency is the key to public trust.** It is true that the quantity of information about cleanup has increased substantially over the years. But transparency means that the utilities and the government need to disclose information that the public needs, even when it is not favorable to them. One solution, which they have so far been unwilling to accept, would be to establish a truly independent third party to oversee their activities. Lack of such an independent oversight organization is one of the main causes for not taking alternative and possibly better, more appropriate measures over the last eight years.

***Tatsujiro Suzuki*** *is vice director and professor at the Research Center for Nuclear Weapons Abolition at Nagasaki University, Japan*

# How Long until Iran Builds a Nuclear Weapon?

Source: http://jcpa.org/how-long-until-iran-builds-a-nuclear-weapon/

Nov 11 – Behrouz Kamalvandi, spokesman for the Atomic Energy Organization of Iran (AEOI), said during a press conference at the Fordow nuclear site on November 7, 2019, that the organization was instructed to enrich uranium to a level of 5 percent but "is capable of reaching an enrichment level of 20 and even 60 percent. At the moment, the need is for 5 percent."[1] He added Iran had reached an enrichment level of 4.5 percent at Fordow this summer, and that the IAEA inspectors who came to examine the site would confirm the 5 percent level.[2] Kamalvandi stressed that the Fordow enrichment facility is essential for the process of enriching uranium to a level of 20 percent for Iran's fuel cycle.[3]

"Today," the spokesman continued, "a container carrying 2,000 kg of UF6 Uranium Hexafluoride gas was transferred from Natanz enrichment plant to the Fordow nuclear plant, and the transfer was done under the supervision of IAEA agents."[4]

Ali Akbar Salehi, the head of Iran's atomic energy organization, announced on November 4, 2019, that the Natanz plant produces today a tenfold increase in enriched uranium production to five kilograms per day, up from 450 grams two months ago. Salehi inaugurated a chain of 60 modern and faster IR-6 centrifuges, replacing the first generation IR-1 models.[5]

Kamalvandi, the AEOI spokesman, added that the Fordow enrichment site is "protected and fortified and that Iran indeed undertook not to enrich uranium there for a period of 19 years, but all the activity there is uranium enrichment for peaceful purposes." He asserted, "While the United States and Israel indeed claim that Iran is trying to achieve a nuclear capability, unfortunately it is they who are working to produce nuclear weapons."

The core of the Arak Heavy Water Reactor in Natanz (*Islamic Republic News Agency, September 9, 2017*).

Kamalvandi's words define Iran's "fourth step" to reduce its commitments under the JCPOA. Iran continues to erode its obligations under the nuclear agreement (JCPOA) in light of the ongoing failure of talks with the European countries on compensating Iran for the United States' withdrawal from the deal and renewal of sanctions on Iran.

As part of the fourth stage, Iran began injecting UF6 Uranium Hexafluoride gas into 1,044 centrifuges at the underground nuclear site in Fordow. The nuclear deal allowed Iran to operate IR-1 centrifuges, Iran's first model, that were spun empty under the terms of the 2015 JCPOA. Iran claims that according to articles 24 and 36 of the agreement, it is allowed

to forgo its obligations if the other side does not meet its own commitments and that this does not constitute a violation of the deal. The United States called Iran's latest move, "a big step in the wrong direction." The AEOI spokesman said Iran had taken this step to encourage the European signatories of the nuclear deal to uphold their commitments and to "bring them back to reality," meaning Iran is not the only one that is supposed to honor its obligations.

Kamalvandi reiterated Iran's position that, from an ideological and a strategic standpoint, Iran "is not even thinking about a nuclear bomb or other weapons of mass destruction." He recalled Supreme Leader Khamenei's *fatwa* [religious ruling] on nuclear weapons: "As the Leader of Iran said and even emphasized in the fatwa, the production or accumulation of nuclear weapons or weapons of mass destruction, or the use of them, is against our ideology."

The renewal of the enrichment activity at Fordow is significant in terms of enrichment capability. From a level of 8,600 SWU/kg (Separative Work Units, the measurement unit for the enrichment procedure), that capability has now risen to 9,500 SWU, very close to the enrichment level that Iran reached before signing the nuclear deal. "How far we will be able to go toward a million SWU," said Kamalvandi, "depends on the capability of our equipment."[6]

**Iran Designs and Produces its own Nuclear Equipment**

Iran's nuclear technology head, Ali Akbar Salehi, announced on November 10, 2019, that Iran was ready to share its expertise in nuclear power production with its Persian Gulf neighbors. The offer extends to nuclear energy technology.

Salehi was speaking at a groundbreaking ceremony at the extension of the civilian nuclear power plant (NPP) at Bushehr in southern Iran. The construction of the first Bushehr facility began in 1975, and it was delayed and redesigned several times by German and Russian firms. It finally came online in 2011, under Russian management.

The head of Iran's nuclear energy organization said that six years after its groundbreaking, the expanded Bushehr NPP is operated entirely by Iranian experts with all the necessary equipment installed indigenously. The building costs of the reactor will be paid over the course of six to eight years, and with oil fuel costing $60 a barrel today, the reactor will save almost $700 million annually.

Ali Akbar Salehi, head of Iran's Atomic Energy Organization, shows Iran's President Hassan Rouhani models of nuclear centrifuges. (*Iranian President's Office*)

The International Atomic Energy Agency reported in October 2019 that Iran is designing and producing all necessary nuclear equipment, including various models of centrifuges. Ali Asghar Zarean, special advisor to Salehi, emphasized, "100 percent of the Iranian nuclear industry is local, and today Iran can independently provide all its requirements in design and production of different centrifuge models."


Iranian centrifuge models (*Iranian press*)

As part of the strategy it has adopted, Iran continues to build capabilities that will enable it to return quickly to a fully active military nuclear program whenever it chooses to do so. At the same time, Iran continues to develop the nuclear power plant (NPP) complex in Bushehr.

U.S. Secretary of State Mike Pompeo said that the steps Iran is taking to erode its commitments to the nuclear deal are shortening its breakout time toward producing nuclear weapons. In any event, it appears that Iran does not intend to budge from its condition for a renewal of the negotiations – the lifting of the sanctions. Hence, the freeze in the talks with the European

partners over the deal appears likely to continue, and so do Iran's steps toward renouncing its commitments under the agreement.

## Sunflowers used to clean up radiation

Source: https://japantoday.com/category/national/sunflowers-used-to-clean-up-radiation

Aug 18 – Scientists have discovered that sunflowers can pull radioactive contaminants out of the soil. Researchers cleaning up the Fukushima site in Japan are putting the flowers to the test. The idea was tried back in the mid-1990s near the Chernobyl power plant meltdown. Soil scientist Michael Blaylock, who worked on that project, and who is vice president of systems development at Edenspace Systems Corp in the U.S., tells Living in Japan's Bruce Gellerman how this clean-up-by-plant works.

GELLERMAN: So, sunflower plants and nuclear power plants - what's the connection?

BLAYLOCK: Well, the connection there is really that sunflowers are really good at taking up certain radioactive isotopes. And that's really the connection between the sunflowers and the nuclear power plants.

GELLERMAN: So basically, the plant just kind of grows, and as it grows, it's sucking the radiation out of the soil?

BLAYLOCK: That's correct. Those radioisotopes mimic some of the nutrients that the plant takes up normally. And so the plant really doesn't distinguish between those radioactive isotopes and some of the nutrients like potassium and calcium that it takes up as a matter of course.

GELLERMAN: Well, you worked at Chernobyl back in the mid-1990s. Did it work?

BLAYLOCK: It was very effective for the water. The soil was a little bit of a different story because cesium in soil is a little bit tricky. Strontium is in soil, too. If you can't take both of them out, taking just the strontium doesn't necessarily get you to where you want to be if you leave the cesium around.

GELLERMAN: So why is cesium harder to get out than strontium?

BLAYLOCK: Well, **cesium mimics potassium**. The clay layers on a very small scale, the atomic structure, they have what we call, for lack of a better word, a cavity in between those clay layers. And the potassium fits very nicely into those cavities and that's the way that soils retain potassium. Cesium, being very similar to potassium, fits in those same cavities and it becomes fixed in the soil and it is very difficult for it to come out. Whereas strontium is very similar to calcium and calcium is in a form that is very available to plants - we don't have that problem.

GELLERMAN: Well, we're trying this at Fukushima. Do you think it could actually work there?

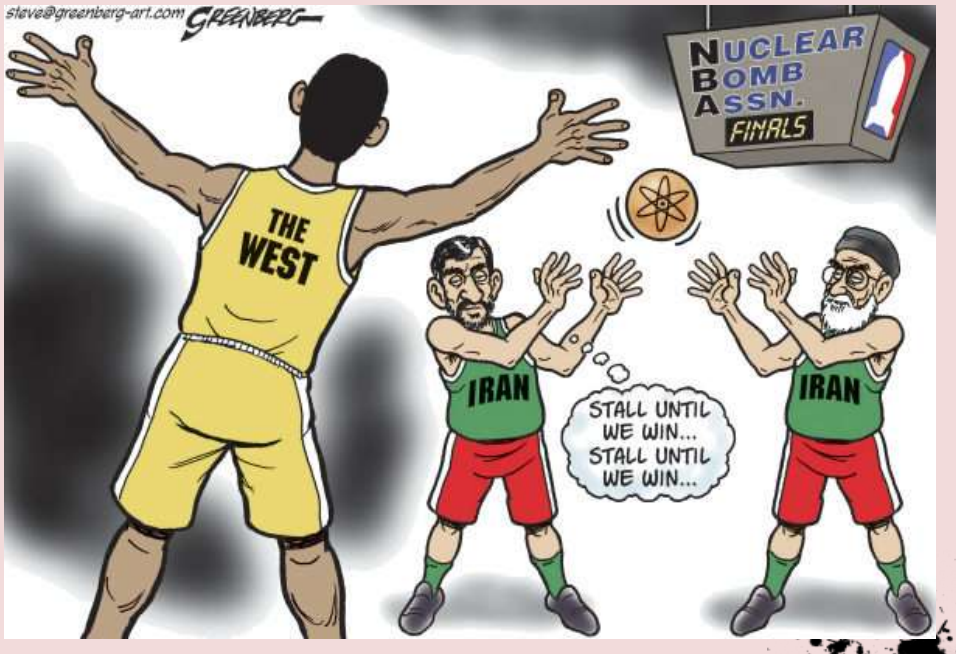
BLAYLOCK: It could, given the right set of circumstances. You know, one thing we found in Chernobyl is, we came there a number of years after the fact. And so that gave plenty of time for that cesium to become fixed in the soil, and it's going to become very dependent on the soil types. You know, soils that have very high mica contents, certain clays, are going to be very difficult to remove the cesium from, once the cesium gets fixed. But under the right set of circumstances, they could be effective in removing those contaminants from the soil.

GELLERMAN: So which part of the plant stores the radioactivity?

BLAYLOCK: You don't want to have to dig up roots – that's a very difficult process. It can be done but it's much easier to harvest leaves and stems. So, we focus our efforts on those plants that do a good job of translocating from roots to shoots.

GELLERMAN: Is the sunflower the best plant for this?

BLAYLOCK: Sunflowers are attractive because they grow well and produce a lot of biomass quickly. It doesn't take a lot of management to grow sunflowers as compared to some other crops; they are adaptable to a lot of different climates. So, I don't know that it is the best plant, but it is certainly one that meets the criteria that we need.
GELLERMAN: So. **when you harvest the plant, it's radioactive!**
BLAYLOCK: Yeah, the biomass, or the harvested material, would be radioactive.
GELLERMAN: What do you do then? How do you get rid of the radioactivity in the plant?
BLAYLOCK: The real process here is, what we're trying to do is, concentrate that radioactivity from the soil, which is a fairly low concentration, to a much higher concentration in the plant material. You still have to dispose of that plant material, but you move that particular contaminant or radioactive isotope from silica, aluminosilicate matrix in the soil, which is very difficult to deal with, to a carbon-based substance in the plant material. You concentrate that, so you have a lot less material to dispose of, and you can leave that soil, which is a resource that's hard to replace – you can leave that soil in place and just remove the contaminant.
GELLERMAN: And the radiation doesn't kill the plant as this is happening?
BLAYLOCK: Typically, not. If they're high enough to where they're going to affect the plant growth, it's not going to be an area that's suitable for this type of approach.
GELLERMAN: I can see unexpected consequences from something like this. I mean, here you have these sunflower plants, and the seeds dry, and birds eat the seeds and then they fly off, and they're radioactive.
BLAYLOCK: Yeah, that could be a risk. I mean, typically, when we performed this, we would always harvest plants before they seeded out because the main idea is to harvest biomass. You want to produce as much vegetative material as possible. And once the plants start producing seeds, its flowers start forming, it's not producing a lot more vegetative matter to remove that contaminant, so typically once the plant flowered, we harvested and we would replant again. We're not interested in producing seeds.
GELLERMAN: What about the hard-nosed question about money? How much does this cost relative to other technologies?
BLAYLOCK: Relative to other remediation technologies, it's not that expensive. But when you factor in that there's sampling and disposal of the material, it's certainly not free, but, you know, on a cost basis as compared to the cost of storing soil for a very long period of time, very large quantities of soil, it's a very attractive option.
GELLERMAN: You know, there's something very special about sunflowers. I mean, they're beautiful. And there's something poetic, I think, going on here because they're also an anti-nuclear symbol.
BLAYLOCK: Yeah, it is an interesting set of circumstances. And to see a field of plants out there growing in an area that previously was not vegetated, and you'd be able to harness nature to do some of the things that we need to do to, you know, correct our mistakes, it is something that's very pleasant to look at and to see. And it's one of those touchy-feely things that you feel really good about.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

# EXPLOSIVE NEWS

# Discover the spray used by Belgian police to train specialist dogs at airports

Source: https://www.euronews.com/2019/10/28/discover-the-explosive-spray-used-by-belgian-police-to-train-specialist-dogs-at-airports

Oct 28 – The explosive TATP has been used in several deadly terrorist attacks over the past two decades, which is why it is important that police are able to detect it.

But the substance is extremely dangerous to handle, making it difficult to train police dogs or to test detector devices in crowded places like airports. That's why European researchers have come up with a safe alternative — a **TATP spray**.

Brussels Airport was the site of a bomb attack in 2016 that claimed 32 lives and injured over 300 other people.


Here, police have trained specialist dogs to trace even the tiniest amounts of explosives.

Rony Vandaele, director of Belgian Federal Police's canine unit, told Euronews the dogs are better than all the alternatives.

"We can train them very well, we can teach them different kinds of explosives, and the way they work and the speed they work at is very effective," he said.

And you can't use a robot to replace them, to do the same work in the same amount of time".

To train the dogs, officers spray pieces of luggage with a solution containing TATP and line them up with people carrying unsprayed bags.

The police dogs reliably find the correct bags hidden among the passengers.

Vandaele said the spray contained "real TATP, but in a very small quantity."

"So it's a very useful and safe way to train dogs, and be sure that they can detect the suicide attackers willing to do attacks in some public space."

The spray is developed at the European Commission Joint Research Centre (JRC) in Geel, in the north of Belgium. produced with advanced equipment in well-controlled laboratories.

Authorities across the EU use it to ensure their explosive detection methods meet stringent European standards.

The spray is part of a test kit containing samples of various dangerous materials produced for aviation security inspectors.

Security staff are trained to use this kit with equipment like the electronic detectors that passengers will be familiar with seeing at airport checkpoints.

"The main component of the [TATP] spray is isopropanol, so it can be safely transported whenever there's need to use it," said Dimitris Kyprianou, a chemist at the JRC in Geel.

"Isopropanol quickly evaporates, leaving some TATP on the surface — a very small amount which is safe to handle".

It helps security staff identify TATP quickly and reliably.

Bartel Meersman, who leads the transport and border security unit at the JRC in Geel, said their work "gives necessary tools to the authorities to verify the equipment or to work better with the dogs.

"Of course, we're working to increase security in Europe, so if people go to a rock concert or they take the airplane at the airport that they can be secure, that they can travel or attend the event in a secure way".

## Why explosives detectors still can't beat a dog's nose

Source: https://www.technologyreview.com/s/614571/explosives-detectors-dogs-nose-sensors/

Oct 24 – For nearly as long as armies have fought one another, they have enlisted animals to help. Horses, especially, were decisive for millennia. As historian Morris Rossabi has written of the Mongol conquest of Asia, "Mobility and surprise characterized the military expeditions led by Genghis Khan and his commanders, and the horse was crucial for such tactics and strategy. Horses could, without exaggeration, be referred to as the intercontinental ballistic missiles of the thirteenth century." Historian David Edgerton notes that as late as the First World War, "Britain's ability to exploit world horse markets was crucial to its military power." Horses are still of occasional importance, as in the American invasion of Afghanistan in 2001, when Special Forces troops on horseback called in bomb strikes via satellite radios, using laser designators and GPS reference points to guide the bombs. But horses are only very rarely the tool that separates defeat from victory: in all but the most exceptional circumstances, they have been replaced by tanks, trucks, satellites, and airplanes.

Yet while horses are largely gone from modern armies, dogs are not. **As of 2016, the US military counted over 1,740 military working dogs among its ranks.** At Lackland Air Force Base in San Antonio, the military breeds its own sleek puppies—mainly German shepherds and Belgian Malinois—who are groomed for military service from their first whimper. Some will wash out; others will go on to four to seven months of basic obedience instruction before receiving more specialized training in how to guard bases, ambush enemy combatants, and sniff out explosive devices. From there the field narrows further. The US Army estimates that to produce 100 war-ready dogs, it must train 200.

Before entering buildings in Afghanistan, Thomas, a US army paratrooper who asked to be identified by a pseudonym, would often send his platoon's Belgian Malinois in first to ensure that no enemy soldiers or other surprises waited inside. During one day of particularly fierce fighting, Thomas was in a building, looking for somewhere to treat a wounded soldier, when he heard a noise from an adjacent room. As he rounded the corner to investigate, he remembers seeing "a shadow and a flash of light." It was a Taliban-hired Chechen fighter with an AK assault rifle aimed directly at his face.

Just as the fighter squeezed the trigger of his weapon, the platoon's dog came blazing into the room from the hallway and latched onto his neck, jerking him backwards. His shot was diverted, sparing Thomas's life.

After that, Thomas brought the dog on every mission he could. "Sometimes people would say to me—'Oh, you don't need a dog for that,'" he says. "And I'd say, 'Yeah, I need a dog. Are you on the ground? You're not on the ground. I'm bringing the dog.'"

The military also relies heavily on dogs to sniff out explosives. **Dogs' sense of smell is estimated to be 10,000 to 100,000 times stronger than the average human's.** Billions of dollars' worth of research on artificial detectors have yet to produce anything better. Unlike metal detectors, which are also used to locate roadside bombs and landmines, canines can be trained to pick up on non-metallic explosive devices concocted from fertilizer and other

household items. This talent has proved particularly useful in Afghanistan, where many buried explosives are improvised from common chemicals packed into plastic jugs.

**Scientists have long tried—and failed—to create devices capable of outperforming a dog's snout.** Starting in 1997, DARPA dedicated $25 million to an initiative called "Dog's Nose," which distributed grants to scientists to develop landmine detectors. At that point, an estimated 100 million mines were buried in approximately 60 countries. But according to the DARPA program's director, Regina Dugan, the technology to find them had not advanced much since the Second World War. "The only landmine detection equipment issued to US soldiers in the field were the metal detector and a sharp, pointy stick," she wrote in 2000. (The stick was to prod the ground for anomalies.)

The resulting machines, most of which featured polymer-coated tubes that reacted when exposed to explosives, seemed promising when used in sterile laboratories. But in more realistic environments' things got messier. When one of the machines was pitted against landmine-detecting dogs at Auburn University in Alabama in 2001, the highest-performing canines were approximately 10 times more sensitive. In a 22-acre grassy facility in Missouri where DARPA invited participants to test their devices, some were too responsive, reacting to plants and soil in addition to explosives.

A decade later, in 2010, the commander of the Joint Improvised Explosive Device Defeat Organization (JIEDDO) admitted that despite a whopping $19 billion of government investment in spy drones, radio jammers, and aircraft-mounted sensors meant to combat improvised explosive devices (IEDs), dogs remained unparalleled as detectors of the dangerous devices. While sensors typically found half of the IEDs before they exploded, dog teams located 80% of them.

**NIST**

The newest artificial detectors can detect smaller traces of chemicals than a dog can. But those detectors are big, explains Matthew Staymates, a mechanical engineer and fluid dynamicist at the National Institute of Standards and Technology (NIST): "It's got to plug into a wall, you need an enormous amount of infrastructure, gases, and vacuum pumps—and you have to bring the sample to your machine."

Nonetheless, artificial detectors have a role to play in places like airports, where all passengers must pass through security checkpoints, and dogs have provided inspiration for improving them. Staymates used a 3D printer to replicate the nose of a female Labrador retriever named Bubbles. The result is a snout-shaped extension that goes on the front of commercially available explosives detectors. It sniffs air like a dog, inhaling and exhaling several times a second instead of continuously sucking air in as such machines normally do.

The researchers found that this method, counterintuitively, pulls in samples of air from farther away, drawing in more of the chemicals floating around. "Nine times out of 10, you don't know where the bad guy with a pipe bomb in his backpack is," Staymates explains. "So, you want to be able to sample the environment in a smart way, and dogs have given us a lot of insight into what that looks like."

Despite this progress, a dog is still much more effective than an electronic bomb-sniffer—not least because an animal, like a human but unlike a machine, can react to unpredictable situations. So, some scientists have focused their efforts not on replacing working animals, but on improving their performance.

In 2017, a team at MIT's Lincoln Laboratory developed a new mass spectrometer, about the size of a large dresser, that could identify trace amounts of chemicals on a par with canine performance. Not only was it impressively sensitive, but it was fast, completing its assessments in about one second. The researchers were excited about the device's potential not to substitute for bomb-sniffing dogs, but rather to help train them. The team had dogs locate explosives previously hidden in canisters, which were also analyzed with the spectrometer. The machine discovered that some of the perceived errors the dogs made—identifying explosives in supposedly empty vessels—weren't errors at all; the containers had been cross-contaminated. That allowed the trainers to better regulate when to praise and reward their canine students, reinforcing their detection abilities.

Though some labs wanted to adapt the machine to replace dogs, the MIT team disagreed. In a news release at the time, Roderick Kunz, who led the research, said: "Our feeling is that such a tool is better directed at improving the already best detectors in the world—canines."

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

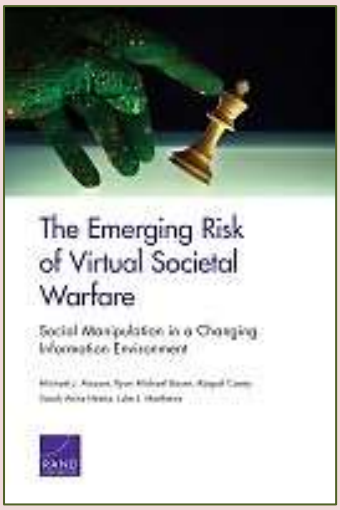
CBRNE DIARY

# CYBER NEWS

# Emerging Risk: Virtual Societal Warfare

Source: http://www.homelandsecuritynewswire.com/dr20191023-emerging-risk-virtual-societal-warfare

Oct 23 – The evolution of advanced information environments is rapidly creating a new category of possible cyberaggression which involves efforts to manipulate or disrupt the information foundations of the effective functioning of economic and social systems.




In a new RAND report — The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment — researchers are calling this growing threat "virtual societal warfare" in an analysis of its characteristics and implications for the future.

To understand the risk of virtual societal warfare, the report's authors surveyed evidence in a range of categories to sketch out some initial contours of how these techniques might evolve in the future. **They grounded the assessment in (1) detailed research on trends in the changing character of the information environment in the United States and other advanced democracies; (2) the insights of social science research on attitudes and beliefs; and (3) developments in relevant emerging technologies that bear on the practices of hostile social manipulation and its more elaborate and dangerous cousin, virtual societal warfare.**

The authors then provide three scenarios for how social manipulation could affect advanced societies over the next decade.

RAND says the analysis suggests an initial set of characteristics that can help define the emerging challenge of virtual societal warfare, including that national security will increasingly rely on a resilient information environment and a strong social topography, and that conflict will increasingly be waged between and among networks. Although more research is urgently required, the authors conclude by pointing to several initial avenues of response to enhance democratic resilience in the face of this growing risk, including by building forms of inoculation and resilience against the worst forms of information-based social manipulation and by better understanding the workings and vulnerabilities of emerging technologies.

## Key Findings

- National security will increasingly rely on a resilient information environment and, even more fundamentally, a strong social topography. These elements likely require classic forms of information security as well as strong mediating institutions and a population continuously inoculated against the techniques of social manipulation.
- The barrier between public and private endeavors and responsibilities is blurring; national security will rely on the cooperation of private actors as much as public investments. The technologies and techniques of this form of conflict are increasingly available to a wide range of actors. Private power in this realm matches and, in some cases, exceeds public power.
- Conflict will increasingly be waged between and among networks. State actors are likely to develop such networks to avoid attribution and strengthen their virtual societal warfare capabilities against retaliation. It will be much more difficult to understand, maintain an accurate portrait of, and hit back against a shadowy global network.

## Recommendations

- Invest in research and understanding to account for the limits of our awareness of the true character of the evolving information environment and its likely directions, key causal dynamics in that evolution, how populations react to various forms of social manipulation, and what the most effective answers might be.
- Begin building forms of inoculation and resilience against the worst forms of information-based social manipulation.
- Take seriously the leading role played by social media today and the precedent-setting character of many of the information control debates playing out in that realm.
- Make investments designed to erect new, broadly trusted informational mediating institutions that can help Americans make sense of events.
- Begin working toward international norms constraining the use of virtual societal warfare.
- Better understand the workings and vulnerabilities of emerging technologies, especially artificial intelligence–driven information channels, virtual and augmented reality, and algorithmic decisionmaking.

**Table of Contents**

The Evolving Infosphere
- Chapter Three
  Insights from Social Science
- Chapter Four
  Emerging Technologies
- Chapter Five
  Future 1: The Death of Reality (2025 Scenario)
- Chapter Six
  Future 2: Silos of Belief (2024 Scenario)
- Chapter Seven
  Future 3: The Rise of the Algorithms (2026 Scenario)
- Chapter Eight
  The Emerging Risk of Virtual Societal Warfare

## EU Report: Cybercriminals Targeting Profits and Children

Source: https://i-hls.com/archives/95712

Oct 28 – The European Union's police agency has recently noted that cybercriminals are exploiting online vulnerabilities and utilizing new technology to target more profitable victims.

Europol has recently published its annual Internet Organized Crime Threat Assessment Report. In it, the agency has mentioned that digital data has become a major target for hackers and cybercriminals. The report further notes that "data security and consumer awareness are paramount for organizations".


The annually published report is mainly intended to give law enforcement and legislators the tools to analyze cybercrime trends. The cybercrimes that raise the most concern among these agencies are often fraud, theft, and child sexual exploitation.

The report also mentions how "deep fake" technologies, technologies that make it seem as though someone is saying or doing something that they aren't, raises concern for online child sexual exploitation.

International police has also raised concerns regarding online scams where "employees receive requests for money in emails purportedly sent from within their own companies," as mentioned by Courant.com. Also known as Business Email Compromise (BEC), this method of scamming companies has already cost victims over $1 billion dollars in the past year.

As a general trend, the number of cyberattacks is going down. However, criminals are now targeting larger and more profitable targets, causing major economic damage.

## Artificial Intelligence Research Needs Responsible Publication Norms

Source: http://www.homelandsecuritynewswire.com/dr20191030-artificial-intelligence-research-needs-responsible-publication-norms

Oct 30 – After nearly a year of suspense and controversy, any day now the team of artificial intelligence (AI) researchers at OpenAI will release the full and final version of GPT-2, a language model that can "generate coherent paragraphs and perform rudimentary reading comprehension, machine translation, question answering, and summarization—all without task-specific training."

Rebecca Crootof writes in *Lawfare* that when OpenAI first unveiled the program in February, it was capable of impressive feats: Given a two-sentence prompt about unicorns living in the Andes Mountains, for example, the program produced a coherent nine-paragraph news article. At the time, the technical achievement was newsworthy—but it was *how* OpenAI chose to release the new technology that really caused a firestorm.

She writes:

> *There is a prevailing norm of openness in the machine learning research community, consciously created by early giants in the field: Advances are*

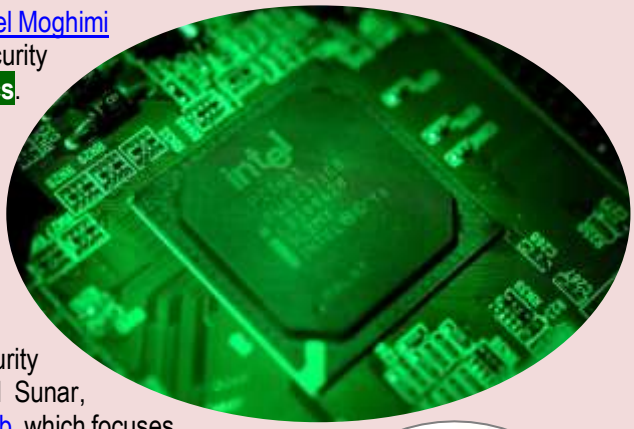
*expected to be shared, so that they can be evaluated and so that the entire field advances. However, in February, OpenAI opted for a more limited release due to concerns that the program could be used to generate misleading news articles; impersonate people online; or automate the production of abusive, fake or spam content. Accordingly, the company shared a small, 117M version along with sampling code but announced that it would not share key elements of the dataset, training code or model weights.*


*While some observers appreciated OpenAI's caution, many were disappointed. One group of commentators accused the organization of fear-mongering and exaggerating the dangers of the technology to garner attention; others suggested that the company had betrayed its core mission and should rename itself "ClosedAI." In May, OpenAI released a larger, 345M version of the model and announced that it would share 762M and 1.5B versions with limited partners who were also working on developing countermeasures to malicious uses. Again, some applauded. Others remained unimpressed.*

*Regardless of whether GPT-2 was dangerous enough to withhold, OpenAI's publication strategy spurred a much-needed interdisciplinaryconversation about principles and strategies for determining when it is appropriate to restrict access to AI research.*

## Vulnerabilities Affecting Billions of Computer Chips Discovered

Source: http://www.homelandsecuritynewswire.com/dr20191113-vulnerabilities-affecting-billions-of-computer-chips-discovered




Nov 13 – Polytechnic Institute (WPI) security researchers Berk Sunar and Daniel Moghimi led an international team of researchers that discovered serious security vulnerabilities in computer chips made by **Intel Corp. and STMicroelectronics**. The flaws affect billions of laptop, server, tablet, and desktop users around the world. The proof-of-concept attack is dubbed TPM-Fail.

The two newly found vulnerabilities, which have been addressed, would have allowed hackers to employ timing side-channel attacks to steal cryptographic keys that are supposed to remain safely inside the chips. The recovered keys could be used to compromise a computer's operating system, forge digital signatures on documents, and steal or alter encrypted information.

"If hackers had taken advantage of these flaws, the most fundamental security services inside the operating system would have been compromised," said Sunar, professor of electrical and computer engineering and leader of WPI's Vernam Lab, which focuses on applied cryptography and computer security research. "This chip is meant to be the root of trust. If a hacker gains control of that, they've got the keys to the castle."


WPI says thatthe flaws announced the other day are located in TPMs, or trusted platform modules, which are specialized, tamper-resistant chips that computer manufacturers have been deploying in nearly all laptops, smart phones, and tablets for the past ten years. Following an international security standard, TPMs are used to secure encryption keys for hardware authentication and cryptographic keys, including signature keys and smart card certificates. Pushing the security down to the hardware level offers more protection than a software-only solution and is required by some core security services.

One of the flaws the WPI team discovered is in Intel's TPM firmware, or fTPM—software that runs in the Security and Management Engine in processors the company has produced since it launched its Haswell processor microarchitecture in 2013. Haswell CPUs are used in the popular Core i3, i5, and i7 family of processors. The vulnerability is in the chip that supports trusted execution services—what should be a secure area of the processor. These small

crypto chips are the basis of the root of trust for a large portion of the computers used today. The idea is that if the TPM is secure, so is the rest of the computer.
The second flaw is in STMicroelectronics' TPM. Notably, the STMicroelectronics' vulnerability is in a chip that has received a strong industry-recognized security certification from Common Criteria—a highly acknowledged security stamp of approval based on international specifications designed to ensure technology meets high security standards preferred in industrial and government deployments.
The WPI researchers worked with Thomas Eisenbarth, a professor of IT security at the University of Lübeck, and Nadia Heninger, an associate professor of computer science and engineering at the University of California, San Diego.
Once discovered, the flaws were reported to the chip makers by the WPI researchers, who also have described the flaws, how they were discovered, and how they could have been exploited in a paper that will be presented at the 29th USENIX Security Symposium in Boston next August. It also will be presented at the Real World Crypto Symposium in New York City in January.
Researchers like Sunar and Moghimi routinely search for security flaws in software, hardware, and networks, and ethically report them to the companies so the problems can be patched before malicious hackers exploit them. No technology is bug free, so researchers help companies find and fix security flaws that could otherwise lead to massive hacking attacks, malware infections and zombie systems.
"We provided our analysis tools and results to Intel and STMicroelectronics and both companies worked with us to create a patch or make sure a security patch will be provided for the next generation of these devices," said Moghimi, a PhD candidate in WPI's electrical and computer engineering department.
Sunar and Moghimi were members of a multi-university research team that found the series of security flaws behind the Fallout and ZombieLoad attacks reported last spring, as well as another vulnerability known as Spoiler, which exploits side effects of speculative execution.
Broadly, these vulnerabilities are categorized as side-channel attacks, which hackers use to surreptitiously grab information about how a computer behaves while performing sensitive operations and then using that information to access internal data.
Using their own analysis tool, the researchers conducted black-box timing analysis of TPM devices to discover timing leakages that allow an attacker to apply lattice techniques to recover 256-bit private keys for and ECSchnorr cryptography signatures. The leakages make the TPMs vulnerable to remote attacks that reveal cryptographic keys and make applications that use them less secure than they would be without the TPM.

**Flaw in Intel fTPM**

One of the security flaws Intel patched today is in a cryptographic library—in the fTPM set inside the Intel Management Engine processor. With this vulnerability, researchers used the timing leakage to recover the signature key in less than two minutes. Intel is patching the security flaw with an update to the library.
Intel's fTPM is a widely used TPM product that runs in a dedicated microprocessor for carrying out cryptographic operations, like making sure data has not been maliciously altered, ensuring data remains confidential, and proving the identity of both the sender and recipient of the data. The microprocessor is embedded with multiple physical security measures, designed to make it tamper resistant.
WPI's Moghimi explained that if hackers gained access to the fTPM, they could forge digital signatures, enabling them to alter, delete, or steal information.

**STMicroelectronics Flaw**

The research team discovered a flaw in the STMicroelectronics' TPM, which is based on the company's popular ST33 chip, an embedded security platform used in many SIM modules, using integrated circuits designed to securely store authentication information. The chip maker announced earlier this year that more than 1 billion ST33 chips have been sold.
The vulnerability in STMicroelectronics' TPM basically leaks the signature key, which should remain safely inside the hardware. It is designed to enhance the system's security. With the key, a hacker could access, steal or alter encrypted electronic documents. Using the flaw in the STMicroelectronics chip, researchers extracted the private ECDSA key from the hardware after less than one and a half hours of data collection.
"STMicroelectronics developed a new ST33 chip with vulnerability countermeasures in the firmware," said Moghimi. "We verified the new chip. It is not vulnerable to TPM-Fail."
The vulnerable chip has received a CC4+ rating from Common Criteria, which ranks security levels from one (lowest) to seven (highest).
"The certification has failed," said Sunar. "Such certifications are intended to ensure protection against a wide range of attacks, including physical and side-channel attacks

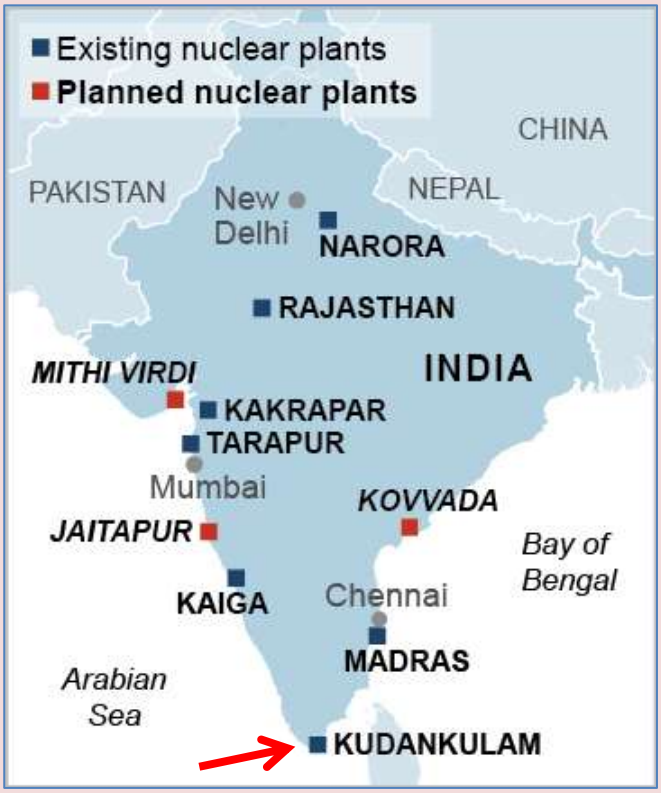
against its cryptographic capabilities. This clearly underlines the need to reevaluate the CC process."
Intel, based in Santa Clara, Calif., has been the world's largest computer chip maker by revenue since 1992. STMicroelectronics, Europe's largest semiconductor chip maker based on revenue, is based in Geneva, Switzerland.

# Lessons from the cyberattack on India's largest nuclear power plant

**By Alexander Campbell and Vickram Singh**
Source: https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant

Nov 14 – Indian officials acknowledged on October 30th that a cyberattack occurred at the country's **Kudankulam nuclear power plant**. An Indian private cybersecurity researcher had tweeted about the breach three days earlier, prompting Indian

authorities to initially deny that it had occurred before admitting that the intrusion had been discovered in early September and that efforts were underway to respond to it.
According to last Monday's *Washington Post*, **Kudankulam is India's biggest nuclear power plant,** "equipped with two Russian-designed and supplied VVER pressurized water reactors with a capacity of 1,000 megawatts each. Both reactor units feed India's southern power grid. The plant is adding four more reactor units of the same capacity, making the Kudankulam Nuclear Power Plant one of the largest collaborations between India and Russia."
While reactor operations at Kudankulam were reportedly unaffected, this incident should serve as yet another wake-up call that the nuclear power industry needs to take cybersecurity more seriously. There are worrying indications that it currently does not: A 2015 report by the British think tank Chatham House found pervasive shortcomings in the nuclear power industry's approach to cybersecurity, from regulation to training to user behavior. In general, nuclear power plant operators have failed to broaden their cultures of safety and security to include an awareness of cyberthreats. (And by cultures of safety and security, those in the field—such as the Fissile Materials Working Group—refer to a broad, all-embracing approach towards nuclear security, that takes into account the human factor and encompasses programs on personnel reliability and training, illicit trafficking interception, customs and border security, export control, and IT security, to name just a few items. The Hague Communiqué of 2014 listed nuclear security culture as the first of its three pillars of nuclear security, the other two being physical protection and materials accounting.)
This laxness might be understandable if last week's incident were the first of its kind. Instead, there have been over 20 known cyber incidents at nuclear facilities since 1990. This number includes relatively minor items such as accidents from software bugs and inadequately tested updates along with deliberate intrusions, but it demonstrates that the nuclear sector is not somehow immune to cyber-related threats. Furthermore, as the digitalization of nuclear reactor instrumentation and control systems increases, so does the potential for malicious and accidental cyber incidents alike to cause harm.




This record should also disprove the old myth, unfortunately repeated in Kudankulam officials' remarks, that so-called air-gapping effectively secures operational networks at plants. Air-gapping refers to separating the plant's internet-connected business networks from the

operational networks that control plant processes; doing so is intended to prevent malware from more easily infected business networks from affecting industrial control systems. The intrusion at Kudankulam so far seems limited to the plant's business networks, but air gaps have failed at the Davis-Besse nuclear power plant in Ohio in 2003 and even classified US military systems in 2008. The same report from Chatham House found ample sector-wide evidence of employee behavior that would circumvent air gaps, like charging personal phones via reactor control room USB slots and installing remote access tools for contractors.

**The consequences of a cyber-based intrusion at a nuclear power plant could range from loss of confidential employee or business information to potentially causing a reactor shutdown or physical damage.** The industry must realize that cyberattacks can be the main event, rather than simply a means to enable more traditionally imagined threats like physical intrusions. And regardless of the consequences of a given incident, public statements like those from Indian authorities last week that refuse to even admit the possibility of cyberattack will undermine public trust—an existential resource for many nuclear power programs.

Despite speculation about potential North Korean responsibility or escalation with Pakistan, revealing the culprits and motives associated with the Kudankulam attack matters less for the nuclear power industry than fixing the systemic lapses that enabled it in the first place. The good news is that solutions abound: The Nuclear Regulatory Commission has issued guidance for US operators on improving workforce development and performance assessment for cybersecurity at nuclear power plants. And the National Nuclear Security Administration includes cybersecurity in their security assessments at US and international facilities, along with technical exchanges and training programs. It also developed a course on cybersecurity for nuclear power plant operators in partnership with the International Atomic Energy Agency—which has published its own technical guides on computer security, and recently held its first cybersecurity course for nuclear power plant operators.

Countries need not depend solely on international organizations or other governments for this expertise. Public-private partnerships like the World Institute for Nuclear Security and World Association of Nuclear Operators also share information about best practices and can serve as a knowledge conduit for states where nuclear power implicates national security concerns.

The challenge now is integrating this knowledge into the workforce and maintaining it over time. But the institutionalization of cybersecurity does not present an insurmountable barrier.

One item to note, however, is that the problem's scale and complexity is only likely to grow as more states join the nuclear power club. And even with years of experience, no country is immune from succumbing to cyberattack: Last week's incident occurred in a country whose nuclear power program dates back to the 1950s, and previous cyberattacks have struck nuclear facilities in countries with similarly long-established nuclear power programs, including Japan, France, and the United States. That they have still fallen victim to breaches bodes ill for prospective newcomers like Jordan, whose national Computer Emergency Response Team is only two years old. One can expect that nuclear newcomers with less indigenous cybersecurity expertise will need more help from international partners, and will face a steeper uphill climb towards maintaining that workforce.

If there is a silver lining to the recent cyberattack, it is that India now has an opportunity to become a leader in nuclear cybersecurity. India has established the Global Centre for Nuclear Energy Partnership as a forum for bilateral and multilateral cooperation in nuclear security that could be widened to include cybersecurity.

The problem of cybersecurity is not new to the nuclear power industry, and it does not require solutions radically different from those already in place in fields such as finance and commercial aviation. The nuclear industry's history of safety and security culture, and the body of research on sector-specific cybersecurity recommendations, together can offer a path toward a nuclear power industry that better defends itself against cyber threats. The avenues for fostering cooperation and sharing best practices have been established, as has the need for workforce development.

But last week's example of a well-established nuclear power program responding to a breach with denial, obfuscation, and shopworn talk of so-called "air-gaps" demonstrates how dangerously little progress the industry has made to date.

***Alexander Campbell*** *is a research assistant at the Center for Global Security Research at Lawrence Livermore National Laboratory, where he studies offensive cyber strategies and internet governance. He holds a master's degree in international affairs and a bachelor's degree in political science from Columbia University.*

***Vickram Singh*** *is a postdoctoral researcher at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on international nuclear energy development and its impacts on nonproliferation. He holds a doctorate in materials science and engineering from the University of Nevada at Reno, and a bachelor's degree in chemical engineering from the University of Tennessee at Knoxville.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

# DRONE NEWS

# Rogue drones to be targeted by new hi-tech 'detect and destroy' unit set up by Home Office

Source: https://www.telegraph.co.uk/news/2019/10/20/rogue-drones-targeted-new-hi-tech-detect-destroy-unit-set-home/

Oct 20 – Rogue drones will be brought down by "detect and destroy" technology under plans for a new national counter-drone force to prevent Gatwick-style disruption, ministers have announced.

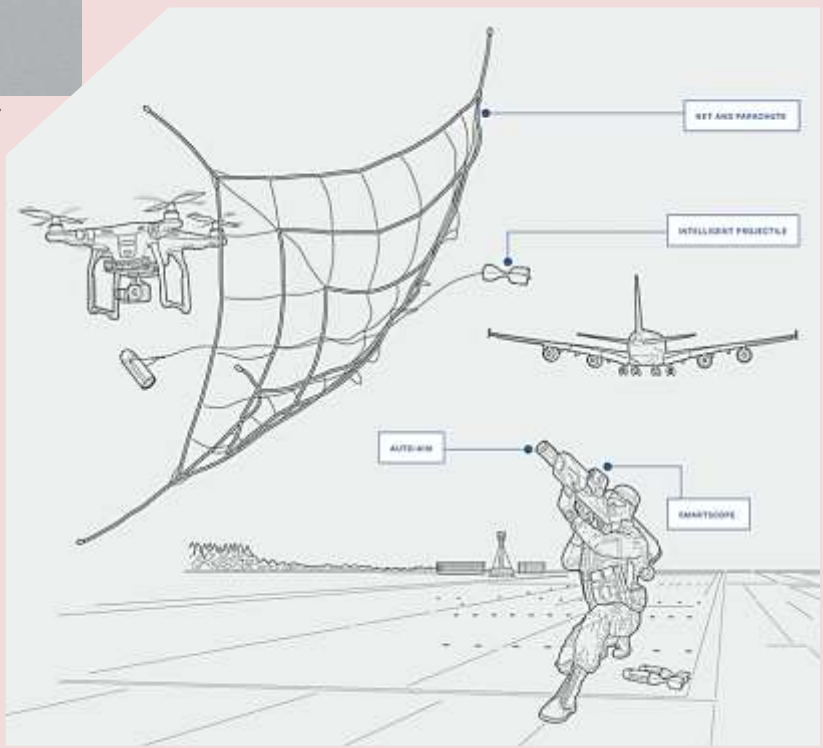
The new mobile special unit, to be set up by the Home Office, will be available to any police force or law enforcement agency in the UK to counter potential drone threats at major events or malicious attacks such as the chaos at Gatwick airport last Christmas.

The unit is expected to have military-grade cameras, radar and radio frequency scanners to detect rogue drones, similar to those deployed by the Army at Gatwick.

To bring them down, there is electronic jamming equipment and shoulder-launched bazookas that fire projectiles which deploy a net as they near a drone, ensnare it and float it to the ground with a parachute.

**A bazooka with a 100 metre range has been tested by police at Heathrow while a more powerful version capable of reaching 300 metres is being developed.**

The planned unit is part of a three-year "counter-drone" strategy which includes a new international standard for Unmanned Aerial Vehicles (UAVs) where all would be fitted with "geofencing." This uses their GPS to stop them flying over sensitive sites like power plants, airports or prisons.



It follows an agreement last month by the Five Eyes group of nations - the UK, US, Canada, Australia and New Zealand - to "identify what more could be done at the manufacturing stage to mitigate drone risk by design."

The Telegraph understands that aviation watchdogs led by the US Federal Aviation Administration (FAA) want all drones to have an electronic "licence plate" so they can be detected in the sky and their ownership immediately established.

**Planned new laws will give police more powers to search premises for potential rogue drone operators and issue £100 penalty notices for minor drone violations.**

**From next month all owners of drones weighing more than 250 grammes will be required by law to register their device with the Civil Aviation Authority (CAA) and take an online safety test. Anyone who fails to do so faces fines of up to £1,000.**

Brandon Lewis, the Security Minister, said: "This Government is proud of the UK's burgeoning drone industry and we will do all that we can to ensure that the UK firmly establishes itself as a world leader in this industry.

"But to ensure the drone industry can thrive in this country we must be able to crack down effectively on those who would use drones to cause harm or disruption.

"There is no silver bullet to help protect our infrastructure and our citizens from malicious or careless drone use. That's why this strategy outlines a broad range of work to ensure we can effectively tackle the threat."

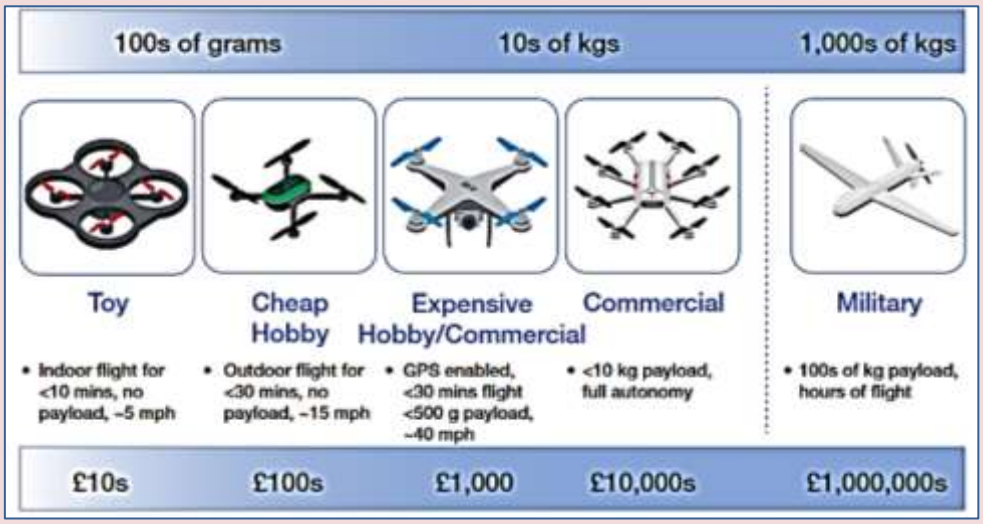
A new Government-industry group is to be established to research and test the latest counter-drone equipment for use by the new anti-drone force and by police forces, most of which have their own drone technology to help map accidents, search and rescue.
New national police guidance will be drawn to help forces tackle malicious drone incidents and a new national standard will be established for police recording of illegal drone activity to build a picture of the drone threat.
There were 168 police recorded drone incidents in England and Wales in 2018, and 165 drones were recovered at prisons in 2016 and 2017.
**The use of drones has grown rapidly with more than 5,000 commercial operators currently registered in the UK. The industry is expected to contribute an extra £42 billion to the UK economy by 2030, with more than 76,000 commercial and public sector drones expected to be in use by this date**.

**EDITOR'S COMMENT:** The juice is in the last paragraph of the article: 42 billion UKP by 2030. Hope that this money will be sufficient to compensate the victims of a future airplane accident or terrorist attack using a commercial UAV

## British Government Launches Counter-Drone Unit and Strategy

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/british-government-launches-counter-drone-unit-and-strategy/

Oct 23 – The U.K. government announced on October 21 that it will develop a new mobile counter-drone unit to be deployed to drone related incidents and major events across the country, as part of the new "Counter-Drone" Strategy.
The strategy includes plans to drive forward the establishment of international design standards for manufacturers to enable safety features to be designed in from the start and make drones safe to use. Many commercially-available drones already include geo-fencing capabilities – software that can restrict a drone from flying in certain areas, such as airports. The government is engaging directly with drone manufacturers and industry on how these capabilities can be improved.




The new mobile counter-drone unit will contain detection and disruption equipment, which can be deployed by police and other emergency responders to protect major events and rapidly respond to drone incidents across the U.K.
Security Minister Brandon Lewis said there is no "silver bullet" to help protect infrastructure and citizens from malicious or careless drone use. "That's why this strategy outlines a broad range of work to ensure we can effectively tackle the threat."
The strategy also includes:

- the Air Traffic Management and Unmanned Aircraft Bill, announced in the Queen's Speech, which will give police increased powers to tackle illegal drone use
- a new national standard for police recording of illegal drone activity to help build a picture of the drone threat
- national guidance for police to assist them during malicious drone incidents
- ongoing work with industry to research and test the latest counter drone equipment
- a government communications campaign to educate the general public and continue to encourage safe drone use

Over the next three years, the government will also work with partners to compile a catalogue of approved counter-drone technology to assure police and the owners and operators of critical national infrastructure sites that they are investing in the most effective and appropriate technology. The government also plans to work with international partners to promote the importance of common international standards for counter-drone systems.
The use of unmanned aircraft has grown significantly in recent years and the industry is expected to contribute an extra £42 billion to the UK economy by 2030, with more than 76,000 commercial and public sector drones expected to be in use by this date.

However, this also increases the risks of malicious use. **Latest statistics show there were 168 police recorded drone incidents in England and Wales in 2018, and 165 drones were recovered at prisons in 2016 and 2017.**
Earlier this year it was announced that from November 30 2019, every operator of a drone weighing more than 250g will need to register with the Civil Aviation Authority and all remote pilots will have to have passed an online competency test. The online system will go live on November 5.
Anyone responsible for a drone or unmanned aircraft (including model aircraft) weighing between 250g and 20kg and used outdoors will need to register as an operator to obtain an operator ID. Drones or model aircraft must be labelled with the operator ID. In addition, anyone flying a drone or unmanned aircraft weighing between 250g and 20kg will need to take and pass an online education package. This is free and renewable every three years.
Protest groups including Extinction Rebellion have said they will use drones to disrupt flight operations at British airports. In December 2018, hundreds of flights were cancelled at London-Gatwick Airport following drone sightings close to the runway.
The strategy however focuses on the highest security risk areas including the use of drones to facilitate terrorist attacks, commit serious and organized crime, disrupt critical national infrastructure, and their potential use by hostile state actors.

## Illegal drones ground water-dropping helicopters at critical moment in Maria fire battle

Source: https://www.latimes.com/california/story/2019-11-01/maria-fire-drone-hinders-firefighting-efforts-as-blaze-doubles-in-size-overnight

Nov 02 – **As flames rapidly spread along a hillside in Santa Paula early Friday morning, firefighters were faced with a perilous dilemma: ground night-flying helicopters working to contain the growing fire or risk an aerial collision with a thrill-seeking drone.**

A Ventura County Fire Department helicopter pilot radioed in at 3:19 a.m. that a drone had been spotted flying above the flames, apparently trying to take a photograph or video of the scene below. Air operations were immediately stopped for at least 45 minutes until the sky was clear.

But at 4:05 a.m., another drone sighting occurred.

The aerial fight against the wildfire was upended for another hour while at least two helicopters with night-flying capabilities that had been deployed to help contain the Maria fire were grounded. Meanwhile, the blaze that broke out atop South Mountain, just south of Santa Paula, shortly after 6 p.m. Thursday marched toward the small agricultural towns of Somis and Saticoy.

The interruption of the aerial firefighting underscores growing concerns about how drones can bring added dangers to pilots battling major fires.

**According to the National Interagency Fire Center, aerial firefighting efforts have been shut down at least nine times this year because of drone use, and at least 20 drone incursions have hindered firefighting capabilities nationwide from January through October. A report shared with The Times showed that of those 20 incursions, five were in California**.
While the unmanned aerial vehicles are small, drones can wreak incredible havoc. A collision with a wing, engine or any part of a larger aircraft can cause severe damage.
**"A bird collision with a plane can cause a plane to go down," said Jessica Gardetto, a spokesperson for the National Interagency Fire Center. "These are hard plastic items."**
Firefighting tactics from the sky aren't guaranteed to stop a blaze, but they can significantly slow the spread. And a fire can grow exponentially over the course of 20 minutes, let alone one or two hours, Gardetto said.
The Maria fire spread to nearly 10,000 acres, and it's far from clear whether the interruption in water drops made an impact. The fire shifted direction Friday and raced toward Santa Paula, causing more evacuations. As of Saturday morning, it was 20% contained.

"I don't know if it would have made a difference, but it sure wouldn't have been a bad thing to keep them flying," said Scott McLean, a deputy chief with the California Department of Forestry and Fire Protection.

**Firefighting aircraft such as water-dropping helicopters and super scooper planes typically dip to 150-200 feet off the ground when dumping their loads**, he added.

In the event of a drone collision, there's only so much room an aircraft has to safely land, potentially impacting those on the ground as well.

"It stifles our mitigation," McLean said.

Drones have been a cause of concern for California firefighters for several years. In 2015, the Legislature passed a bill that allowed firefighters to destroy drones that impeded their efforts to battle fires and imposed and created penalties for drone operators who interfered with firefighters.

That same year, the state launched a public service campaign with a television commercial titled "If you fly, we can't," in which Cal Fire pilots talk about the danger of sharing the skies with hobby drones. Officials have expressed frustration at not being able to catch more of those who operate the drones, speculating some are hobbyists who want to post dramatic videos on social media or sell them to TV stations.

**The huge 2015 Lake fire in the San Bernardino Mountains grew after a drone interrupted plans to deploy an air tanker water drop.**

Beyond wildfires, drones have been known to interfere with airport traffic. In January, London's Heathrow Airport had to halt departing flights after a drone sighting. The incident occurred just three weeks after multiple drone sightings ignited chaos at the nearby Gatwick Airport.

Drones have proved useful in combating fires, but only when in the right hands. In 2017, the Los Angeles Fire Department used the unmanned aircraft for the first time while combating the Skirball fire in Bel-Air.

"They provide real-time situational awareness from a bird's-eye perspective to the incident commander so they can see what's going on at their emergency and then change their tactics accordingly to mitigate the hazards," Capt. Erik Scott, an LAFD spokesman, said at the time.

But the Federal Aviation Administration prohibits recreational drone users from flying near emergencies and "any type of accident response, law enforcement activities, firefighting or hurricane recovery efforts."

In Ventura County on Friday, the water dropping aircraft pounded the Maria fire as anxious residents fled their homes.

In one Santa Paula neighborhood, a man stood on his roof spraying his home with water from a garden hose as police and fire officials urged residents to evacuate. Others covered their mouths and noses as they fled to avoid thick smoke that choked the neighborhood.

"They're on top of this," said resident Elizabeth Sylvester. "They're doing the best they can. I'm scared. This isn't the first time we've been through this."

Residents in the Anacapa Mobile Park raced to fill their cars with as much as they could fit as flames licked the hillside nearby. People carried suitcases, garbage bags and boxes filled with blankets, clothes and food as firefighters and police hurried from door to door, telling people to evacuate.

Winneke Knuppel, who has lived in the mobile home park for 22 years, took down a slew of wind chimes on her property as she kept an eye out for her cat, Geronimo.

"I can't leave until my cat comes back," she said. "I can't find him. I'm really anxious. I'm staying as long as I can."

As the gusts began to pick up Friday morning, dozens of fire vehicles staged around homes along the rolling hillsides of West La Loma Avenue prepared to protect the properties from possible flare-ups. Agricultural employees wearing masks worked nearby in citrus groves.

Michael Minjares, who works in the agricultural industry, said he stopped his car to see how close the fire was to thousands of avocado trees near Briggs and Pinkerton roads early Friday. He worried the winds and fire will decimate next year's crop.

"That's a lot of avocados. That's a concern," he said. "You have crops in the hills on fire. Crop insurance is important."

Minjares said the area on fire now is the only spot not torched by the Thomas fire.

"It's makes you leery when thinking about it," he said as three planes and two helicopters circled above.

**EDITOR'S COMMENT:** A new threat has been added in the long list of threats: "Arson – wildfire – commercial drones". In the middle of a chaotic incident who will think to deploy anti-drom measures (of course, if they are available!).

# The United States should drop its opposition to a killer robot treaty

**By Lisa A. Bergstrom**

Source: https://thebulletin.org/2019/11/the-united-states-should-drop-its-opposition-to-a-killer-robot-treaty/


Demonstrators standing beside the "Broken Chair" statue in Geneva, a symbol of the damage done by landmines and cluster munitions, called on countries to ban autonomous weapons. Credit: Clare Conboy/Campaign to Stop Killer Robots

Nov 07 – Landmines, cluster munitions, incendiary weapons, blinding lasers, exploding bullets, and much more: The list of weapons banned or regulated by international humanitarian law has grown steadily over the past 150 years. If an international campaign of civil society organizations—supported by about two dozen countries and growing—is successful, there could soon be another to add: autonomous weapons.

Given the unprecedented risks autonomous weapons pose, and the strength of the movement against them, a new treaty regulating such weapons is both desirable and viable. Whether that treaty is effective, however, will depend primarily on whether the United States decides to engage in negotiating it and convinces other militarily important countries to do the same.

**Not yet deployed**

Autonomous weapons, or "killer robots," as their opponents and the media often call them, are weapons that select and attack targets without direct human control. Think of a drone scanning the battlefield and using artificial intelligence to identify and fire upon a suspected enemy combatant, without waiting for a human operator to approve the strike.

The exact definition of a lethal autonomous weapon is hotly contested. While critics also express concern about non-lethal, anti-materiel, or semi-autonomous weapons, for now international talks have focused only on fully autonomous, lethal anti-personnel weapons. Under this broad definition, no military has deployed such weapons yet, but the technology to do so already exists and is developing rapidly.

To address the humanitarian risks of autonomous weapons, about 100 countries have been discussing the possibility of negotiating a new treaty within the Convention on Certain Conventional Weapons (CCW), a little-appreciated, United Nations-affiliated forum for

regulating inhumane weapons. Since 2014, the slow-moving CCW has agreed to renew talks on the issue without being able to reach the consensus the convention requires to actually start negotiating a treaty.

**Too soon to regulate?**

One of the driving forces behind these discussions is an international movement of groups and activists opposed to the unrestricted use of autonomous weapons. Chief among these are the ubiquitous International Committee of the Red Cross and the more militant Campaign to Stop Killer Robots, a coalition of nongovernmental organizations, including Human Rights Watch, that have been active in earlier campaigns to ban landmines and cluster munitions. So far, the campaign has managed to convince about two dozen countries—including Austria, Brazil, and Mexico—to support a preemptive ban on the development and deployment of lethal autonomous weapons. Several more countries, like Germany and France, support a political declaration, but not a legally binding treaty.

The Campaign to Stop Killer Robots and other critics charge that autonomous weapons are immoral and dangerous because they lack the human traits (like mercy) needed for moral decision making, as well as the ability to distinguish between civilians and combatants and to judge the proportionate use of force, two key principles of international humanitarian law. The critics argue convincingly that if the development of autonomous weapons is left unregulated it could lead to a destabilizing arms race. This threat would be made worse by the difficulty in determining who is responsible for the actions of an autonomous weapon, meaning a small incident could spark an international crisis. As with drones, autonomous weapons could make it easier for countries to start unnecessary wars by keeping soldiers off the battlefield, offering the illusion of "risk-free" military intervention but providing no protections for civilians.

The United States, Russia, Israel, and a few other countries oppose either a new treaty or a political declaration. These countries are investing heavily in robots and artificial intelligence. They argue it is too soon to know how autonomous weapons might be used in the future and therefore too soon to know how best to regulate them, if at all. The United States has stated that autonomous weapons could even improve compliance with international law by being better than humans at identifying civilians and judging how to use force proportionately.

**Prospects for a standalone treaty**

Unhappy with the lack of progress in the CCW, the Campaign to Stop Killer Robots is increasingly urging countries to consider bypassing the convention entirely to negotiate a separate treaty, stating, "If the CCW cannot produce a credible outcome [at its annual meeting on November 15], alternative pathways must be pursued to avoid a future of

autonomous warfare and violence." Unfortunately, such a decision, while understandable and feasible, would be unlikely to produce a truly effective treaty.

One might ask what chance nongovernmental organizations like Human Rights Watch have for achieving a standalone treaty against the opposition of some of the world's most powerful militaries. Plenty, actually.

By the 1990s, the widespread and indiscriminate use of landmines had become a humanitarian disaster, and the members of the CCW tried to solve the crisis by strengthening an existing CCW treaty regulating this weapon. Frustrated by the perceived weakness of the CCW agreement, the International Campaign to Ban Landmines pushed for a new treaty, under the auspices of the Canadian government, that would ban all landmines without requiring the burdensome consensus decision-making of the CCW. The resulting Mine Ban Treaty mostly ended the large-scale use of landmines outside of a few conflict zones and earned the campaign a Nobel Peace Prize.

In 2008, a similar coalition of nongovernmental organizations repeated this feat, successfully pushing for a Convention on Cluster Munitions outlawing this once-ubiquitous weapon, after years of talks in the CCW had produced only modest results. Even though the United States, Russia, and other major military powers have not joined either treaty, the treaties have created a powerful stigma against landmines and cluster munitions.

Given this history of success, it is tempting to conclude that a strong, standalone treaty is the best way to deal with the threat posed by autonomous weapons, despite the fact that countries like the United States and Russia would almost certainly refuse to join. Autonomous weapons, however, are not landmines or cluster munitions. Landmines and cluster munitions were used around the world for decades in conflicts large and small, in many cases causing great civilian harm. Treaties banning these weapons have value even when the United States, Russia, China, and other major military powers do not participate. In contrast, autonomous weapons are a developing technology likely to be used by only the most advanced militaries for some time. A treaty that excludes almost all the countries with the interest and ability to deploy autonomous weapons would have comparatively little value either as arms control or as a humanitarian norm builder.

At a time when even the taboos against chemical and nuclear weapons appear to be waning, it is hard to imagine that Russia, for example, would consider its autonomous weapons program constrained by the perceived stigma created by a treaty it had no hand in making. A more modest treaty, negotiated in the CCW with the agreement of the world's major military powers, offers the best chance of providing meaningful restrictions on autonomous weapons in the foreseeable future.

**A US policy solution**

What could the United States do to achieve such a treaty? The CCW treaty on blinding laser weapons may offer a guide. While blinding lasers and autonomous weapons differ in terms of their military utility and humanitarian threat, both weapons became the subject of campaigns to ban them before they were ever deployed. Opponents of autonomous weapons point to this analogy as proof that a weapon can be banned preemptively, but it also shows how the United States can use a national policy to help reach a difficult international compromise. The United States had long resisted any attempts to regulate the use of lasers to cause blindness, worried that any such regulation could interfere with unrelated military uses of lasers. Then in 1995, as CCW negotiations were underway, the Defense Department adopted a limited national ban on blinding laser weapons. By using this new policy as a basis for negotiations, the United States was able to broker an agreement in the CCW that satisfied countries that wanted a broader ban, countries that opposed any ban, and the requirements of the US military. In doing so, the United States was able to make sure the treaty did not restrict other, less controversial uses of lasers—a concern that is highly relevant to autonomous weapons as well.

In fact, the United States already has a national policy that could serve as the basis for a new CCW treaty. In 2012, the Department of Defense issued a directive requiring "appropriate levels of human judgment over the use of force," thereby becoming the first country to publicly adopt a national policy on autonomous weapons. The Pentagon even tasked a committee of ethicists, scientists, and other experts with creating an ethical framework for artificial intelligence—their just-released report endorses strong principles of responsibility, traceability, and more .

Clearly, the US government shares some of the activists' concerns over the ethics of autonomous weapons and is comfortable with some limitations on their use. If the United States can strengthen its existing national restriction on autonomous weapons, it would be well placed to negotiate a new treaty in the CCW. While there is no guarantee that Russia and other countries would agree to start negotiations, US support would increase the pressure on them considerably.

"Killer robots" will soon no longer be confined to the realm of science fiction. To address the new risks autonomous weapons will bring, the world needs a new and effective treaty regulating them. The best chance to achieve such a treaty is for the United States to drop its opposition and take an active role in negotiating a new agreement in the existing forum for regulating inhumane weapons.

***Lisa A. Bergstrom** is a technology and security specialist in Berkeley, California, with interests in nuclear proliferation, conventional weapons policy, and Russian*

*studies. She received her Master of Arts in Security Studies from the Edmund A. Walsh School of Foreign Service at Georgetown University, where she concentrated in technology and security.*

**EDITOR'S COMMENT:** (1) What is the difference between a robot with a machine gun and a Humvee with a machine gun? (2) Is this fear directed to anthropoid armed robots supported by AI only? Do they fear that one day these devises will take over the planet – like "*Hardware", "Killerbots", "Terminator", "Kill Command"* and alike? (3) In the meantime, I would prefer a "Drone Treaty" that is already a visible threat – especially when terrorists will start using them.

# Lawmakers Want to Ban Unauthorized Drones from Flying Over Stadium Concerts

Source: https://www.nextgov.com/emerging-tech/2019/11/lawmakers-want-ban-unauthorized-drones-flying-over-stadium-concerts/161254/

Nov 12 – Lawmakers recently introduced bipartisan legislation to strengthen security in the skies above stadiums as more and more drones gain clearance to operate across America's airspace.

The Stadiums Operating under New Guidance, or SONG Act, produced by Sens. Marsha Blackburn, R-Tenn., Ed Markey, D-Mass., and Lamar Alexander, R-Tenn., authorizes the Federal Aviation Administration to issue temporary flight restrictions over concerts and other events that take place at stadiums across the nation.

"When patrons go to a stadium, they are protected by dozens of law enforcement on the ground," Blackburn told *Nextgov* Tuesday. "Given the way technology now enables drones to roam the skies, it is necessary to consider how we can protect that airspace."

Federal support and technological advancements have accelerated drone use over the last half-decade and in-sky congestion is only anticipated to get worse. Earlier this year, Google's Wing Aviation received federal approval to operate as a drone commerce airline and Amazon got the OK to test its own. The Postal Service also announced it's exploring introducing drones into its vehicle fleet and package delivery giant UPS received approval to operate the first national drone airline system that's unlimited in size and scope. But while it's an exciting time for commercial and personal drone use to blossom, it's also ushered in a new paradigm of airspace dangers and challenges. Alleged drone sightings near the runways of London's Gatwick Airport disrupted the flights of about 140,000 passengers and closed the airport for 33 hours last December.

Blackburn shared a copy of the new one-page bill with *Nextgov* and explained that although it does not implement any new restrictions, it offers the FAA greater authority to issue temporary flight restrictions, or TFRs. Currently, the statute that enables FAA to grant TFRs is limited to sporting events in stadiums, so the temporary restrictions are routinely issued for NFL and MLB games, as well as NASCAR events and NCAA Division One football games.

"When a music concert is held in the very same stadium, often with the same size or a bigger crowd, the air space cannot be secured by a TFR," Blackburn said.

The SONG Act aims to correct that limitation and enable FAA to issue TFRs for entertainment events outside of sports that occur at these same venues. Policy experts worked with the FAA to carefully craft the legislation and Blackburn added that she was inspired to propose the bill after concerns were raised directly by her constituents.

"We have heard from tour companies and entertainment industry managers in Tennessee that were denied TFRs despite working closely with the FAA," Blackburn said. "In one instance, a music organizer tracked down three illegal drones flying directly over crowds."

The ultimate hope, she said, is to enhance public safety. It's a target that likely resonates with drone industry insiders who are also working to advance the space.

Jeff Thompson, the CEO of Red Cat, a provider that offers distributed data storage, analytics and services to boost drone performance and make the systems more trackable and accountable, noted that while thousands of airplanes make up the United States' commercial fleet, it's anticipated that there'll eventually be millions of drones occupying that same airspace.

"It's going to be 10x the number of drones in the air than traditional airlines," he said.

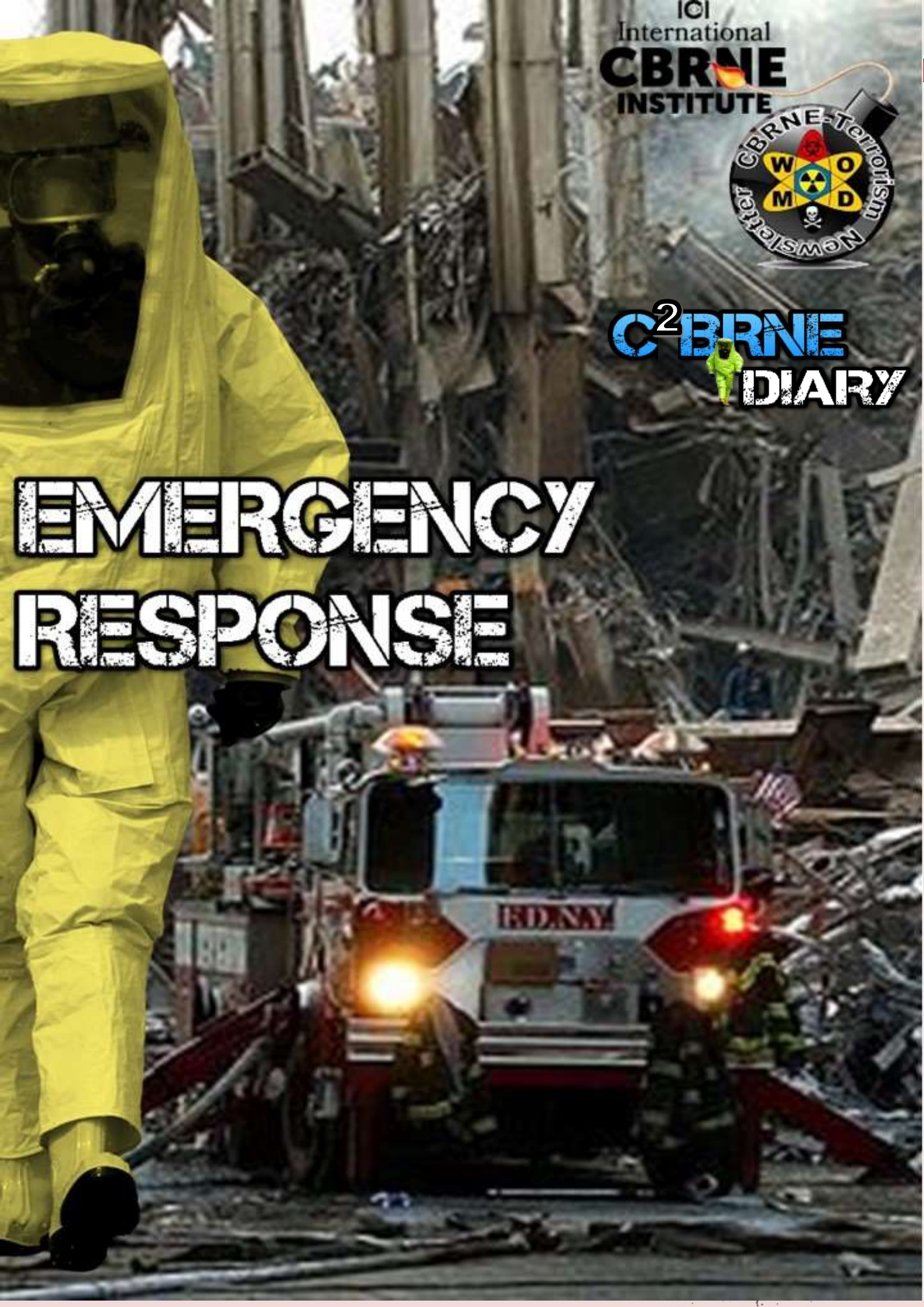
On top of commercial entities like UPS and Google, hobbyists and racing competitors are flying drones, and other industrial entities like agriculture-based and gas and oil companies are also operating large fleets. Thompson said the majority of those who want to responsibly employ drones welcome federal support that will enable them to fly safely and properly.

"If we can get more and more guides, goal posts and regulations, so that we know what we are allowed to do, we can make the technology work really well—and make it more accountable, reliable and safe," he said.

A companion measure was also introduced to the House of Representatives in July.

***Brandi Vincent*** *reports on the federal government's use of and policies for emerging technologies—including but not limited to supercomputing, artificial intelligence, biometrics, and the internet of things. Before joining Nextgov, Brandi*

*helped create news for millennials at Snapchat and mixed media at NBC News. She grew up in south Louisiana and received a master's in journalism from the University of Maryland.*


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

# Motorola Launches New Touchscreen Radio and Virtual Assistant for Public Safety

Source: https://www.hstoday.us/subject-matter-areas/law-enforcement-and-public-safety/motorola-launches-new-touchscreen-radio-and-virtual-assistant-for-public-safety/

Oct 24 – Motorola Solutions has launched **APX NEXT™,** its next-generation mission-critical Project 25 (P25) public safety radio with LTE for enhanced communications and data-centric application services. The company also announced ViQi™, a public safety virtual assistant that provides vital information to first responders in the field and allows users to operate APX NEXT via voice control.


APX NEXT is the newest mission-critical P25 radio offering in Motorola Solutions' purpose-built APX portfolio. It is FirstNet Ready™ and comes with embedded LTE connectivity enabled by the FirstNet communications platform to deliver voice and data to first responders in the field.

APX NEXT was created after more than 2,000 hours of extensive field research and testing with numerous law enforcement agencies, and is Motorola Solutions' first APX radio to feature a touchscreen with a user interface designed specifically for public safety. **The touchscreen can be used in the rain and when wearing gloves.** It offers one-touch access to radio controls, large touch targets and an optimized user interface designed for fast navigation.

ViQi voice control enables users to quickly manage radio controls through intuitive voice commands. Iti is an application service available on APX NEXT and will be integrated into other solutions as the company continues to research, and collaborate with users, on new ways to streamline officer workflows and guide better decisions through artificial intelligence and machine learning.

ViQi currently allows officers to discreetly retrieve critical information from remote databases through simple voice queries, including license plate numbers, driver's license information, and vehicle identification numbers. Motorola Solutions is working on future iterations of ViQi, such as calling for vehicle assistance, taking statements and foreign language speech translation.

# U.S. Border Patrol Agents Leverage Emerging S&T Tech to Ensure the Security of Our Nation's Borders

Source: https://www.dhs.gov/science-and-technology/news/2019/11/05/snapshot-us-border-patrol-agents-leverage-emerging-st-tech

Nov 05 – Smugglers, human traffickers, undocumented immigrants and potential terrorists attempt to illegally cross our borders and enter the United States on a regular basis. The United States Border Patrol (USBP) is tasked with pursuing and apprehending these individuals before they enter the country. However, tracking groups and individuals both day and night over complex terrain can be a difficult and potentially dangerous task. Successfully apprehending individuals who do not want to be found can be extremely challenging, even with proper training and extensive experience.

To help address this ongoing challenge and ensure USBP agents can perform their job both safely and effectively, the Department of Homeland Security (DHS) Science and Technology Directorate recently collaborated with the USBP and the Federal Law Enforcement Training Centers (FLETC) to deliver a multi-part solution by implementing innovative tools and capabilities that enable USBP agents to leverage the knowledge, skills, and abilities of expert trackers (professionals trained to detect, track, follow and apprehend potential adversaries) and use emerging technologies to maximize their tracking performance.

USBP agents are a crucial part of the Homeland Security Enterprise, which consists of a network of hardware, software and highly-trained individuals that work together to ensure national security.


**As part of DHS's efforts to continue improving this network of capabilities, and in turn, national security, S&T has developed, operationalized and implemented new training tools and technologies – Sign Cutting and Tracking Training, Augmented REality Sandtable (ARES), and night vision technology – to help maximize the effectiveness of USBP agents as they work to protect the U.S. border.**

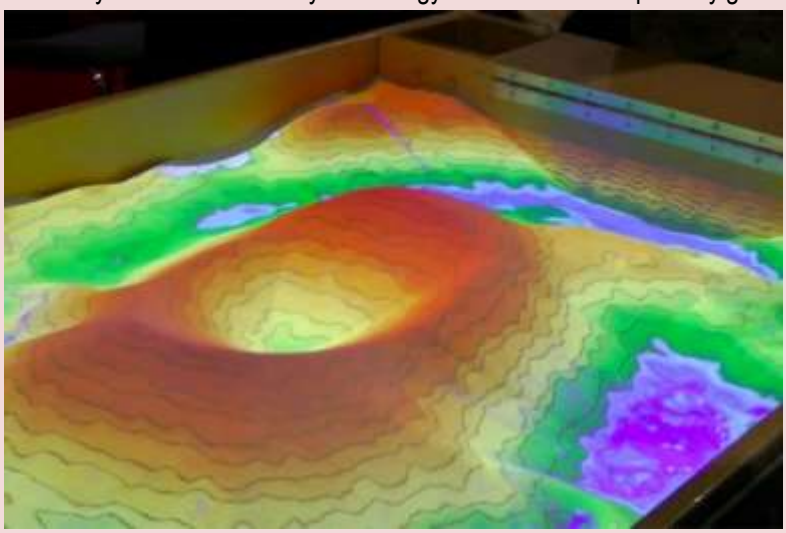
S&T's Sign Cutting and Tracking Training solution consists of 2-D and 3-D training videos, a 90-minute computer-based training course, night vision technology and innovative commercial off-the-shelf augmented reality technologies that were scouted by S&T. S&T filmed the 2-D and 3-D videos along the southern border at locations in California, Arizona and Texas with expert trackers and then developed instructional content for a computer-based training course that teaches agents how to identify visual signs of human activity across different terrain, environments and times of the day. The Sign Cutting and Tracking Training solution then leverages night vision, augmented reality technology and virtual reality technologies to increase situational awareness in order to further enhance how to accurately identify and track the movement (also known as "sign cutting") of individuals and groups along the border.

The effectiveness and operational impact of the Sign Cutting and Tracking Training solution was recently demonstrated during a Post Transition Performance Assessment conducted at the USBP Academy. In this assessment, two groups of newly-hired border patrol agents were given either the legacy sign cutting and tracking instruction, or the new S&T developed computer-based training during that two hour period. Both groups then went out into the field for their practical exercises to demonstrate their skills in "tracking boxes" that instructors used to assess their

tracking performance. Those agents that trained using S&T's new Sign Cutting and Tracking Training solution performed 63 percent better than agents who received the legacy classroom instruction.

As part of efforts to expand and enhance the Sign Cutting Tracking Training solution, S&T is also implementing multiple virtual reality and Augmented REality Sandtable (ARES) technologies. Originally developed by the U.S. Army, S&T has repurposed the ARES technology to increase situation awareness in bot training and operations; enhance USBP and FLETC training; conduct mission pre-planning/pre-briefing; conduct operational exercises; allocate deployment of resources; enhance after action review; and improve real-time decision making and mitigation of risk during field operations.


ARES is an interactive digital sand table that uses augmented reality and/or virtual reality technology to create a 3D map of any given terrain. It uses uses a projector to display a topographical map of the desired environment on top of sand in a large sandbox, on the floor in larger spaces, or in a virtual or augmented reality environment. The sand projection uses a motion sensor that keeps track of changes a user makes in the shifting or layout of the sand and then appropriately adjusts the computer-generated terrain projection to match the sand. ARES serves as a low-cost solution that gives USBP the capability to dynamically create terrain for a specific area of interest, visualize lines of sight and overlay different types of maps to create a 3-D hologram. The ARES floor-projected version can be used for briefing larger groups, as well as a virtual reality version for individuals. All of these variations can even be networked together for coordination of exercises or operations in different locations. In some cases, the virtual reality versions of ARES are being transitioned to remote locations where staff are not able to access a physical sand table or floor projection. S&T is exploring other potential uses of the ARES technology in wildland firefighting, evacuation planning and execution as well as search and rescue and emergency management operations.



Finally, S&T is delivering night vision technology to FLETC, to enhance their capabilities in developing night tracking skills. This technology will serve as a valuable tool for FLETC to use as part of their Backcountry Tactical Tracking Training Program, which develops agent

and officer skills in tracking as part of missions to ensure border security, counter human and drug trafficking, capture fugitives, and conduct search and rescue operations.

"One of the most prevalent challenges in law enforcement response is operating during hours of darkness," said Scott Glisson, Senior Instructor for Tracking, Land Navigation and Field Skills, FLETC. Through the use of night vision technology S&T is transitioning, officers and agents will have the ability to exceed the human limitations imposed during night time operations. Officer and agent response times can be measurably reduced with the use of this tech and their operational safety is also enhanced by giving them tactical advantage over potential suspects."

S&T deployed and transitioned two ARES sandtables, a virtual reality system and the Sign Cutting and Tracking Training solution with full 3D capabilities to the USBP Yuma Sector Headquarters on October 21, 2019. S&T will also be deploying and transitioning these tools, along with night vision technology, to FLETC's training centers in Glynco/Brunswick, Georgia, and Artesia, New Mexico. The capabilities of these tools and technologies will ensure USBP, FLETC and the agents and officers they train will be able to maximize their performance and have immediate and ongoing access to cutting edge, top-of-the-line solutions.

"The new and improved Sign Cutting and Tracking Training solution, ARES and the night vision technology are just a couple examples of solutions being delivered by S&T to enhance national security, and are resulting in measurable performance impacts," said DHS S&T Progarm Manager Darren P. Wilson. "When combined with 3-D video capabilities and computer-based training course content, these technologies enable USBP and FLETC to maximize the knowledge, skills and abilities of agents and officers who are tasked with identifying and tracking activity along the border, enforcing immigration laws, countering drug and human trafficking, pursuing fugitives and conducting search and rescue operations."

▶▶ To learn more about S&T's Sign Cutting and Tracking Training solution, watch short video.


## National Response Framework, Fourth Edition

*Fri, November 08, 2019*

The National Response Framework (NRF) provides foundational emergency management doctrine for how the United States responds to all types of incidents. The NRF is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the nation.

## A World At Risk: Annual Report on Global Preparedness for Health Emergencies

*Mon, October 07, 2019*

The Global Preparedness Monitoring Board explores and identifies the most urgent needs and actions required to accelerate preparedness for health emergencies, focusing in particular on biological risks manifesting as epidemics and pandemics. The Board identified seven actions for implementation to prepare for pressing threats.


## Disasters and People With Serious Mental Illness

*Mon, September 09, 2019*

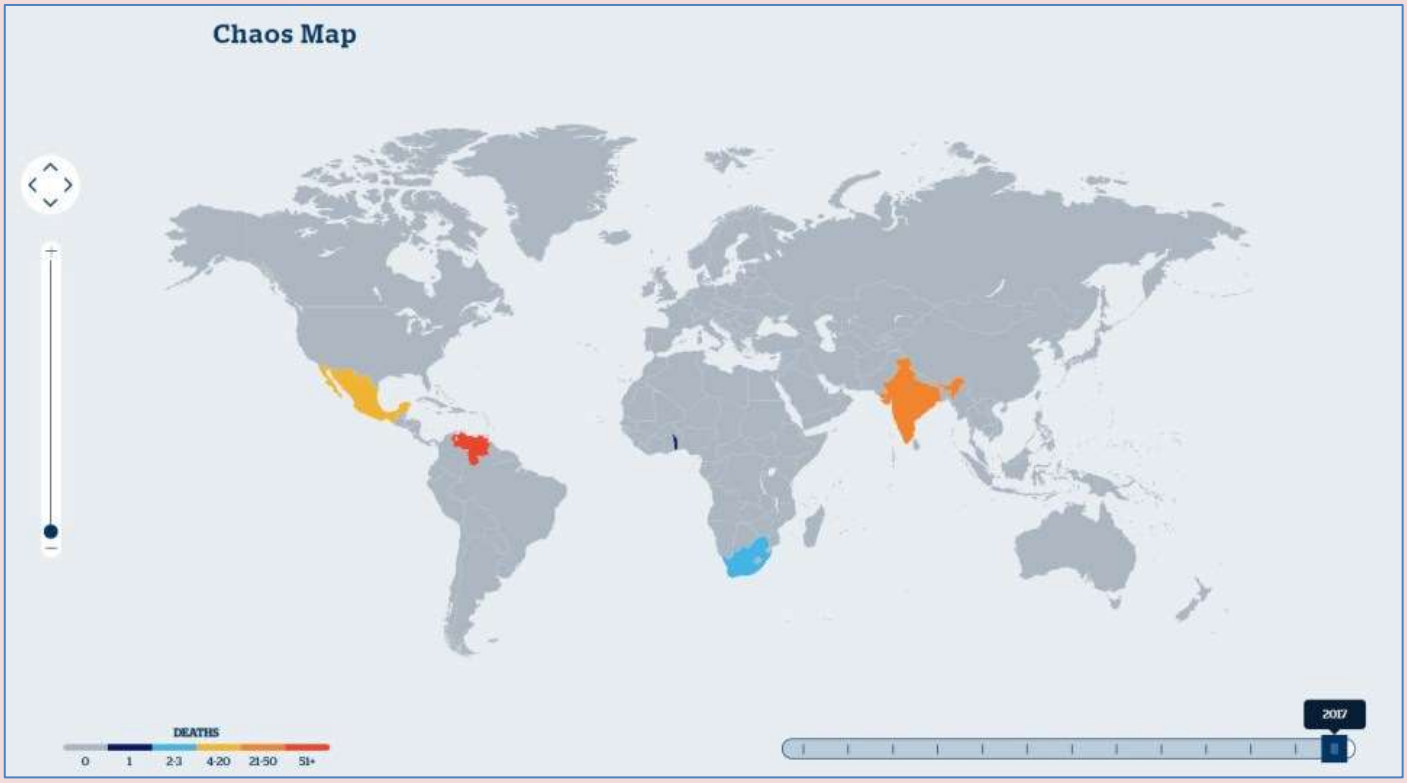
This bulletin focuses on the experiences of individuals with serious mental illness (SMI) before, during, and after disasters. Research focused on individuals with schizophrenia, bipolar disorder, major depression, and post-traumatic stress disorder (PTSD), and on individuals with SMI as defined in part through functional limitations.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
2
BRNE
DIARY
ASYMMETRIC
THREATS

# Chaos Map

**By Anna Scholz-Carlson** (Thomson Reuters Foundation)
Source: https://aru.ac.uk/global-sustainability-institute-gsi/events/global-chaos-maps
**Map:** https://aru.ac.uk/global-sustainability-institute-gsi/research/global-risk-and-resilience/global-chaos-map-project

LONDON: As the planet warms, deadly conflicts over water, food and fuel shortages and price hikes for those essentials are expected to start increasing dramatically, including in relatively stable parts of the world like Europe, researchers warned on Thursday.
A new interactive **"Chaos Map" from Britain's Anglia Ruskin University (ARU)** displays 1,300 deaths from violent social unrest and suicides linked to water, food and fuel insecurity over a 13-year period from 2005 to 2017.




Researchers said it would help predict future tensions over disruptions to key resources.
Governments worldwide have yet to put in place measures to reduce the risks of conflict, such as food stocks and agreements with neighbouring countries to share supplies, they added.
Without better preparedness, more frequent climate shocks - including floods and droughts that damage harvests - could lead to large-scale violence and the collapse of global markets, they warned.
"We are vulnerable at the moment - it's an urgent call," said Aled Jones, director of the ARU's Global Sustainability Institute and co-leader of the team behind the map.
**The interactive tool shows the location of deaths and their causes year by year, based on data drawn from news reports verified by researchers, alongside commentary on some cases.**
**The majority occurred in Africa and Asia, with the highest fatalities in Venezuela, India, Yemen, Tunisia and Sri Lanka.**
Conflict over water - mainly tied to control of water infrastructure - caused more deaths than food and fuel instability in the period studied, said Jones.
The largest incident reported was 425 deaths from clashes in 2006 between Sri Lanka's government and Tamil Tiger insurgents who were accused of blocking access to local water supplies, according to the researchers.
More common were smaller events such as the 2012 death of a man in the Indian city of Howrah, when late deliveries by a water truck caused a brawl to break out in a waiting crowd.
But cases of fatal unrest are not limited to politically unstable places, the researchers said.

Growing dissatisfaction with food and fuel costs has also led to violence in Europe, including the death of a demonstrator who was hit by a motorist in Paris during France's "yellow vest" protests sparked by fuel-tax hikes last year, Jones said.
Meanwhile, access to food "is an issue in every country from the UK to North Africa to the Middle East", he added, noting how the use of food banks has risen in Britain.
Developing a holistic European food strategy with all states working together on food reserves, trade plans and policy responses was crucial, he said.
That would not only protect against climate shocks but also help Europe prepare for possible influxes of migrants from more fragile countries, driven by climate disasters and conflicts, which could put pressure on food supplies, said Jones.
After a prolonged decline, hunger is on the rise again globally - partly due to climate change, said Gernot Laganda, who heads work on climate and disaster risk reduction at the U.N. World Food Programme and was not involved in the map.
Governments need to understand the evolving nature of threats "when living in a dynamic environment where climate change increases risks" - and get ready to respond, he told the Thomson Reuters Foundation.
People caught in situations that are experiencing both climate extremes and conflict are a pressing concern because of the difficulty of getting aid to them, he added.