HZS C²BRNE DIARY
Dedicated to Global First Responders
November 2021
11\21

To vaccinate or not to vaccinate? That is the question!

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

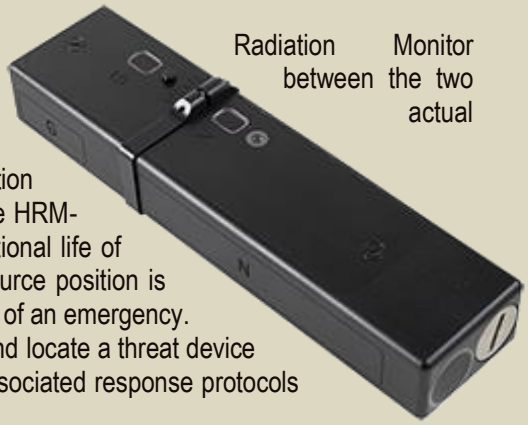
HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DIRTY R-NEWS

Handheld Radiation Monitor Simulator

Source: https://www.argonelectronics.com/hubfs/Products/Product%20Sheets/HRM-SIM-EN.pdf



Argon Electronics is proud to have launched a training simulator for the Handheld Radiation Monitor (HRM), made by Sensor Technology Engineering. Thanks to the close partnership between the two companies, the look, feel, and response of the HRM-SIM is remarkably similar to the actual detector.

The HRM-SIM, replicates the self-contained gamma ray and thermo neutron radiation detector for use in the interdiction and localization of nuclear materials. Moreover, the HRM-SIM is powered by the same commercial batteries as the actual detector, the operational life of which is typically 160 hours. Even the effect of user body shielding to determine source position is realistically simulated, which ensures survey teams understand what to do in the event of an emergency.

Argon's HRM-SIM is for training operators who need to quickly and discreetly detect and locate a threat device or radiological materials in an unpredictable radiation background and practice the associated response protocols and procedures should a reading be obtained.

All user interface components are exactly the same as the real detector to ensure the ultimate training experience. The response speed and characteristics are very similar to the real detector, which allows realistic source search/find training to be carried out.

Additionally, the HRM-SIM's simulated delivered sensitivity enables it to detect the RadSim-GS4 simulation Gamma/Neutron source at a free space distance of typically 160 feet (50 meters) distance line of sight.

The HRM-SIM offers a highly realistic approach to radiation training that will ensure your personnel are knowledgeable and confident when faced with radiological emergencies in the field. Moreover, no preventative maintenance, calibration, or consumables (except batteries) are required, ensuring the whole life cost of ownership is minimal.

GAO: National Strategy Needed to Prevent Radioactive Materials from Becoming Dirty Bombs

By Kylie Bielby

Source: https://www.hstoday.us/federal-pages/government-reports-and-summaries/gao-national-strategy-needed-to-prevent-radioactive-materials-becoming-dirty-bombs/

Oct 25 – Dangerous radioactive material is used in many medical and industrial applications. But, in the hands of terrorists, it could be used to construct a radiological dispersal device, or dirty bomb, that uses conventional explosives to disperse the material.

Recent security threats have raised concern that terrorists could target radioactive material for theft and use in a domestic attack. From 2010 through 2019, the U.S. Nuclear Regulatory Commission (NRC) reported 2,133 nuclear materials events, which include instances of lost or stolen radioactive materials, radiation overexposures, leaking sources of radioactive material, and other events.

Current assessments of the threat environment show an increasing interest in using radioactive material for making a dirty bomb. Americium-241, cobalt-60, cesium-137, and iridium-192 are the most prevalent high-risk radioactive materials in the U.S. economy today, and they are frequently found in dangerous quantities. Replacing technologies that use radioactive materials with safer alternatives can protect people and reduce potential financial costs. For example, in May 2019, an accidental release of cesium-137 at the University of Washington showed that even small quantities of radioactive materials pose risks and can cost millions to clean up.

The Government Accountability Office (GAO) has examined six common medical and industrial applications that use high-risk radioactive materials—identified through agency and expert reports—and found that three applications already have technically viable alternative technologies in many circumstances and for which there is market acceptance.

For example, x-ray provides a technically viable alternative to replace cesium-137 blood irradiators, one of the common applications. Another of the applications GAO studied has a technically viable alternative, though only in certain limited circumstances, and the two remaining applications do not yet have viable alternatives. For example, alternatives to replace americium-241 used in oil and gas well logging equipment, another common application, are still under development.

GAO reported that users of applications that employ high-risk radioactive materials identified six factors they take into account when determining whether to adopt alternative technologies: technical viability of alternatives, device cost, costs to convert (such as facility renovations), disposal of radioactive materials, regulatory requirements, and liability and other potential costs associated with possessing high-risk radioactive materials.

GAO@100 Highlights

Highlights of GAO-22-104113, a report to congressional committees

October 2021

ALTERNATIVES TO RADIOACTIVE MATERIALS

A National Strategy to Support Alternative Technologies May Reduce Risks of a Dirty Bomb

Why GAO Did This Study

Radioactive material, which is dangerous if mishandled, is found in many medical and industrial applications. In the hands of terrorists, it could be used to construct a radiological dispersal device, or dirty bomb, that uses conventional explosives to disperse the material. Replacing technologies that use dangerous radioactive materials with safer alternatives may help protect people and reduce potential socioeconomic costs from remediation and evacuation of affected residents.

Senate Report 116-102 included a provision for GAO to review alternative technologies to applications that use radioactive materials. This report examines (1) the potential for adopting alternative technologies in the United States for the six most commonly used medical and industrial applications; (2) factors affecting adoption of alternative technologies; and (3) federal activities relating to alternative technologies in the United States. GAO reviewed relevant documents to identify potential alternative technologies, conducted interviews with users of applications that employ radioactive material to identify factors affecting adoption of alternatives, and interviewed federal officials to discuss current federal activities relating to alternative technologies.

What GAO Recommends

Congress should consider directing an entity to develop a national strategy to support alternative technologies. The federal agencies involved in research and adoption of alternative technologies neither agreed nor disagreed with our matters for congressional consideration.

View GAO-22-104113. For more information, contact Allison Bawden at (202) 512-3841 or bawdena@gao.gov.

What GAO Found

GAO examined six common medical and industrial applications that use high-risk radioactive materials—identified through agency and expert reports—and found that three applications already have technically viable alternative technologies in many circumstances and for which there is market acceptance. For example, x-ray provides a technically viable alternative to replace cesium-137 blood irradiators, one of the common applications. Another of the applications has a technically viable alternative, though only in certain limited circumstances, and the two remaining applications do not yet have viable alternatives. For example, alternatives to replace americium-241 used in oil and gas well logging equipment, another common application, are still under development.

Irradiator with Radioactive Material (left) and Alternative Technology (right)

Sources: Brookhaven National Lab and Rad Source Technologies Inc. | GAO-22-104113

Users of applications that employ high-risk radioactive materials identified six factors they take into account when determining whether to adopt alternative technologies: technical viability of alternatives, device cost, costs to convert (such as facility renovations), disposal of radioactive materials, regulatory requirements, and liability and other potential costs associated with possessing high-risk radioactive materials. An accident at the University of Washington in May 2019 shows that liability and other potential costs would likely range from millions to billions of dollars if radioactive materials were accidentally released or used in a dirty bomb. These largely uninsured socioeconomic costs are an implicit fiscal exposure for the federal government, which could be expected to provide financial assistance.

Several federal agencies and interagency entities support research and promote adoption of alternative technologies. For example, the National Nuclear Security Administration (NNSA) has removed 355 irradiators since 2004 and subsidized the replacement of some with x-ray technology. Congress also established the goal for the NNSA to eliminate the use of cesium-137 blood irradiators in the United States by 2027. At the same time, the Nuclear Regulatory Commission licenses radioactive materials for irradiators, consistent with its mission. Currently, no strategy exists to guide federal efforts to find alternatives and reduce risk. A strategy to support alternative technologies would ensure a cohesive federal approach and potentially reduce the implicit fiscal exposure associated with addressing socioeconomic damage from a dirty bomb.

United States Government Accountability Office

An accident at the University of Washington in May 2019 shows that liability and other potential costs would likely range from millions to billions of dollars if radioactive materials were accidentally released or used in a dirty bomb. These largely uninsured socioeconomic costs are an implicit fiscal exposure for the federal government, which could be expected to provide financial assistance.

▶▶ Read the full report at GAO

Several federal agencies and interagency entities support research and promote adoption of alternative technologies, GAO found. For example, the National Nuclear Security Administration (NNSA) has removed 355 irradiators since 2004 and subsidized the replacement of some with x-ray technology. Congress also established the goal for the NNSA to eliminate the use of cesium-137 blood irradiators in the United States by 2027. At the same time, the NRC licenses radioactive materials for irradiators, consistent with its mission.

Currently, no strategy exists to guide federal efforts to find alternatives and reduce risk, leading to a lack of coordination between agencies, and in some cases, resulting in agencies working at cross-purposes. According to GAO, there is no cohesive federal strategy because the federal government has yet to resolve two opposing objectives: permanent risk reduction where possible, and the continued licensing of high-risk radioactive materials without an evaluation of available alternatives.

NNSA officials told GAO that the Office of Science and Technology Policy (OSTP)-led interagency effort to develop the White House's 2016 Best Practices Guide injected a sense of top-level investment that temporarily reinvigorated interagency coordination around alternative technologies. However, White House officials in the previous and current administrations told GAO that OSTP has taken no further action to date to verify if agencies are implementing these practices.

A national strategy to support alternative technologies would ensure a cohesive federal approach and potentially reduce the implicit fiscal exposure associated with addressing socioeconomic damage from a dirty bomb. GAO therefore wants Congress to consider directing an entity to develop a national strategy to support alternative technologies.

Nuclear Weapons and Europe

By Brian Cloughley

Source: https://www.strategic-culture.org/news/2021/10/12/nuclear-weapons-and-europe/

Oct 12 – On October 5 the U.S. State Department announced that the U.S. military's arsenal of nuclear weapons numbered 3,750 as of September 30, 2020. It was stated with satisfaction that "This number represents an approximate 88 percent reduction in the

stockpile from its maximum (31,255) at the end of fiscal year 1967", although it wasn't mentioned that the reduction since 2018 was only 35.

On the same day, the U.S. Defense Department publication *Stars and Stripes* reported that "an Air Force fighter jet slated to debut later this year in Europe passed a milestone when it dropped mock nuclear bombs during training flights designed to ensure its ability to fulfil NATO's nuclear deterrence mission . . . The successful test of the F-35A Lightning II came as the 48th Fighter Wing, based at Britain's RAF Lakenheath, reactivated the 495th Fighter Squadron last week ***for a new mission in Europe***. [Emphasis added.] Ahead of the fighter model's arrival at Lakenheath, two F-35As that took off from Nellis Air Force Base, Nevada, completed a full weapon system demonstration, regarded as a graduation flight test for achieving nuclear certification."

In February 2021 U.S. Secretary of State Antony Blinken informed the Conference on Disarmament in Geneva that "President Biden has made it clear: the U.S. has a national security imperative and a moral responsibility to reduce and eventually eliminate the threat posed by weapons of mass destruction" and President Biden pledged to "take steps to reduce the role of nuclear weapons in our national security strategy," but it has not been made clear how elimination of the threat from nuclear weapons or reduction of their role in U.S. military strategy can be achieved by training more combat aircraft pilots in the use of nuclear weapons and then deploying them to Europe with their strike aircraft.

The United Kingdom has an equally interesting perspective in what it describes as its "leading approach to nuclear disarmament" and is increasing its arsenal of nuclear weapons. As the Royal United Services Institute noted in March, the UK's 2021 *Integrated Review of Security, Defence, Development and Foreign Policy* states that the UK is "raising a self-imposed limit on its overall nuclear warhead stockpile" of the current 225 warheads.

U.S. deployment of nuclear strike aircraft to the UK signals to continental Europe that planning for nuclear war against Russia is accelerating.

The Review, headed "Global Britain in a Competitive Age", explains that in 2021 it had been announced as national policy that there would be a reduction in "our overall nuclear warhead stockpile ceiling from not more than 225 to not more than 180 by the mid-2020s. However, in recognition of the evolving security environment . . . this is no longer possible, and the UK will move to an overall nuclear weapon stockpile of no more than 260 warheads." Then it assured the international community that in spite of increasing the number of its nuclear weapons delivery systems the United Kingdom is "strongly committed to full implementation of the NPT in all its aspects, including nuclear disarmament."

It is intriguing that the present British government would have us believe that more nuclear weapons and deployment of 27 U.S. nuclear-capable F-35 aircraft to the UK's Royal Air Force base at Lakenheath are in some fashion compatible with nuclear disarmament, but what is consistent is their linkage with the stockpiles of U.S. nuclear bombs already in Europe.

It is not known if there are or will be any U.S. nuclear weapons kept at Lakenheath, and no doubt the UK government would be comfortable with such storage which would add comparatively few bombs to the hundred or so already stored in vaults in air bases at Kleine Brogel in Belgium, Büchel in Germany, Aviano and Ghedi in Italy, Volkel in the Netherlands, and Incirlik in Turkey. It is regrettable that while the U.S. and Britain insist that they are trying to reduce the threat of nuclear war they are actually increasing and expanding numbers, locations and strike capabilities of nuclear weapons' systems.

The U.S.-Nato military alliance policy is that "nuclear weapons are a core component of NATO's overall capabilities for deterrence and defence," resting almost entirely on U.S. nuclear delivery capabilities which are to be expanded at vast expense, with the new generation of Intercontinental Ballistic Missile Systems, now referred to as the Ground-Based Strategic Deterrent, likely to cost 95 billion dollars — if there are no cost overruns.

As stated by the Congressional Budget Office, it is "required by law to project the 10-year costs of nuclear forces every two years" and its latest paper, "Projected Costs of U.S. Nuclear Forces, 2021 to 2030" makes sobering reading because it is projected that U.S. taxpayers, in this era of fiscal crises, will be required to pay sixty billion dollars a year for nuclear forces over the next ten years. The Office estimates that "about $188 billion of the $551 billion total over the 2021–2030 period would go toward modernizing nuclear weapons and delivery systems. Of that amount, $175 billion would go toward modernizing the strategic nuclear triad, and $13 billion would be for modernizing tactical nuclear weapons and delivery systems." **And this does not include funding of such massive projects as the F-35 strike aircraft which will cost some $1.6 *trillion*.**

The political justification for massive military spending on conventional and nuclear weapons by the governments in London and Washington is their contention that Russia and China pose a threat and that, in the words of the 2021 U.S. *Interim National Security Strategic Guidance*, Russia, for example, is "determined to enhance its global influence and play a disruptive role on the world stage." (Presumably Washington means the sort of disruption that Associated Press reported on October 7 when "Europe's soaring gas prices dropped . . . after Russian President Vladimir Putin suggested his country could sell more gas to European spot buyers via its domestic market in addition to through existing long-term contracts.")

The surge in deployment of nuclear systems and the overall tenor of nuclear weapons developments in Europe do not meet with approval in the European community. For example, a survey published in January revealed that 74% of Italians, 58% of Dutch and 57% of Belgians and 83% of Germans want U.S. nuclear weapons removed from their countries, and another poll (albeit by the Campaign for Nuclear Disarmament) found that 77% of Britons favour a total ban on nuclear weapons.

Europe is in a state of flux, and not only because of the economic and social effects of the pandemic. For example, the Warsaw government's recent refusal to abide by European Union laws could result in Poland leaving the EU (which would be greeted with approval by most EU citizens) but this would have no effect on the U.S.-Nato military buildup — the "Enhanced Forward Presence" along Russia's borders, backed to the hilt by nuclear weapons.

U.S. deployment of a further squadron of nuclear strike aircraft to the UK, for a "new mission in Europe", combined with its existing stocks of nuclear weapons in Europe and Britain's undebated decision to increase its nuclear weapons arsenal are signals to continental European nations that planning for nuclear war against Russia is accelerating. While these countries prefer to engage with Washington and London in a balanced fashion and wish to maintain cordial relations, it would be advisable to question the motives behind the growing emphasis on nuclear war and insist on a reduction in confrontational deployments.

***Brian Cloughley** is a British and Australian armies' veteran, former deputy head of the UN military mission in Kashmir, and Australian defense attaché in Pakistan.*

EDITOR'S COMMENT: Why do numbers matter? One bomb per city (Hiroshima & Nagasaki) was enough to end WWII. Why do they compete about numbers and delivery systems? All nuclear powers will target cities and critical infrastructures, not valleys, deserts, and mountains. All of them have second-strike capabilities. The day after will sustainable to justify the "victory"? Environmental pollution; contaminated citizens; near-zero commerce and distribution of vital goods. Finally, one country will dominate others and rule in the new post-nuclear planet. Rule of what? Ruins, debris, and death plus massive radiation consequences? On October 25, 2021, German Defense Minister Kramp-Karrenbauer had talked about the possibility of deploying atomic arms against Russia. He told the Berlin-based Deutschlandfunk broadcaster: "*We have to make it very clear to Russia that in the end – and that is also the deterrent doctrine – we are prepared to use such means so that it has a deterrent effect beforehand and no one gets the idea to attack NATO partners*." Unrealistic statements from a country responsible for two World Wars. The overall conclusion is that human stupidity is more powerful and by far more hazardous than nuclear weapons and people should do something about it. Yesterday!

Solving the puzzle: The HazMat Guys use Argon's sims in an escape room

Source: https://www.argonelectronics.com/blog/solving-the-puzzle-the-hazmat-guys-use-argons-sims-in-an-escape-room

Oct 15 – Bryan Sommers, Argon Electronics' North American Business Development Manager, first met the HazMat Guys in early 2021. He was invited onto their podcast to discuss HazMat training and to listen to their feedback on the demonstration he provided for two of Argon's latest radiation simulation technologies—the RadEye Sim and the RadSIM GS4 gamma radiation source.

If you haven't yet had the chance to listen to the podcast, it is available in full here.

Who are the HazMat Guys?

The HazMat guys are Bobby Salvesen and Mike Monaco, who have both been involved in firefighting for around 25 years. Bobby is currently Deputy Chief instructor for the Nassau County Fire Service Academy, and Mike is a Master Instructor with the International Association of Fire Fighters.

Their mission is to create a space to provide information and share ideas about Hazardous Materials response through their podcast, forums, and articles. The resources are meant for colleagues, instructors, and students.

Moreover, in 2020, they launched the HazMat Guys e-University. This online learning platform contains courses from leading HazMat professionals on subjects from "Decontamination" to "From meth labs to chemical suicide".

Argon Electronics was delighted to have had the opportunity to share our latest simulation radiation training devices with The HazMat Guys, and the pair also seemed to value the experience. Mike said he was "blown away by the product I got to demo...it was so realistic".

The HazMat guys' difficulties with conventional training

When describing the challenges presented in his field, Mike says that "Training is one of the hardest paradigms to break in the world of HazMat. There has, for the most part, only been two paths to walk down—lecturing or hands-on training."

He continues that, "Lecturers are great when it comes to disseminating information, but they lack the ability to truly test a student's knowledge in different or abstract situations. This renders classroom training all but unless since many of the more complicated HazMat incidents require our knowledge to be used to think outside the box."

Mike also sees a problem for hands-on training as "Students can be taught to use equipment and understand its function, but the challenge for an instructor is how to create a situation that can better mimic the stress and pressure of being on the scene."

The HazMat guys take Argon's SIMs to an escape room

G iven the HazMat guys' perceived difficulties with conventional training, Argon was delighted to hear that Bobby and Mike had been so impressed with the simulation devices that they wanted to test them in a U.S. escape room.

They designed an escape room to solve the issues that traditional training presents and integrated Argon Electronics' simulation equipment to provide an even higher level of detail.

The HazMat guys are primarily instructors, so their main focus is always centred around how the scenarios they create and the equipment they use will help students learn. Ultimately, they are concerned with how students' reactions can be improved in preparation for a real-life emergency event.

And they sounded impressed with Argon's equipment. Mike said that "Argon's meters almost perfectly mimic actual functions, and we can challenge a student's knowledge, technique, teamwork, critical thinking, and understanding in a way never before seen. We can simultaneously challenge a student without sacrificing realism, situational pressures, or proper functionality."

Argon's simulators used in the escape room

RadEye GF-10 SIM

Argon Electronics' RadEye GF-10 simulator was designed to respond to RadSIM GS4 electromagnetic sources.

Key features include:

- Interface components that are identical to those of the real detector (including display, indicators, switch panel, vibrator, and sounder)
- Response speed and characteristics that behave exactly as the real detector does when approaching or moving away from the simulation source
- Simulated sensitivity that enables the simulator to detect the RadSIM GS4 simulation source at a free space distance of approximately 200 feet
- Powerful proprietary signal processing which ensures simulated readings are repeatable each time the trainee revists the same scenario location
- Simulation of the effects of user body shielding so survey teams can confidently and accurately interpret their detector readings and alarms
- Inverse square law response that is within real detector tolerance
- Selectable units of measurement (Sv/hr, Rem, CPS)

RadSIM GS4

The RadSIM GS4 Simulator provides a simulated gamma radiation source that is incredibly believable.
Instructors have the freedom to create a diverse array of search exercises while remaining free from all of the usual regulatory and administrative restrictions of working with live sources.
Key features of the RadSIM GS4 include:

- The ability to create "live source" radiological survey exercises where survey teams can experience realistic dose rate and dose readings, inverse square law response and the shielding effects of different materials
- Isotropic emission which enables the source to be detected at a distance of up to 200 feet when using a standard sensitivity simulation detector - or up to 300 feet free space if using a high sensitivity simulation detector
- No preventative maintenance, calibration, or consumables (aside from batteries), which keeps the whole life cost of ownership to a minimum

Primary Medical and Industrial Applications for High-Risk Radioactive Materials

Source: https://www.gao.gov/assets/gao-22-104113.pdf

Application	Purpose	Types and typical quantities of radioactive materials used
Blood irradiation	Irradiate blood products to prepare them for transfusion.	cesium-137 (category 1 or 2)
Medical research irradiation	Irradiate cell cultures or animal specimens for research purposes.	cesium-137 (category 1 or 2); cobalt-60 (category 1)
Industrial sterilization	Sterilize medical and food products for public use.	cobalt-60 (category 1)
Stereotactic radiosurgery	Treat brain cancer and cranial nerve disorders with targeted beams of radiation.	cobalt-60 (category 1)
Well logging	Detect and measure the properties of underground geological formations to detect fossil fuel deposits.	americium-241 (category 3); cesium-137 (category 3 or 4)
Industrial radiography	Detect and measure imperfections in industrial pipes and welds.	iridium-192 (category 1 or 2)

Source: GAO analysis of information from the Department of Homeland Security and the National Research Council of the National Academies. | GAO-22-104113

Note: The table does not include all applications of radioactive materials. In addition, according to NNSA officials, well logging users commonly store multiple americium-241 sources that, in aggregate, achieve category 2 quantities.

Blood irradiation. A widely used process whereby donor blood is exposed to radiation, which inactivates a type of white blood cell that may fatally complicate transfusion for some recipients. The most common method of using radiation to treat blood is to place blood bags into a shielded chamber inside of an irradiator containing cesium-137.[1]
Medical research irradiation. Research irradiators are used in medical research to expose cell cultures or animal specimens to gamma radiation from cesium-137 or cobalt-60. Research irradiators are used to study DNA damage, immune response, cancer development, and other areas.
Industrial sterilization. Cobalt-60 panoramic irradiators use gamma radiation to sterilize large quantities of medical devices and food products before being sold to consumers. According to the International Irradiation Association, gamma-based sterilization using cobalt-60 represents about 40.5% of the sterilization market, with non-radioisotopic methods making up the remainder. Gamma-

[1] Hospitals and research centers in the United States and around the world are addressing concerns about radiological security, safety and liability by replacing blood irradiators that use radioactive cesium-137 with safe, effective, FDA-approved X-ray technology.

based industrial sterilization is typically conducted in warehouses, and involves conveying pallets of product through a shielded room to be exposed to radiation from large quantities of cobalt-60.
Stereotactic radiosurgery. A large, helmet-like device focuses beams of gamma radiation from several cobalt-60 sources to treat brain and cranial illnesses. Gamma Knife® devices use cobalt-60 to treat tumors and nerve disorders.
Well logging. As an aid to searching for oil, gas, and water, or conducting environmental or other forms of underground monitoring, well logging devices using americium-241 and cesium-137 are used to examine geologic features around a borehole or well. Well logging devices are lowered downhole and emit radiation and take readings on the characteristics of an underground formation, such as its chemical and mineral contents.
Industrial radiography. Hand-held iridium-192 radiography "cameras" are used for the non-destructive inspection of welds, pipes, and other materials. Industrial radiography typically exposes the object to gamma radiation that, once deposited onto a detector, produces a fine-detail image of any imperfections in the object.

The International Atomic Energy Agency's Code of Conduct on the Safety and Security of Radioactive Sources defines the five categories for radiation sources to help ensure that sufficient controls are being used to achieve safety and security:

- **Category 1 sources**, if not safely or securely managed, would be likely to cause permanent injury to a person who handled them or was otherwise in contact with them for more than a few minutes. It would probably be fatal to be close to this amount of unshielded material for a period of a few minutes to an hour. These sources are typically used in radiothermal generators, irradiators, and radiation teletherapy.
- **Category 2 sources**, if not safely or securely managed, could cause permanent injury to a person who handled them or was otherwise in contact with them for a short time (minutes to hours). It could possibly be fatal to be close to this amount of unshielded radioactive material for a period of hours to days. These sources are typically used in industrial gamma radiography, high- and medium-dose rate brachytherapy, and radiography.
- **Category 3 sources**, if not safely or securely managed, could cause permanent injury to a person who handled them or was otherwise in contact with them for hours. It could possibly—although it is unlikely to—be fatal to be close to this amount of unshielded radioactive material for a period of days to weeks. These sources are typically used in fixed industrial gauges such as level gauges, dredger gauges, conveyor gauges, spinning pipe gauges, and well-logging gauges.
- **Category 4 sources**, if not safely managed or securely protected, could possibly cause temporary injury to someone who handled them or was otherwise in contact with or close to them for a period of many weeks, though this is unlikely. It is very unlikely anyone would be permanently injured by this amount of radioactive material. These sources are typically used in fixed or portable gauges, static eliminators, or low-dose brachytherapy.
- **Category 5 sources** cannot cause permanent injury. They are used in x-ray fluorescence devices and electron capture devices.

Only Categories 1 and 2 for radiation sources are defined by NRC requirements

▶▶ **Read also:** https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1227_web.pdf

Hiroshima atomic bombing survivor Sunao Tsuboi dies at 96

Source: https://www.yakimaherald.com/news/nation_and_world/hiroshima-atomic-bombing-survivor-sunao-tsuboi-dies-at-96/article_5df2ce74-4e06-5f53-a2e8-2de12dc80c14.html

Oct 27 — Sunao Tsuboi, a survivor of the Hiroshima atomic bombing who made opposing nuclear weapons the message of his life, including in a meeting with President Barack Obama in 2016, has died. He was 96.
Tsuboi died Oct. 24 in a hospital in Hiroshima in southwestern Japan. The cause of death was given as an irregular heartbeat caused by anemia, Nihon Hidankyo, the nationwide group of atomic bomb survivors he headed until his death, said Wednesday.
When Obama made his historic visit to Hiroshima, Obama and Tsuboi held each other's hand in a long handshake and shared a laugh. An interpreter stood by. Tsuboi, a gentle yet passionate man, recalled he tried to talk fast, to tell Obama he will be remembered for having listened to atomic bomb survivors, known in Japanese as "hibakusha."
"I think he is such an earnest person or has the heart to feel for others," Tsuboi said of the first sitting U.S. president to visit Hiroshima.
Tsuboi was 20 years old when he miraculously survived the U.S. atomic bombing of his hometown on Aug. 6, 1945, in the closing days of World War II.
He suffered such serious burns a part of his ear was gone. When he emerged from unconsciousness 40 days after the bombing, the war was over. He was so weak and scarred he had to start by practicing crawling on the floor.

SUNAO TSUBOI: A-Bomb survivor, standing in front of one of the few pictures taken in the first days of the bombing and in which he can recognize himself between the wounded. Tsuboi was a 20-year-old university student when he was blown 10 meters into the air by the blast from the bomb and burnt from head to toe. He describes the subsequent scene wandering around the city with eyeballs dangling out of their sockets and skin hanging from bones as a living hell. He wandered for a week and fell into a coma. When he came to the war was over but he refused to believe it. "I thought it was a trick" He has since suffered three bouts of cancer and tried to commit suicide with his girlfriend when her parents refused to give them permission to marry. "We woke up and cried together we were so happy to be alive".

“They wanted to kill us. No mistake about that,” Tsuboi said in an interview with The Associated Press in 2013.

The world’s first atomic bomb destroyed Hiroshima, killing 140,000 people instantly and within months. Three days later, the U.S. forces dropped a second nuclear bomb, on Nagasaki, killing another 70,000 people. Japan surrendered on Aug. 15.

Tsuboi made a point to stress what happened in Hiroshima was horrible.

“Here it was about annihilation,” he told the AP.

Tsuboi worked as a junior high school teacher. He was so intent on educating youngsters about anti-nuclear proliferation his nickname became “pikadon sensei,” combining the “flash-boom” onomatopoeia Japanese use to describe the bomb and the word for “teacher.”

“Never give up” was his trademark phrase, especially for his fight for a world without nuclear weapons.

Akira Kawasaki of ICAN, or the International Campaign to Abolish Nuclear Weapons, a coalition of non-government organizations, said the death of a man who had been the poster boy for anti-nuclear proliferation left him with a “big hole” in his heart.

“We must not only mourn the death of a great leader for our cause, but we must also continue in his path, undeterred, and always remember his words,” he told Japanese public broadcaster NHK TV.

Tsuboi is survived by two daughters and a son. A wake and funeral services were held with immediate family Monday and Tuesday, in respect to Tsuboi’s wishes to keep ceremonies low key. His group is still undecided on a memorial service.

JOURNAL OF CLINICAL MEDICINE OF KAZAKHSTAN (E-ISSN 2313-1519)
Review Article DOI: https://doi.org/10.23950/jcmk/11239

Assessment and treatment requirements of public hospitals to radiation emergencies

Athanasios Zafeirakis[1], Ioannis Galatas[2], Panagiotis Efstathiou[3]

[1]Department of Nuclear Medicine, Army General Hospital of Athens, Greece
[2]CBRN Knowledge Center, International CBRNE Institute, Les Bons Villers, Belgium
[3]Hellenic Association on Crisis Management in the Health Sector, Athens, Greece

Received: 2021-07-21.
Accepted: 2021-09-22

J Clin Med Kaz 2021; 18(5):23-29

Corresponding author:
Athanasios Zafeirakis.
E-mail: athzafeirakis@gmail.com;
ORCID: 0000-0002-3544-3050

Abstract

Radiological emergencies present unique challenges to the public health care system and carry the potential for major disruptions to clinical care. This review aims to present, first a brief guide of the main clinical and laboratory diagnostic tools for the assessment of the absorbed dose in cases of radiological emergencies and second, the best treatment options for acute whole body and local radiation syndromes. Clinical and laboratory state-of-the-art biodosimetry tools, therapies for acute radiation syndromes according to the severity of the radiation sickness and isotope-specific preparedness medications as counter-measures for internal contamination are herein proposed as the necessary stockpile of public hospitals against severe radiological accidents.

Key words: radiological incidents, radiation emergencies, biodosimetry, acute radiation syndromes, radiation treatment

Why NATO is Practicing Nuclear Strike Missions

By Walter Pincus

Source: https://www.thecipherbrief.com/column_article/nuclear-strike-missions

Oct 29 — Last week, aircraft and personnel from 14 NATO countries carried out the annual exercise, code-named Steadfast Noon, which involved practicing nuclear strike missions with dual-capable aircraft and unarmed, American-made B61 tactical nuclear bombs, similar to the roughly 150 B61s the U.S. currently has on bases in five European countries.

According to a NATO statement on the exercise, "No live weapons are used. This exercise helps to ensure that NATO's nuclear deterrent remains safe, secure and effective."

No scenario was given for what led to a U.S. President authorizing the apparent use of such devastating weapons in last week's exercise, and that fact alone encouraged me to go back into records to try to show again how doubtful it would be for any such Presidential order to occur.

In this case, I went to the amazing set of Presidential Oral Histories compiled by the Miller Center at the University of Virginia that contain revealing interviews with personnel from the past administrations of Presidents Jimmy Carter, Ronald Reagan, George H. W. Bush, William J. Clinton and George W. Bush.

I focused on the President George H. W. Bush administration with Dick Cheney, when he was Secretary of Defense, and the late Colin Powell, when he was Chairman of the Joint Chiefs. Here is what they said when the issue of possibly using U.S. tactical nuclear weapons came up in late 1990 as the U.S. was preparing Operation Desert Storm to push Saddam Hussein's Iraqi troops out of Kuwait.

As Cheney put it when questioned at the Miller Center in March 2000, "If he [Saddam] uses biological or chemical agents against our troops, all bets are off and we reserve the right to use any means at our disposal to respond…The threat clearly was that we'd use, or threaten to use, nuclear weapons."

Cheney went on, "I asked for—and had to ask a number of times—for there to be some planning done in the Joint Staff about how we would react if in fact, that happened. I said, I

want to know how many tactical nuclear weapons will it take to destroy a division of the Iraqi Republican Guard. Here's your divisions laid out there. You come back and tell me how many nukes."

As for President Bush, who would have had to order their use, Cheney said, "He [Bush] would have been aware that this was a problem, as I say, without question, but I don't recall a conversation with him. The nuclear, tactical nuclear weapons option was something I wanted. I wanted to know myself, if something happened, is this an option? What do you do to them? So as I say, I found out it takes 17 weapons to destroy an Iraqi Republican Guard division. Or at least that is what I was told."

Cheney said he had "read the history of the Eisenhower years and we're trying to build nuclear weapons, and Hiroshima and Nagasaki aren't that far in the past. We'd used them. By the time you get to the 1990s it is not a very realistic option from the standpoint of the U.S. military."

The Cold War scenario had been "we might have to resort to nuclear weapons to stop—and reserved the right to do so—to stop a Soviet invasion of Western Europe," Cheney said, but then he added, "We had problems with some of those weapons; we had to redeploy them. I think there was always doubt, at least in some of our minds, about an 8-inch nuclear round that you are going to launch out of some artillery piece over here and hit a target 10 or 12 miles away, if that was what you were doing. Didn't seem to be necessarily the right thing to do if you didn't have to."

As for Joint Chiefs Chairman Powell, Cheney said, "Colin had strong feelings, Powell did, about tactical nuclear weapons. He didn't like them. Maybe it was his European experience…He was not a big fan of tactical nukes. I think part of that was based on his earlier experiences in the service. But that was, I would say, the dominant thinking in the U.S. Army especially, and the military."

I, myself, know that to have been true, having written about the neutron warhead in 1977. I studied nuclear weapons thereafter and can say the Army disliked the thought of using tactical nuclear weapons because no one knew what would happen after the first one was used.

When Powell, himself, was interviewed in 2011 for the Miller Center collection, he looked back to the 1990s and said, "The Army did not need to have nuclear weapons. We could make the rubble bounce everywhere now. I was pushing Secretary Cheney to eliminate nuclear weapons in the Army. The Marine Corps was already getting rid of them and some of the Air Force weapons and all of the tactical nuclear weapons aboard the ships."

In fact, in advance of President George H. W. Bush's doing away with most deployed U.S. tactical nuclear weapons in September 1991, Powell recalled, "We sat at the President's desk one afternoon and I said, Mr. President, I've talked to the Chiefs, and they all agree with this…even the Chief of Staff of the Army agrees—surprise, surprise. In ten minutes, he approved the elimination of all of our tactical nuclear weapons, except for the number we kept in the Air Force for fighter-bomber delivery."

In a broader sense, Powell said, "Nukes are of course a weapon of mass destruction, but I can list as many countries that have given them up as those who have tried to pursue them…South Africa gave it up. Even Libya gave it up, and Chile. They all abandoned it. And Iran and North Korea. They can't be used. It would be suicidal."

In his Miller Center 2000 interview — and remember this was before the 2003 Iraq invasion when Cheney was Vice President – Cheney recalled during 1990 he had ordered a review of the SIOP, the Single Integrated Operational Plan that provides target options for a U.S. President in the event strategic nuclear weapons are to be used.

Cheney found, as he said back in March 2000, "The number of weapons [in the SIOP plan back then] that were actually going down in a particular geographic area, it didn't make a hell of a lot of sense, frankly. It was clear that there were places where there were one hell of a lot of weapons going down because we just added stuff over the years and had never really gone back and looked at it in those terms."

As a result, he said, "We concluded…we had a lot more nuclear warheads than we needed. That we could cover the target base and do what needed to be done with fewer weapons…We wanted to preserve the Triad [nuclear delivery by submarines, bombers and land-based ICBMs]…But it also offered up the opportunity to put stuff on the table in the course of strategic arms control talks, because now we had something to trade away."

In fact, Cheney's 1991 SIOP study became the basis for Bush's radical arms control reduction proposals to Russia's Mikhail Gorbachev in September 1991.

Other parts of Cheney's 2000 interview are even pertinent today as the Biden administration is preparing its own Nuclear Posture Review, due in the next few months.

For example, Cheney said, "I'm just trying to recreate in my own mind some of my thinking. In a whole other part of the DoD arena, cruise missile technology, we had developed the capability—with standoff conventional weapons, which we demonstrated conclusively in Iraq [meaning Operation Desert Storm]—that we can go in and hit key nodes and shut down a country, take down the power grid, shut down their transportation system, their telecommunication system, whatever it meant. It meant pinpoint strikes with accurate weapons, ***but a conventional warhead*** [emphasis added]. You give me a few cruise missiles, I can shut down any country in the world for a period of time."

In short, Cheney in 2000 recognized that some, if not many, targets programmed for nuclear weapons could be hit by precision conventional weapons.
I would say almost all could be hit with precision conventional weapons or even taken down with cyber weapons. It's time to see nuclear weapons for what they are – and were back in 1945 – terror weapons to end a war, not to fight one.
Another issue being considered for the Biden Nuclear Posture review is a proposal for the U.S. to adopt a "no first use" policy for its nuclear weapons. The Trump Administration, in the 2018 Nuclear Posture Review, rejected that idea and stated that "the United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners."
Again, I turn to the Miller Center oral histories, this time to James Baker's interview in March 2011 when he talked about his time as Secretary of State in the days before Operation Desert Storm. Baker recalled that before he met with Saddam Hussein's closest advisor, Tariq Aziz in January 1991, the Defense Department, meaning Cheney, told him, Baker, "that if they use weapons of mass destruction on our troops, we would respond," meaning use nuclear weapons.
Baker continued, "And so what I said to the Minister [Aziz] was, Minister, if you use weapons of mass destruction on our forces, the American people will demand revenge, and we have the means to exact it. Then I said, 'That is not a threat, it is a promise.' So, after they captured Saddam and debriefed him, they said, 'Why didn't you use your chemical weapons when the Americans were coming?' And he implied—maybe he didn't say this in so many words, but implied—it was because of what Baker told Aziz at Geneva. So, it [the nuclear threat] was effective."
Baker said, "Based on this real-time example of how such a threat really worked to protect our troops," the Obama 2010 Nuclear Posture Review made a mistake when it said it would only use conventional weapons against a non-nuclear state that employed chemical or biological weapons.
Thus, although the NATO exercise last week tested whether the U.S. and its allies were prepared to use tactical nuclear weapons, it's doubtful any real order to do so will ever occur.
On the other hand, as long as the threat to use nuclear weapons exists, such exercises could, as they have done in the past, help avoid lesser military conflicts between countries that possess them or other weapons of mass destruction.

*Pulitzer Prize Winning Journalist **Walter Pincus** is a contributing senior national security columnist for The Cipher Brief. He spent forty years at The Washington Post, writing on topics from nuclear weapons to politics. He is the author of Blown to Hell: America's Deadly Betrayal of the Marshall Islanders (releasing in November 2021) He also won an Emmy in 1981 and the 2010 Arthur Ross Award from the American Academy for Diplomacy.*

'Nuclear deterrent' is not just a loaded term, but an inaccurate one

Source: https://www.thenational.scot/community/19680337.nuclear-deterrent-not-just-loaded-term-inaccurate-one/

Oct 29 – Kevin McKenna made some excellent points in his article "Brigadier Wallace and his delusion over Russia and independence" (Oct 27). In particular, everyone should adopt his suggested terminology of "nuclear threat" to replace "nuclear deterrent". Mr McKenna is right that this latter term "was coined by apologists of mass destruction to justify spending billions on them."
It is seldom that any Tory or Unionist politician (yes, that includes you, Scottish Labour) mentions the nuclear weapons based in Scotland without using the term "deterrent". This is a positively loaded word, with reassuring implications of defence and balance. Indeed, that term has become so pervasive that even politicians who should, and often do, know better, succumb to using it.
Former Tory defence minister Michael Portillo said that Trident does not constitute a deterrent to any nation or organisation we would regard as a threat. It is a status symbol, a vestige of Britain's imperial power and part of the reason the UK still has a permanent seat on the UN Security Council.

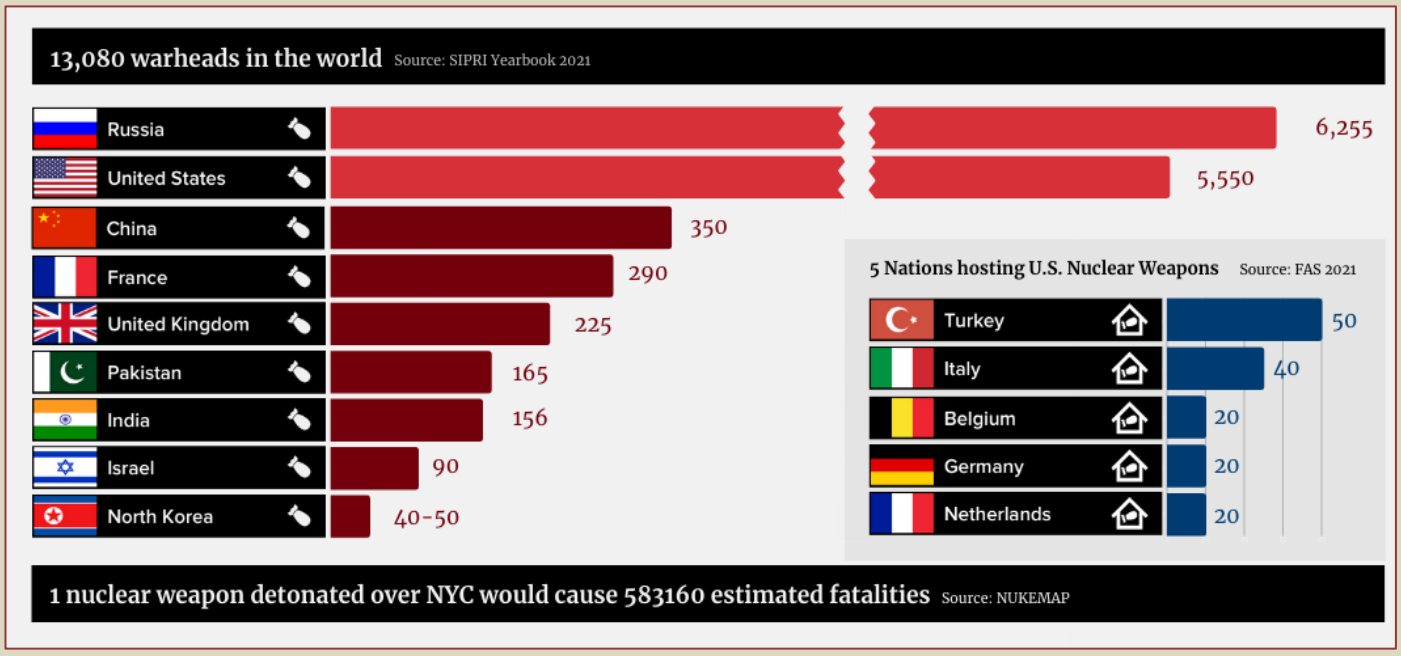
The UK has a Trident arsenal of 200 warheads, each more than six times more powerful than the weapon unleashed on Hiroshima. One submarine typically carries around 40 such warheads, with this total payload being enough to literally wipe out human and most other life on Earth.
Incredibly, the Tories have committed to increase our destructive capability by a further 40 warheads, in contravention of the Nuclear Proliferation Treaty to which the UK is a signatory. Trident is a first-strike weapon of mass destruction, effective against civilian populations in large cities. That is the threat it presents. "If you attack us, you better think about what we can do to you".
"Nuclear threat" deserves general adoption because it not only applies to deployment of these WMDs, but also to the real and ever-present danger of accident, terror and cyber attack that could render much of Scotland uninhabitable. Faslane and Coulport have atrocious safety records, so much so that they stopped publishing annual reports. Only through an FOI request by Deidre Brock MP do we know that there were SIX "radioactive incidents" per MONTH between 2014 and 2017. There are also continuing issues with staffing, discipline and security on the bases.
An independent Scotland can sign and ratify the UN Treaty for Prevention of Nuclear Weapons and have these weapons deactivated and removed. Everyone in Scotland will be immediately more (not less) secure. And to those who cry "The jobs! The jobs!" (yes, this is you, Jackie Baillie) – be assured Scotland will still need the Faslane deep-water naval base, for genuine coastal, fisheries and energy installations security. Not only that, but senior defence jobs will be based here in Scotland, not 400 miles away.

The US nuclear arsenal is becoming more destructive and possibly more risky

By R. Jeffrey Smith
Source: https://publicintegrity.org/national-security/future-of-warfare/nuclear-weapon-arsenal-more-destructive-risky/

Oct 29 – A sophisticated electronic sensor buried in hardened metal shells at the tip of a growing number of America's ballistic missiles reflects a significant achievement in weapons engineering that experts say could help pave the way for reductions in the size of the country's nuclear arsenal but also might create new security perils.
The wires, sensors, batteries, and computing gear now being quietly installed on hundreds of the most powerful U.S. warheads give them an enhanced ability to detonate with what the military considers exquisite timing over some of the world's most challenging targets, substantially increasing the probability that in the event of a major conflict, those targets would be destroyed in a radioactive rain of fire, heat, and unearthly explosive pressures.
The new components — which determine and set the best height for a nuclear blast — are now being paired with other engineering enhancements that collectively increase what military planners refer to as the individual nuclear warheads' "hard target kill capability." This gives them an improved ability to destroy Russian and Chinese nuclear-tipped missiles and command posts in hardened silos or mountain sanctuaries, or to obliterate hardened military command and storage bunkers in North Korea, also considered a potential U.S. nuclear target.
The increased destructiveness of the new warheads means that in some cases fewer weapons could be needed to ensure that all the objectives in the nation's nuclear targeting plans are fully met, opening a path to future shrinkage of the overall arsenal, current and former U.S. officials said in a series of interviews, in which some spoke on condition of anonymity to discuss sensitive technology.
Production of the first of many high-yield nuclear warheads containing the gear, developed over the past decade at a cost of billions of dollars, was completed in July for installation on missiles aboard Navy submarines, the National Nuclear Security Administration announced. It follows the development and installation of similar fuzes — designed by the same nuclear laboratory — on hundreds of smaller-yield submarine warheads in a program completed in January 2019. After the Air Force installs some of the same technology aboard new land-based missiles slated for deployment by the end of the decade, it will be deployed on more than 1,300 warheads in the U.S. arsenal.
The Defense Department has publicly described the components as a routine engineering improvement that provides no substantial new military capabilities. Air Force budget documents provided to Congress describe it as a "form, fit, and functionally equivalent replacement" for existing nuclear warhead fuzes. But those familiar with highly sensitive nuclear planning say it will make the warheads significantly more damaging than previous such weapons.
"It's an astounding piece of technology," said mechanical engineer Paul J. Hommert, who directed the government-owned Sandia National Laboratories during the initial years of the technology's development by a team of several hundred people on its New Mexico campus. He said that while existing U.S. weapons are highly accurate, the sensors the lab created are even better at computing the best moment for a blast to be ignited to produce the highest pressures on targets. They accomplish this even while the warheads approach at speeds that other experts have said exceed 15,682 miles per hour.
"There is more flexibility [in its use] and more robustness," he said. "And that has to lead to sustained confidence and the possibility of additional damage capability." Hommert said he

agreed with others that there are a lot of deeply buried installations, like command posts, that "these will give you a better chance of holding at risk." He called it an "underappreciated" enhancement.
Georgetown University professor Keir Lieber, and Dartmouth University associate professor Daryl Press, a consultant to the Defense Department, have estimated that the fuzes have roughly doubled the destructive power of the U.S. submarine fleet alone.
This shift in weapons capabilities has both military and political consequences, current and former officials and experts said. On one hand, the leaders of target countries, knowing that U.S. nuclear strikes are more certain to be effective in destroying their weapons, might be more deterred from taking provocative actions that could draw a U.S. nuclear attack, some said.
Others worry, however, that those leaders — knowing that many of their protected, land-based weapons and associated command posts could not escape destruction — might be more prone to order their use early in a crisis or conflict, simply to ensure they are not destroyed when incoming warheads arrive, promoting a hair-trigger launch policy that could escalate into a general cataclysm.
Physicist James Acton, who co-directs the nuclear policy program at the Carnegie Endowment for International Peace and has written extensively about the need to avert unnecessary conflicts, said that efforts to modernize the nuclear arsenal should be more focused on ensuring the weapons' safety, security, and reliability, and less on goosing their accuracy.
"If China or Russia believe in a conflict or a crisis that we are going to attack or destroy their nuclear forces and command posts, that gives them an incentive to use nuclear weapons first, or to threaten their use. They have strong incentives to take steps that would further escalate the crisis and create new dangers," Acton said.
Distributing impressive accuracy improvements throughout the U.S. arsenal "will raise concerns in Russia and China about targeting their leadership." He said "I would like to see the United States being more restrained in this," because the additional escalation risks "outweigh a relatively modest increase in utility" against such targets as deeply-buried command posts.
Already, the U.S. can hold at risk many but possibly not all of the key Russian and Chinese targets. "There's an element that exists today" of heightened fear of preemptive attack as a result, said John R. Harvey, a physicist who was the principal deputy to the Defense Department's top nuclear weapons authority from 2009 to 2013 and the director of policy planning at the National Nuclear Security Administration for eight years before that.
But Harvey acknowledged that it's hard to know whether the deployment of additional capabilities to target key enemy warheads will put "the adversary in a posture that would generate a rapid response, which could conceivably be the result of misinterpretation" — a launch of weapons based on the erroneous sensing of an attack or false anxiety about an imminent attack.



Detonating at the optimal second

The warhead fuze and its accompanying sensors and computers are embedded in a stubby capsule about two feet high and a foot wide, compact enough for Hommert to carry a model with him to a congressional hearing in 2014. There he said they would be installed on three new types of warheads atop land and sea-based missiles as well as, in part, a warhead to be carried by U.S. F-16 and F-35 warplanes deployed in Europe.
Hommert and other advocates for the new technology emphasized that by deploying a single new component across the warhead force — a rare exception to the longstanding insistence of the Navy and the Air Force on using unique warhead designs — the

government would save around $170 million. But in practice, the decision to field a common device backfired, when a $5 capacitor in the fuzing system that stores and generates electrical current tested poorly and had to be abruptly replaced by a more expensive device in hundreds of the modules. The resulting production delays set the entire effort back about a year and led to a roughly $750 million hike in its budget.

Widespread installation of the fuzing system nonetheless has aroused little controversy on Capitol Hill, partly because both Democratic and Republican administrations have depicted it as a slight modernization of a single component that they say doesn't violate a 2010 promise by President Barack Obama to foreswear the development of new nuclear weapons or their modification to support new military missions.

It's part of a major, two-decade long effort to modernize major components in five types of existing nuclear warheads at a cost exceeding $40 billion. The government is also simultaneously modernizing virtually all the launchers for these warheads, including key elements in the U.S. missile, bomber, and submarine force, requiring an investment of $634 billion over the next decade and bringing the complete cost of the nuclear arsenal to roughly $1.2 trillion over the next three decades.

Officials say the ambition of the Sandia team was partly to make the fuze of U.S. warheads more resilient in the face of electronic jamming efforts (typically aimed at making a fuze malfunction or detonate too early) and in the midst of high radiation levels caused by other nuclear blasts, including those deliberately set off by Russia at an altitude of about 30 miles over key command centers as part of that country's brutalist missile defense system.

But another aim was to ensure that warheads arriving from varied angles could more assuredly obliterate their targets even if their prospective landing points were slightly off-center.

Older warheads set to detonate when they hit the ground, using a contact fuze, or those that used a less advanced radar or barometric fuze to ignite it at a pre-set altitude were not as assuredly able to destroy all hardened targets, says Theodore Postol, a professor emeritus of science, technology and national security policy from MIT and former consultant to the chief of naval operations on warhead engineering. Bursts too close to the ground or on it also caused higher radioactive fallout and more collateral damage.

"The new radar has the ability to measure the altitude within a few meters of precision" and "can tell you whether you are on the right trajectory" by sensing terrain features. Taking into consideration winds, gravitational forces, and other sensitive flight characteristics, it senses how far off the warhead might land and compensates by adjusting the burst height to maintain the maximum possible force on the target, he said.

Several experts said that enabling the warheads to determine their location while traveling at blinding speed and in milliseconds calculate the right moment to ignite proved a solvable problem with advanced electronics and a team working for a decade with what Sandia boasts is "some of the best tools, equipment and research facilities in the world."

Citing the sensitive nature of the technology in the assembly, the lab declined to make a member of its staff available to discuss it; nor would the National Nuclear Security Administration in Washington, which funded the work. But a Sandia employee overseeing the work, Dolores Sanchez, was quoted in a lab publication in August describing the assembly as "the brains of the warhead. … It looks for the correct code and the correct environmental signals that will unlock the system, and it also ensures that it's an authorized flight. In short, it makes sure it always works when we want it to and never when we don't."

The lab's news release explained further that it was "more than a decade in the making" and that it required multiple tests of the fuze's vulnerability to "impact, vibration, drops, extreme temperatures and massive electrical impulses." Sandia's design was subsequently turned into hardware by Honeywell, which not only manages the lab but operates the federally-owned nuclear weapons production facility in Kansas City that's churning out hundreds of the new systems.

One of the aircraft-delivered warheads that incorporates the fuzing system's new radar and a new, maneuverable tailkit, the B61-12, will be considerably more accurate than its predecessors but have a lower explosive force, producing somewhat less radioactive fallout and destruction outside the vicinity of the target. Both of the submarine-based warheads with the parts of the new fuzing and firing gear, the W76-1 and W88 Alt 370, are also meant to be more destructive, a circumstance that affords the submarines' commanders more latitude to station their vessels in a broader ocean area and launch their missiles toward their targets along more varied trajectories, officials say.

Hans Kristensen, who monitors such technological efforts for the Federation of American Scientists, a nonprofit group in Washington, says that the warhead improvements in total look uncomfortably like new designs. He says in some ways this is not surprising: As the U.S. arsenal has shrunk by roughly a third due to arms agreements struck in the past two decades, "the engineers and weaponeers began looking for ways to enhance the capabilities of the weapons that would be left." And the results, he said, "are so far removed from the Obama era's limitation that [they are] one step short of a new nuclear weapon."

Building weapons like the B-61 that are more accurate and destructive while producing lower collateral damage "makes them easier to use, [and] this is completely accepted now" as a reasonable ambition for weapons designers, Kristensen complained. The issue has been hotly debated, however. Don Cook, who helped oversee nuclear weapons production efforts during the Obama administration, wrote in 2016 that "I believe, a lower-yield, more accurate

U.S. weapon constitutes a better deterrent specifically because it will be regarded by an adversary as more usable and that the likelihood of weapons use is, therefore, lower, not higher."

A new path to nuclear reductions?

Arms reduction agreements between the United States and Russia have typically measured the relative military might of both nations by the numbers of nuclear weapons they held, not how destructive the weapons were. The most recent one, known as New START — a deal that came into force in 2011 and was recently extended until 2026 by President Joe Biden and Russian President Vladimir Putin, limited each nation to 1,550 warheads (the actual numbers are higher because bombers carrying many warheads are counted as carrying one).

But **Navy Admiral Charles A. Richard**, who commands the U.S. Strategic Command that stewards the nuclear arsenal, told the House Armed Services Committee last April that "the size of a nation's weapons stockpile is a crude measure of its overall strategic capabilities. … It is necessary to consider the capability, range, and accuracy of the associated delivery systems."

Richard's words were intended to rebut any claims that China's nuclear arsenal — which has an estimated 350 warheads, or less than a tenth of those deployed and stored by U.S. forces — poses a comparatively small threat to America. "I have no choice but to view China as a significant strategic nuclear threat," Richards said.

But other experts say the same conclusions can be drawn from the improved capabilities of the U.S. force. Their enhanced nuclear killing power justifies taking a look at the plan to spend a trillion dollars on its modernization, operation and maintenance, or the need to keep so many warheads in the stockpile, they say.

The fuze will be "more reliable, almost certainly," said Michael Elliott, a former nuclear bomber weapons system officer who was deputy director of strategic stability for the Joint Chiefs of Staff while the New START treaty was negotiated and previously worked on nuclear plans for the U.S. Strategic Command. "When you improve reliability, you improve effectiveness, and that drives up the probability of success," which could mean that "fewer warheads are needed," including fewer required in a stockpile reserve that others say presently has 2,000 warheads. But Elliott added that any decision to reduce warheads should also be based on "the projected strategic situation and health of our forces."

"Our hard-target kill capability was good before, but it's great now," said Jon Wolfsthal, a key White House adviser on arms control and nuclear issues when Biden was vice president. He said this enhancement had already helped convince the Pentagon's military leaders to agree that the nuclear force could be smaller than it was then and is now.

President Obama made this verdict public in June 2013 after a comprehensive classified review, through a statement affirming that even after the New START limitations were fully met, "we can ensure the security of the United States and our allies and partners and maintain a strong and credible strategic deterrent while safely pursuing up to a one-third reduction in deployed nuclear weapons" beyond what that treaty required.

Wolfsthal, who is now a senior adviser to the Global Zero advocacy group, which seeks the eventual elimination of nuclear arms, said the military's support for this reduction of a third — or about 500 warheads — from the current arsenal wasn't conditioned during the Obama administration's review on a requirement for similar reductions to be taken by Russia, but was decided instead based on an assessment of what the country needed to be able to hold key Russian targets at risk. He and others explained that this was determined in part by a recognition that the American arsenal was becoming more accurate and in part by the fact that the total number of targets that America needed to destroy in Russia had declined.

Wolfsthal said that in his view the reason Obama didn't implement these approved reductions was political, rather than military. Obama and Biden, he said, opposed taking action unilaterally because they hoped to persuade Russia to act similarly, contributing to an overall reduction in global nuclear risks. He said he thought it was "crazy" to be spending so much on new weapons when "we could live with a smaller force."

So far, the Biden administration has said little about its larger plans for the nuclear arsenal besides affirming in budget plans that it intends no major change in the modernization programs created by Obama and continued or slightly expanded by President Donald Trump. An internal administration review of the nation's nuclear posture is just getting under way at the Pentagon, and its leadership changed, drawing expressions of concern from arms control advocates.

Leonor Tomero, a comparatively independent-minded veteran of nuclear oversight on Capitol Hill who Biden had appointed early this year as the deputy policy chief for nuclear matters, was relieved of responsibility for the review and it was handed off to another defense official working in an acting capacity.

While the administration described the resulting personnel change as a simple interoffice reorganization, Sen. Ed Markey, D-Mass., said in a Sept. 24 letter to Biden that he was "concerned that the sudden departure of a top appointee, charged with presenting you

options on the future of the U.S. nuclear weapons enterprise, will result in a draft Nuclear Posture Review that reflects the Cold War era's overreliance on nuclear weapons."
Any prospect of changing paths indeed feels alarming to some. Richard, the Strategic Command commander, told reporters in January that the upcoming review should include "validation that we like the strategy that we have. … And then to be satisfied that the [nuclear weapons] capabilities that we have are able to accomplish that."
But Andrew Weber, the assistant secretary of defense for nuclear, chemical, and biological defense programs from 2009 to 2014 and chair of the Nuclear Weapons Council that approved development of the fuzes, said that in his view their deployment reduces the need to keep developing some smaller nuclear weapons slated for deployment in the next decade.
New air- and sea-launched cruise missiles in particular, he said, are not necessary, and will undermine deterrence because they are stealthy, surprise-attack weapons that will make opponents nervous enough to adopt hair-trigger launch policies. Since they can be deployed with both conventional and nuclear warheads and it's impossible for opponents to tell the difference, their use could cause unintentional escalation from a conventional to a nuclear war.Those two programs are estimated to cost more than $35 billion. It's time, Weber said, to stop "replacing everything mindlessly."

Plutonium is missing, but the government says nothing

By Patrick Malone and R. Jeffrey Smith
Source: https://publicintegrity.org/national-security/plutonium-is-missing-but-the-government-says-nothing/

July 2018 – Two security experts from the Department of Energy's Idaho National Laboratory drove to San Antonio, Texas, in March 2017 with a sensitive mission: to retrieve dangerous nuclear materials from a nonprofit research lab there.
Their task, according to documents and interviews, was to ensure that the radioactive materials did not fall into the wrong hands on the way back to Idaho, where the government maintains a stockpile of nuclear explosive materials for the military and others.
To ensure they got the right items, the specialists from Idaho brought radiation detectors and small samples of dangerous materials to calibrate them: specifically, a plastic-covered disk of plutonium, a material that can be used to fuel nuclear weapons, and another of cesium, a highly radioactive isotope that could potentially be used in a so-called "dirty" radioactive bomb.
But when they stopped at a Marriott hotel just off Highway 410, in a high-crime neighborhood filled with temp agencies and ranch homes, they left those sensors on the back seat of their rented Ford Expedition. When they awoke the next morning, the window had been smashed and the special valises holding these sensors and nuclear materials had vanished.
More than a year later, state and federal officials don't know where the plutonium – one of the most valuable and dangerous substances on earth – is. Nor has the cesium been recovered.
No public announcement of the March 21 incident has been made by either the San Antonio police or by the FBI, which the police consulted by telephone. When asked, officials at the lab and in San Antonio declined to say exactly how much plutonium and cesium were missing. But Idaho lab spokeswoman Sarah Neumann said the plutonium in particular wasn't enough to be fashioned into a nuclear bomb.
It is nonetheless now part of a much larger amount of plutonium that over the years has gone quietly missing from stockpiles owned by the U.S. military, often without any public notice.
Unlike civilian stocks, which are closely monitored by the Nuclear Regulatory Commission and openly regulated – with reports of thefts or disappearances sent to an international agency in Vienna — the handling of military stocks tended by the Department of Energy is much less transparent.
The Energy Department, which declined comment for this story, doesn't talk about instances of lost and stolen nuclear material produced for the military. It also has been less willing than the commission to punish its contractors when they lose track of such material, several incidents suggest.
That nontransparent approach doesn't match the government's rhetoric.
Protecting bomb-usable materials, like the plutonium that went missing in San Antonio, "is an overriding national priority," President Obama's press office said in a fact sheet distributed during the fourth and final Nuclear Security Summit that he hosted in late March 2016, a Washington event attended by more than 50 heads of state.
The administration boasted in the declaration that America's security standards for military-grade materials "meet or exceed the recommendations for civilian nuclear materials" made by the Vienna-based International Atomic Energy Agency. It also touted the strength of its tracking of such materials, which it said would "ensure timely detection and investigation of anomalies, and deter insider theft/diversion."
The United States also boasted about its transparency, explaining that it "has published studies and reviews of nuclear security incidents, including lessons learned and corrective actions taken."

President Donald Trump, speaking to a military audience at Fort Myer in Arlington, Virginia, on Aug. 21, 2017, parroted the Obama administration's refrain that "we must prevent nuclear weapons and materials from coming into the hands of terrorists and being used against us, or anywhere in the world for that matter."
The Trump administration's Nuclear Posture Review, released in February, similarly emphasized the threat posed by nuclear terrorism, and asserted that "preventing the illicit acquisition of a nuclear weapon, nuclear materials, or related technology and expertise by a violent extremist organization is a significant U.S. national security priority."
But America's record of safeguarding such materials isn't sterling. Gaps between the amount of plutonium that nuclear weapons companies have produced and the amount that the government can actually locate occur frequently enough for officials to have created an acronym for it – MUF, meaning "material unaccounted for."

Just a cat or a brick

The gaps have shown up at multiple nodes in the production and deployment cycle for nuclear arms: at factories where plutonium and highly-enriched uranium have been made, at storage sites where the materials are held in reserve, at research centers where the materials are loaned for study, at waste sites where they are disposed, and during transit between many of these facilities.
Production of the bomb materials was so frantic during the Cold War that a total of roughly six tons of the material – enough to fuel hundreds of nuclear explosives – has been declared as MUF by the government, with most of it presumed to have been trapped in factory pipes, filters, and machines, or improperly logged in paperwork. (That figure, which dates from 2012, has not been publicly updated.)
For nearly 40 years, "DOE officials and their predecessors … did not have an effective capability within their accounting systems to know if significant quantities of" bomb-grade uranium were being diverted to illicit use, according to Charles Ferguson, a physicist who is now director of the Nuclear and Radiation Studies Board at the National Academies of Sciences.
The Government Accountability Office declared in Sept. 2015 that the department also had never conducted an authoritative inventory of the location and quantity of plutonium loaned by the United States to other nations, and that eleven foreign sites with U.S.-made bomb-grade uranium had not been visited by U.S. inspectors in the previous 20 years. Many sites inspected before 2010 lacked rigorous security systems, the GAO warned.
Asked for comment, National Nuclear Security Administration spokesman Greg Wolfe said in an email on June 29 that his agency is still working with DOE on that inventory, three years later. He did not say when it would be finished.
Regarding transfers to academic researchers, government agencies, or commercial firms within the United States, the Energy Department's inspector general concluded in 2009 –the most recent public accounting – that at least a pound of plutonium and 45 pounds of highly-enriched uranium loaned from military stocks had been officially listed until 2004 as securely stored, when in fact it was missing.
As little as nine pounds of highly-enriched uranium (the weight of an average cat) or 7 pounds of plutonium (the weight of a brick) can produce a functioning nuclear warhead, according to Hans Kristensen, director of the Nuclear Information Project at the Federation of American Scientists. So the missing amount in this category alone — the MUF stemming from loans to researchers from military stocks — is still enough to produce at least five nuclear bombs comparable to those that obliterated Hiroshima and Nagasaki, experts say. Plutonium in any quantity is also highly carcinogenic.
"Considering the potential health risks associated with these materials and the potential for misuse should they fall into the wrong hands, the quantities written off were significant," the inspector general's report stated. It also harshly criticized the Energy Department for failing to correct dozens of poor accounting and monitoring practices flagged in a probe of the problem eight years earlier.The Energy Department, the inspector general said in its report, still "may be unable to detect lost or stolen material." No independent probe of the department's capabilities has been conducted since then. When asked whether the GAO conclusions were still valid, a spokesman for the department did not respond.

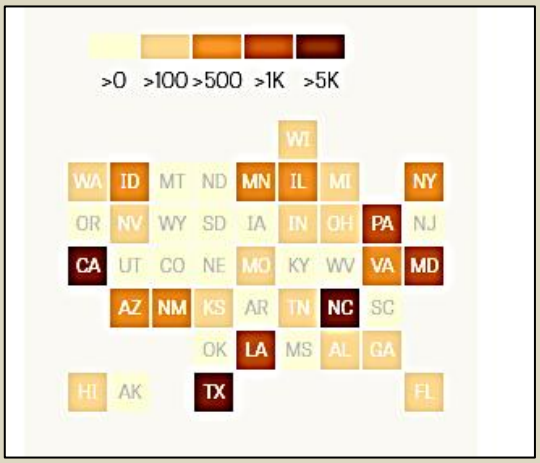
Russians know even less about their own missing bomb materials

The United States is not alone in its uncertainty about the location of bomb-usable materials. U.S. officials who have studied Russia's production practices say its accounting system has many of the shortcomings that America's had, if not more, partly because the Russian factory logbooks were routinely jiggered to match official state production quotas.
Russia hasn't tried to look more deeply into these records to assess the actual quantities of material it produced and can locate now, and thus the size of its own MUF. More than a decade ago, according to U.S. experts, some of its top physicists turned aside efforts by specialists in the United States to collaborate on a study of it. The U.S. National Intelligence Council has repeatedly said that Russian accounting was so poor that undetected smuggling likely occurred.
The details of how or why U.S. nuclear materials go missing from military stocks – or the quantity of such materials involved in individual incidents — are not disclosed by the

government. But the Nuclear Regulatory Commission annually publishes a tally of lost, missing or stolen radioactive material from civilian nuclear stocks (those typically used for oil and gas exploration, medical purposes, academic research and nuclear power).
In a Jan. 2018 report, for example, the NRC stated during the previous year, eight such items had gone missing and two had not been recovered. None were of the type or quantity useable in a nuclear weapon. Whenever additional material goes missing, the NRC discloses it publicly.
The Nuclear Threat Initiative, a nonprofit Washington group that wants to tighten the security of nuclear materials around the globe, noted in a 2015 report that the civilian stocks subject to the most transparent and uniform monitoring amount to just 17 percent of all those held by governments. "The absence of any international standards" for securing and monitoring the remaining 83 percent in military hands is dangerous, the group said.
Concern that nuclear materials are being sought around the world to deliberately cause harm is real, according to the International Atomic Energy Agency. In a 2017 report, the international agency identified 270 times between 1993 and 2016 when individuals acquired nuclear materials "for trafficking or malicious use." Twelve involved highly-enriched uranium, and two targeted plutonium. Some of these cases were "more organized, better resourced and … involved perpetrators with a track record in trafficking nuclear/radioactive material," the report said.

Incidents related to trafficking or malicious use, 1993-2016

Over the past quarter century the International Atomic Energy Agency, which tracks and monitors bomb-useable material across the globe, uncovered 270 times when someone tried or succeeded to get such materials with 'malicious intent.' As of 2016, the last year of available data, these nefarious activities constitute 9 percent of all incidents tracked by the agency. The IAEA reports the incidents include a range of quantities and the problem persists even today.



Radioactive material recoveries

The National Nuclear Security Administration's Off-Site Radioactive Source Recovery Program has scooped up more than 38,000 bits of radioactive material loaned to research centers, hospitals and academic institutions since 1999. More orphaned sources have been collected in Texas than in any other state.

Sloppiness in transit

Ensuring appropriate protections are in place for military-related nuclear materials has ironically proven a lot harder than implementing tight security for civilian nuclear materials, said Miles Pomper, a senior research associate at the James Martin Center for Nonproliferation Studies in Monterey, California, who participated in the NTI study. "Politically and diplomatically, it's a lot more difficult," Pomper said. "We're not having significant conversations on this issue."
In the San Antonio incident, the San Antonio police were dumbfounded that the experts from Idaho did not take more precautions. They "should have never left a sensitive instrument like this unattended in a vehicle," said Carlos Ortiz, spokesman for the San Antonio Police Department.
The personnel from Idaho National Laboratory whose gear was stolen were part of the Off-Site Radioactive Source Recovery Program based at Los Alamos National Laboratory in New Mexico, with an annual budget of about $17 million. Overseen by the National Nuclear Security Administration, the program has scooped up more than 38,000 bits of radioactive material loaned to research centers, hospitals and academic institutions since 1999 – averaging 70 such missions a year. No state has returned more borrowed nuclear materials than Texas, where the recovery program has collected 8,566 items.
Details of the incident were pieced together by the Center for Public Integrity from a police report obtained under a Freedom of Information Act request after a brief description of the incident appeared in an internal Energy Department report.
While the Idaho National Laboratory depicted the site of the theft – a Marriott hotel parking lot -- in a report to the Energy Department as a secure spot with high walls on two sides, a clear line of sight to the hotel's front door, and patrolling guards, San Antonio police statistics show that theft was just one of 87 at the Marriott hotel or its parking lot in 2016 and 2017.
Ortiz said the department called an FBI liaison to a joint terrorism taskforce, who advised them to take as many fingerprints in the car as possible. But detectives found no useable prints, no worthwhile surveillance video of the crime, and no witnesses. A check of local pawn shops – to see if someone had tried to sell the sensors – turned up nothing.

One of the Idaho National Laboratory specialists told them, Ortiz said, "that it wasn't an important or dangerous amount" of plutonium. So they closed the investigation to avoid "chasing a ghost," Ortiz said.
Idaho National Laboratory spokeswoman Sarah Neumann responded that "from INL's perspective, the theft was taken seriously" and properly reported to the police and the Energy Department. But she declined to say if those involved faced any internal consequences. "There is little or no danger from these sources being in the public domain," she said.
Lab documents state that a month after the incident, one of the specialists charged with safeguarding the equipment in San Antonio was given a "Vision Award" by her colleagues. "Their achievements, and those of their colleagues at the laboratory, are the reasons our fellow citizens look to INL to resolve the nation's big energy and security challenges," Mark Peters, the lab director, said in an April 21, 2017, news release.
At the end of the fiscal year 2017, the Energy Department awarded the lab contractor that employed the guards assigned to pick up the nuclear material, Battelle Energy Alliance LLC, an "A" grade and described their overall performance as "excellent." It further awarded them 97 percent of their available bonuses, providing $15.5 million in profit, and in December 2017 the Department of Energy announced a five-year extension of Battelle's contract to operate Idaho National Laboratory, giving the contractor the job until at least 2024.
The NRC, in contrast, has imposed six financial penalties on civilian institutions that lost or mishandled nuclear materials in the past year and a half alone (it has imposed and then waived penalties on another 20 institutions during this period). The largest penalty imposed was $22,500 against Qal-Tek Associates, a radiation detector manufacturer in Idaho Falls, for failing to "contain" radioactive materials during their transport, according to a published notice of the fine.
The most recent NRC fine was imposed this May against Idaho State University for its inability to find a quarter-sized piece of plutonium in a radiation meter that it had borrowed from Idaho National Laboratory in 1991. An Idaho State University employee conducting an inventory of such materials last October expected to find 14 of the Plutonium-239 pieces, each weighing less than four-hundredths of an ounce, but found just 13. The inspector reported this discrepancy to the university's radiation safety officer, who in turn reported it to the NRC.
The NRC imposed fines totaling $8,500 for the college's mishandling of the plutonium, and the years-long delay in reporting it missing. Idaho State University paid the fines June 6, according to Cornelis Van der Schyf, the university's vice president for research and dean of the graduate school. The missing plutonium's whereabouts remain unknown.

***(Update: July 20, 2018, 1:30 pm:** In a letter to Energy Secretary Rick Perry following publication of this article, Rep. Joaquin Castro (D-Texas), who represents San Antonio, expressed concern about the missing radioactive materials and asked Perry to explain why the public was not notified when the theft occurred. He also asked Perry to detail any other such incidents in Texas over the past five years, asked for a personal briefing on the problem, and said he hopes Perry takes seriously "a culture of nuclear security and prudence.")*

EDITOR'S COMMENT: A 2021 Internet search about the fait of the stollen plutonium revealed nothing; most probably it was never recovered and is still an orphan source.

Incident reported in an unfinished nuclear plant in Turkey

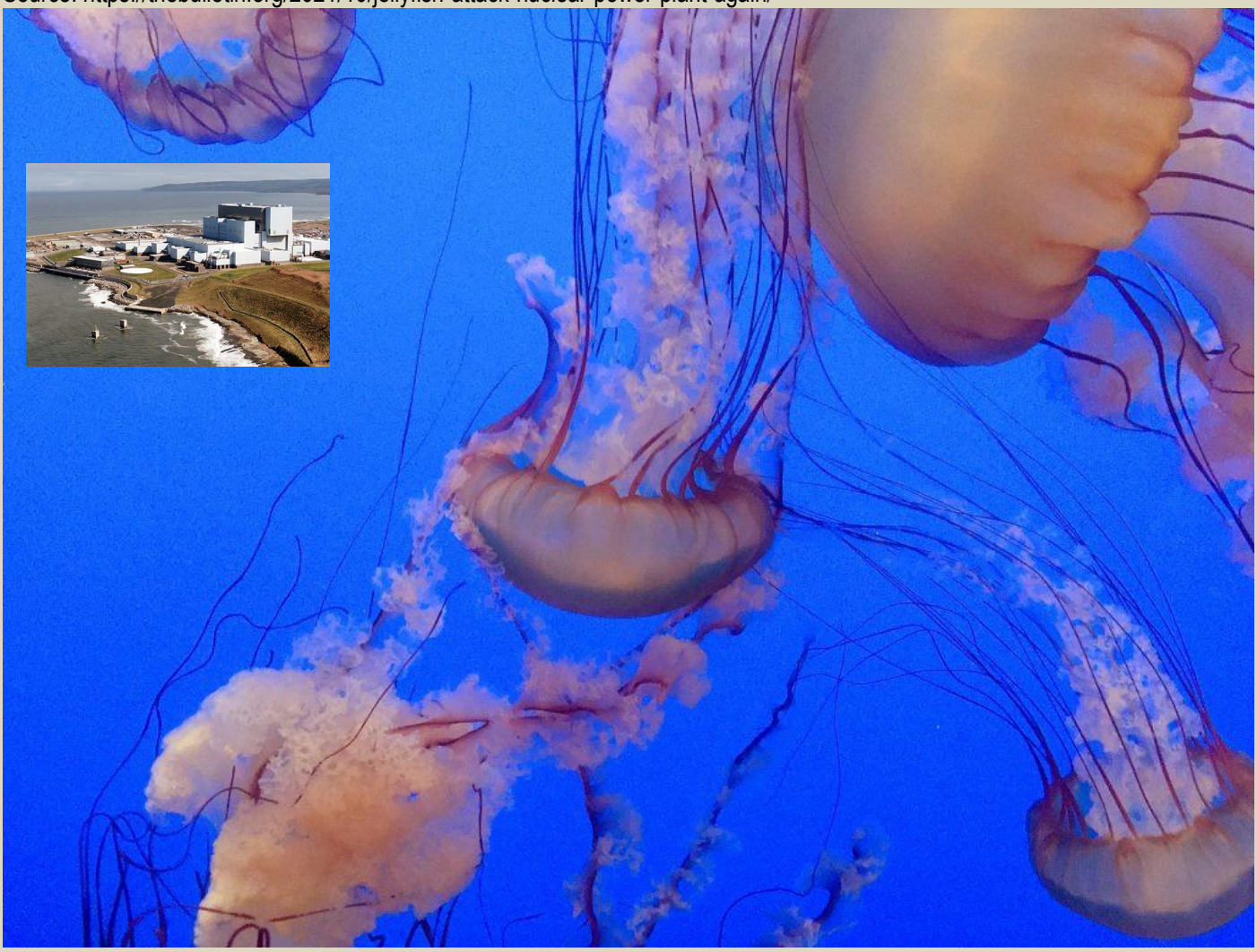
Source: https://en.mehrnews.com/news/180235/Incident-reported-in-an-unfinished-nuclear-plant-in-Turkey

Oct 31 – Turkish local media reported an incident at the Akkuyu Nuclear Power Plant, which is still under construction in Mersin in southern Turkey.
An incident has been reported at the Akkuyu Nuclear Power Plant, which is still under construction in Mersin in southern Turkey, "cumhuriyet" daily reported on Sunday.
"The construction of a Turkish nuclear power plant in Mersin has been a disaster for Turkey and Mersin," said Ali Mahir Başarır a member of the Turkish parliament's commission from the Republican People's Party (CHP) about the incident.
A small fire broke out after an explosion at an electric transformer and caused panic among the workers and the people in the area.

"Now there is a fire in the transformer. As I have said before, with this nuclear power plant, they are placing dynamite in Mersin, beneath the Mediterranean," the MP said.
He also noted that the Turks are building the nuclear plant in cooperation with the Russians while they still have **not decided what to do with the nuclear waste.**

Jellyfish attack nuclear power plants. Again and again.

By Susan D'Agostino
Source: https://thebulletin.org/2021/10/jellyfish-attack-nuclear-power-plant-again/



Sea nettle jellyfish swimming at Monterey Bay Aquarium in Monterey, CA. Credit: Photollama. Accessed via Wikimedia Commons. CC BY-SA 4.0.

Scotland's only working nuclear power plant at Torness shut down in an emergency procedure when jellyfish clogged the sea water-cooling intake pipes at the plant, according to the *Scotland Herald* this week. Without access to cool water, a nuclear power plant risks overheating. The intake pipes can also be damaged, which disrupts power generation. And ocean life that gets sucked into a power plant's intake pipes risks death.
The threat these gelatinous, pulsating, umbrella-shaped marine animals pose to nuclear power plants is neither new nor unknown. (Indeed, the *Bulletin* reported on this threat in 2015.) Nuclear power plant closures—even temporary ones—are expensive. To protect marine life and avert power plant closures, scientists are exploring early warning system options. For example, researchers at Cranfield University in the United Kingdom launched a project earlier this year to determine whether drones may be used to provide estimates of jellyfish locations, amounts, and density.

"The successful operation of [beyond visual line of sight drones] will enable us to detect threats from marine ingress at an earlier state and prevent disruption to the power plant," Monica Rivas Casado, a senior lecturer in environmental monitoring at Cranfield, said. In the United Kingdom, 20 percent of electricity is nuclear, a percentage roughly equaled in the United States, compared with approximately 10 percent globally.

Blooms of translucent jellyfish with their trailing, stinging tentacles are sometimes described as "invasions" because they often emerge en masse in way that appears sudden. Still, determined observers may find early clues of a jellyfish bloom. Spotting jellyfish swarms by way of drones requires balancing recognition accuracy with recognition speed—at least if the goal is to take preventative action to avoid nuclear power plant disruption. Scientists have been at work developing algorithms that foster this balance, including one study that delivered results within a desirable timeframe and over 90 percent accuracy.

In another early-detection effort, scientists have investigated the potential for acoustic characteristics of these sea creatures to detect their numbers, density, and threat level. The creatures' underwater undulations create sounds—known as "echo energy" or "acoustic scatterings"—that give them away, as long as humans are willing to listen.

The clash between gelatinous jellyfish and hulking nuclear power plants has a long history. These spineless, brainless, bloodless creatures shut down the Torness nuclear power plant in 2011 at a **cost of approximately $1.5 million per day**, according to one estimate. Swarms of these invertebrates have also been responsible for nuclear power plant shutdowns in Israel, Japan, the United States, the Philippines, South Korea, and Sweden.

Humans have unwittingly nurtured the adversarial relationship between jellyfish and nuclear power plants. That is, human-induced climate change has raised ocean water temperatures, setting conditions for larger-than-usual jellyfish populations. Further, the relatively warm water near nuclear power plant discharge outlets may attract jellyfish swarms, according to one study. Also, pollution has lowered oxygen levels in sea water, which jellyfish tolerate more than other marine animals, leading to their proliferation.

Some look at jellyfish and see elegant ballerinas of the sea, while others view them as pests. Either way, they are nothing if not resilient. Jellyfish are 95 percent water, drift in topical waters and the Arctic Ocean, and thrive in the ocean's bottom as well as on its surface. Nuclear power plant operators might take note: Older-than-dinosaur jellyfish are likely here to stay.

Susan D'Agostino *is an associate editor at the* Bulletin of the Atomic Scientists. *Her writing has been published in* The Atlantic, Quanta Magazine, Scientific American, The Washington Post, BBC Science Focus, Wired, Nature, Financial Times, Undark Magazine, Discover, Slate, The Chronicle of Higher Education, *and others. Susan is the author and illustrator of* How To Free Your Inner Mathematician: Notes on Mathematics and Life *(Oxford University Press, 2020). She is a member of the editorial board of the Mathematical Association of America's* Math Horizons *magazine. Susan earned a PhD in mathematics at Dartmouth College and an MA in science writing at Johns Hopkins University. She has received science writing fellowships from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.*

The untold story of the world's biggest nuclear bomb

By Alex Wellerstein

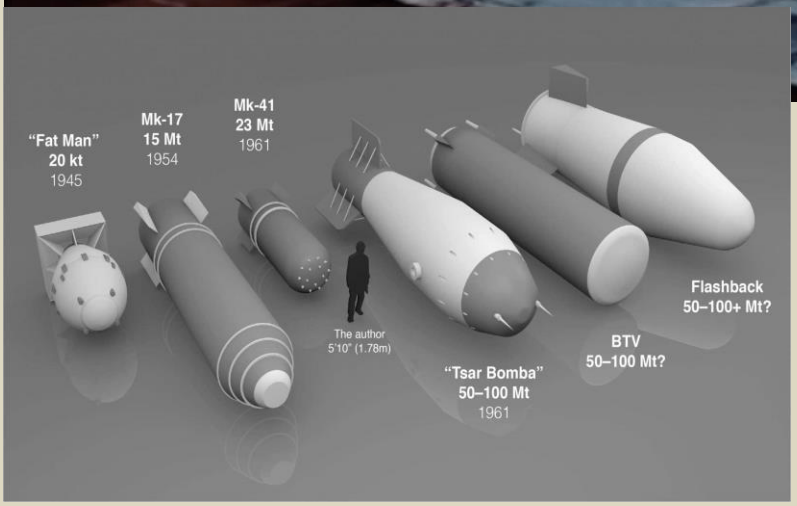
Source: https://thebulletin.org/2021/10/the-untold-story-of-the-worlds-biggest-nuclear-bomb/

Oct 29 – In the early hours of October 30, 1961, a bomber took off from an airstrip in northern Russia and began its flight through cloudy skies over the frigid Arctic island of Novaya Zemlya. Slung below the plane's belly was a nuclear bomb the size of a small school bus—the largest and most powerful bomb ever created.

At 11:32 a.m., the bombardier released the weapon. As the bomb fell, an enormous parachute unfurled to slow its descent, giving the pilot time to retreat to a safe distance. A minute or so later, the bomb detonated. A cameraman watching from the island recalled:

A fire-red ball of enormous size rose and grew. It grew larger and larger, and when it reached enormous size, it went up. Behind it, like a funnel, the whole earth seemed to be drawn in. The sight was fantastic, unreal, and the fireball looked like some other planet. It was an unearthly spectacle!

The flash alone lasted more than a minute. The fireball expanded to nearly six miles in diameter—large enough to include the entire urban core of Washington or San Francisco, or all of midtown and downtown Manhattan. Over several minutes it rose and mushroomed into a massive cloud. Within ten minutes, it had reached a height of 42 miles and a diameter of some 60 miles. One civilian witness remarked that it was "as if the Earth was killed." Decades later, the weapon would be given the name it is most commonly known by today: Tsar Bomba, meaning "emperor bomb."



▶▶ **Read the full article at the source's URL.**

Alex Wellerstein *is an Associate Professor and Director of the Science and Technology Studies program at the Stevens Institute of Technology. His first book,* Restricted Data: The History of Nuclear Secrecy in the United States, *was published by the University of Chicago Press in April 2021.*

American humor!

US nuclear submarine hit an underwater mountain, not another ship, in the South China Sea last month

Source: https://www.scmp.com/news/world/united-states-canada/article/3154508/us-nuclear-submarine-hit-underwater-mountain-not

The Seawolf-class fast-attack submarine USS Connecticut (Photo: US Navy via AP)

Nov 01 – A US Navy nuclear submarine that was severely damaged in an accident while submerged in the South China Sea last month **struck an uncharted underwater seamount**, the US Navy said Monday.

The US 7th Fleet, which operates in the western Pacific, said an investigation had concluded that the USS Connecticut smashed into a geological formation and not another vessel on October 2.

"The investigation determined USS Connecticut grounded on an uncharted seamount while operating in international waters in the Indo-Pacific region," a 7th Fleet spokesperson said in an emailed statement.

The conclusions of the probe have been handed over to Vice-Admiral Karl Thomas, the commander of the US 7th Fleet, to "determine whether follow-on actions, including accountability, are appropriate", they said.

The US Navy confirmed the incident a week after it took place, only saying that Connecticut, a nuclear-powered fast-attack submarine, "struck an object while submerged".

USNI News, published by the US Naval Institute, a think tank close to the Navy, reported that there were some moderate and minor injuries in the accident.

It said the crash damaged the sub's forward ballast tanks and forced it to sail on the surface for a week back to Guam for repairs.

The ship's nuclear plant was not damaged, the publication said.

EDITOR'S COMMENT: Perhaps a window with a strong LED headlight and a navigator set in the bow of the submarine will help avoid future accidents with erupting sea mountains!

What's known—and not known—about India's nuclear weapons budget

By Urvashi Sarkar

Source: https://thebulletin.org/2021/11/whats-known-and-not-known-about-indias-nuclear-weapons-budget/

Indian Prime Minister Modi addresses the crew of INS Arihant. Accessed via Wikimedia Commons. Credit: Prime Minister's Office. Copyrighted work of the Government of India, licensed under the Government Open Data License – India (GODL).

Nov 02 – In 2016, India inducted its first nuclear-powered ballistic missile submarine, the INS Arihant, into its navy, extending nuclear military capabilities from land and air to the sea. "Arihant" translates to "destroyer of the enemy," a name chosen for its "subtlety and appropriateness." A year after Arihant's induction, the vehicle reportedly suffered damage, prompting a member of Parliament to ask about the cost of repairs. A defense minister responded, "The information cannot be divulged in the interest of National Security."

In India, acute poverty persists against a backdrop of urgent development priorities that jostle for financial resources. Meanwhile, India's lack of transparency around nuclear weapon expenditures—including the government agencies responsible for approval, spending, and audits of those expenditures—carries on. Indian taxpayers deserve to know how much their government spends on nuclear weapons, particularly compared to spending on education and health. Also, transparency on nuclear weapons expenditures would signal to the world that India's claimed commitment to disarmament is not empty talk.

Indian government secrecy on nuclear defense systems costs is not new. In 2001, for example, the government declined to say how much it paid for multirole fighter aircraft, citing a confidentiality clause in the contract. More recently, the Indian government refused to divulge expenditures incurred in developing and testing an interceptor ballistic missile, leasing submarines from Russia, or developing a land-based ballistic missile known as Prithvi-II.

"There is a now a culture of not asking questions on issues which the government categorises as national security," said Venkatesh Nayak, an activist who has filed several right-to-information requests with the Indian government. India's equivalent of the US Freedom of Information Act, the Right to Information Act has been a great source of information about many government and private programs in India—excepting those run by nuclear agencies.

Government agencies that focus on nuclear weapons often omit the word "nuclear" from their websites and reports. Instead, they say that nuclear weapons are "strategic." Terms like "strategic forces," "strategic purposes," and "strategic weapons" obfuscate meaning. India's Strategic Forces Command, responsible for procuring, holding, and maintaining the country's nuclear weapons, was recently added to a list of intelligence and security organizations exempt from the Right to Information Act.

Sparse information about Indian nuclear weapon expenditures

When the Indian government divulges information on nuclear costs, it does so sparingly. In 2010, for example, the government stated the cost of test firing Dhanush, a nuclear-capable ballistic missile, was 110 million Indian rupees ($1.46 million). In 2013, the Indian Parliament was informed that the cost of upgrading a Mirage-2000 fighter aircraft was 1.67 billion Indian rupees ($22.27 million) per aircraft. The cost of INS Arihant was $2.9 billion, at least according to one media report, but the figure's source and cost breakdown were unclear.

One comprehensive attempt at trying to understand costs of India's nuclear weapons program was undertaken by economist C. Rammanohar Reddy in 2003. Based on piecing together the scarce data and drawing heavily on a 1998 cost estimate of the US nuclear weapons program, Reddy estimated that India would spend approximately 0.5 percent or more of its gross domestic product on nuclear weapons over the decade that followed. This cost estimate included expenditures on fissile material for bombs, delivery systems, and command and control infrastructure. To estimate the full cost, Reddy noted that he would also need to factor in past costs related to nuclear research reactors that provide plutonium for nuclear weapons, weapons-grade plutonium production, previously built aircraft development, and land- and sea-based ballistic missiles. Since Reddy's prediction, leading experts have noted the difficulty in providing more recent estimates.

"…[E]ven government bureaucracies like the Comptroller and Auditor General (CAG) and the Ministry of Statistics and Programme Implementation, whose function is to monitor expenditures and criticize cost overruns, do not seem to have access to expenses relating to weapons facilities," wrote MV Ramana, a physicist focused on international security and nuclear energy at the University of British Columbia. To the extent they have tried to oversee expenditures, the Comptroller and Auditor General of India has criticized some of the agencies involved in defense research for project cost overruns and shortcomings in budgeting and accounts.

To complicate matters further, civilian and military nuclear facilities often overlap, which means nuclear weapon expenditures may be presented as part of the civilian energy program.

Some information may be gleaned from scattered op-eds by members of the defense community or from quotes by unnamed sources. For example, a 2014 article attributed information on the cost breakdown of INS Arihant to an unnamed source. The International Campaign to Abolish Nuclear Weapons estimates that India spent $2.48 billion on nuclear weapons in 2020. Although better than nothing, one cannot have much confidence in these numbers. Reliable estimates of India's spending on nuclear weapons do not exist.

That said, these expenditures seem to be increasing, at least if one looks at the overall budgets of the umbrella agencies charged with overseeing nuclear activities. The Department of Atomic Energy, which is responsible for both nuclear energy and weapons, saw its budget increase from 121.15 billion rupees during the 2010-11 fiscal year to 182.21 billion rupees in 2019-20—both inflation-adjusted to 2020 ($1.62 billion to $2.43 billion in inflation-adjusted 2020 US dollars). In other words, the budget of the department went up by over 50 percent over the decade, even after adjusting for inflation. But the budget documents do not provide a breakdown of expenditure by program, which makes it impossible to determine how much is allocated to nuclear weapons.

India's Defense Research and Development Organization produces weapons systems and defense technologies domestically for the army, navy, and air force. This agency is in charge of developing missiles and other means of delivering nuclear weapons. From the 2013-14 fiscal year to 2019-20, its budget increased from 139.30 billion to 185.40 billion in inflation-adjusted 2020 Indian rupees ($1.86 billion to $2.47 billion in inflation-adjusted 2020 US dollars, a 33 percent increase). Since the Defense Research and Development Organization is also exempted from questions under the Right to Information Act, the percentage spent on developing nuclear weapons is unknown.

What about Pakistan's lack of transparency in its nuclear budget?

Like India, Pakistan's nuclear-weapon spending is hard to estimate, as funds for its program are placed under a secret budget head, according to Pakistani journalist Baqir Sajjad Syed. "The cost of Pakistan [sic] nuclear weapons programme cannot be estimated with any reliability," Zia Mian, a physicist and nuclear policy expert at Princeton University, writes. In

2011, Mian noted that Pakistan could be spending between $800 million and $2 billion annually on nuclear weapons, including health and environmental costs.
Of Pakistan's $10 billion military budget for 2019-2020, Mian suggests that spending on nuclear weapons was approximately 10 percent. Pakistan's military spending also includes the substantial assistance it receives from the United States and China.
Still, the Indian government should not justify secrecy around its nuclear weapon program costs by comparing itself to Pakistan—a country it accuses of sponsoring terror attacks and of being a failed state. India has long aspired for recognition as a global leader. Financial transparency on nuclear weapon spending offers India an opportunity to demonstrate leadership on the global stage.

The case for India to disclose nuclear weapon expenditures
"Powerful lobbies, including the military-industrial complex, weigh heavily on parliaments and governments and impose priorities that have no democratic legitimacy," a statement from the UN Office of the High Commissioner for Human Rights said. The statement urges states to proactively inform their citizens about past, present, and future military expenditures.
The national health budget in India has been less than a quarter of the defense budget in the last two years—even as the country was dealing with a COVID-19 pandemic and a devastating public health crisis. India's defense budget places the country among the world's top five military spenders, according to the Stockholm Institute of Peace and Research.
Meanwhile, Indian government spending on healthcare is among the lowest worldwide—a fact reflected in poor health infrastructure and exorbitant private healthcare. India is also among the nations with the most malnourished and stunted children and has an escalating rate of non-communicable diseases.
According to the economist Jayati Ghosh, Indira Gandhi, the former Indian prime minister under whom India conducted its first nuclear tests once noted that the cost of an intercontinental ballistic missile was 340,000 primary schools or 65,000 health care centers.
India should take steps towards disclosing nuclear weapon expenditures. Transparency would allow for important analysis about the balance of nuclear spending with education and health, bolster its claims as a responsible nuclear power committed to disarmament, and set a "subtle and appropriate" example for other nations to follow.

***Urvashi Sarkar** is a freelance journalist in Mumbai, India who graduated from Jawaharlal Nehru University and Asian College of Journalism. She reports on nuclear policy, foreign policy, climate change, refugee issues, and other topics. Her work has been published in* Caravan, Al Jazeera, Himal South Asian, The Wire, People's Archive of Rural India, Asia Times*, and others. She has received recognition for humanitarian reporting by the International Committee for the Red Cross and Press Institute of India and for gender sensitivity by the Laadli-Population Fund of India. She was a journalism fellow at the UN and the People's Archive of Rural India. Sarkar is a member of the Bulletin Editorial Fellows Program.*

Germany And Russia Threaten Nuclear Arsenal Use Against Each Other

By Lucy Gorman
Source: https://theowp.org/reports/germany-and-russia-threaten-nuclear-arsenal-use-against-each-other/

Nov 03 – A protest note was handed to the German military by the Russian Defense Ministry in response to comments about deterring Russia's nuclear capabilities. Germany especially had been coming out with statements about the pressing need to focus on Russia and reducing their nuclear capabilities, causing Russia to deliver the note. According to *Reuters*, Russia announced it would break off existing institutionalised contacts with NATO and the alliance agreed on a new plan to defend against any potential Russian attack.
In an interview last Thursday, incumbent Defence Minister Annegret Kramp-Karrenbauer stated that: "We have to make it very clear to Russia that in the end — and that is also the deterrent doctrine — we are ready to use such means [nuclear weapons] so that it has a deterrent effect beforehand and nobody gets the idea…" It is alarming that Germany is quick to state that they would put to use such weapons against Russia. The spokeswoman for the Russian Foreign Ministry, Maria Zakharova, said that "there are level-headed people in the German leadership who can prevent their defence minister from recklessly wanting to test our armed forces." It is unknown what the note from Russia stated, but it introduces a possible strife between the two nations over nuclear power.
Janis Kluge, an expert at the German Institute for International and Security Affairs, views the current relationship between Berlin and Moscow as at an all-time low in post-Soviet history. Germany-Russia relations have always been complicated with shifts from alliances to total warfare. The recent rise in negative relations stemmed from Russia's seizure of Crimea from Ukraine in 2014. Within NATO, Germany was quick to impose multiple rounds

of harsh sanctions against oil and other Russian industries. This leaves Germany and Russia with unstable relations today, meaning the note is indicative of a possible major conflict between the two.

Germany has made an aggressive threat towards Russia by stating that they would go as far as to use nuclear weapons in acts of deterrence. This puts hundreds of millions of people at risk, as a deadly conflict would arise if Germany took such severe action. Germany's initial comments and responses to the situation are intended to make Russia fearful of an attack and be cautious with their nuclear program. Weapons of mass destruction like the ones in question are obviously catastrophic, which pushes the common reaction to often be the use of them as it is the only way to counter such a massive threat. It is ironic that many nations choose to fight the problem with further use of the same weapons. However, nations may not see many alternatives to preventing the spread of nuclear power as they have to put forth a large enough and credible type of threat.

According to the *Arms Control Association*, Russia possesses approximately 6,400 nuclear warheads, making it the largest stockpile in the world. This raises fear among others and creates unstable relations between NATO and Russia. It is also unsettling that Russia has the power to threaten nuclear conflict in response to any other conventional conflicts. All of these then raise the question: why is this problem persisting and why have nations not figured out how to end this threat?

Following the conclusion of the Cold War there have been treaties and efforts put in place by nations to promote the decline of nuclear proliferation. Many of these efforts have been between nations in NATO and Russia including the Anti-Ballistic Missile Treaty, Treaty on the Non-Proliferation of Nuclear Weapons (in which Russia is still apart of), and the UN Treaty on the Prohibition of Nuclear Weapons which Russia chose not to sign. Some of these have had successes in Russia leading them to reduce their programs, however, there are often questions surrounding possible Russian violation of the terms, or nations pulling out of the treaty causing other parties to build up their nuclear arsenal in fear. These negotiations have proven to be no simple fix as it is difficult keeping nations like Russia accountable and knowing if countries are reporting accurate information.

The current situation, responses, and issues have been outlined above, but it is additionally important to discuss what could be done differently. Germany's comments about Russian nuclear programs and the possible use of such weapons against them are alarming and threatening. This reaction creates an escalating situation and a spread of fear throughout the two nations and all other parties i nvolved. Attempting to deter Russian nuclear capabilities with aggressive action is only likely to make the circumstance worse. Russian leadership will likely become agitated and they still will not have any incentive to want to cooperate with other nations' demands.

Looking forward, nations like Germany and even all NATO nations should have a greater focus on building relations with Russia rather than straining them. It is advisable that countries such as the U.S. collaborate with Germany to deescalate the situation while formulating a better plan to work with Russia. This should not include the threat of nuclear warfare but rather how collective agreements can be met and respected. It is important to identify why Russia has nuclear weapons or feels the need to expand their program. They may feel threatened by other nations and need a means to protect themselves. In this situation it is important to make the other nation feel protected rather than threatened unlike what Germany is promoting, because that only gives Russia more reason to build up their arsenal. If leaders can reach agreements not only with nuclear programs but in many areas of national security, the economy, and others it is likely Russia would be more willing to comply.

As stronger relations are being established, nuclear treaties can be introduced or revised to increase the likelihood of Russia complying. There has been success in the past such as the Strategic Offensive Reductions Treaty (SORT) where the U.S. and Russia both agreed to reduce their stockpiles to a certain number, which they did. Instances like this show that when nations collaborate or agree to something together there is a greater chance parties comply. Fighting fire with fire would only escalate matters and no nation in the world wants to go to war when nuclear weapons are involved. Germany also is tying its hands when they state that they would use nuclear warfare- are they actually likely to launch an attack? Collaborations and agreements that delve into various areas of society have a much greater outcome and less risk involved that puts the public in danger. Germany should work to establish these with Russia with the backing of alliances like NATO and the UN.

Lucy Gorman *has been a correspondent intern at the OWP since 2021. She is a junior at the University of North Carolina at Chapel Hill, studying Peace, War, and Defense and Psychology with a concentration in intelligence and international relations. Through her studies, she has developed a special interest in counter-terrorism, understanding the effects of war on populations, and regions of the Middle East and East Asia.*

EDITOR'S COMMENT: Although Germany has the technical capability to produce weapons of mass destruction, since World War II it has generally refrained from producing those weapons. However, Germany participates in the NATO nuclear weapons sharing arrangements and trains for delivering United States nuclear weapons. Germany is among the powers which possess the ability to create nuclear weapons but has agreed not to do so under the Treaty

on the Non-Proliferation of Nuclear Weapons and Two Plus Four Treaty. Germany is very close to making the same mistake Afghanistan recently did; they trusted the US! Has Germany granted that the US will allow the use of their nuclear weapons against the Russians? In addition, do they think that the Russians will not retaliate against the US by attacking their major cities and critical infrastructure? A country that ignited two World Wars should have a smaller mouth and keep in mind that "*it is useless for the sheep to pass resolutions in favor of vegetarianism, while the wolf remains of a different opinion*" (William Inge[2]).

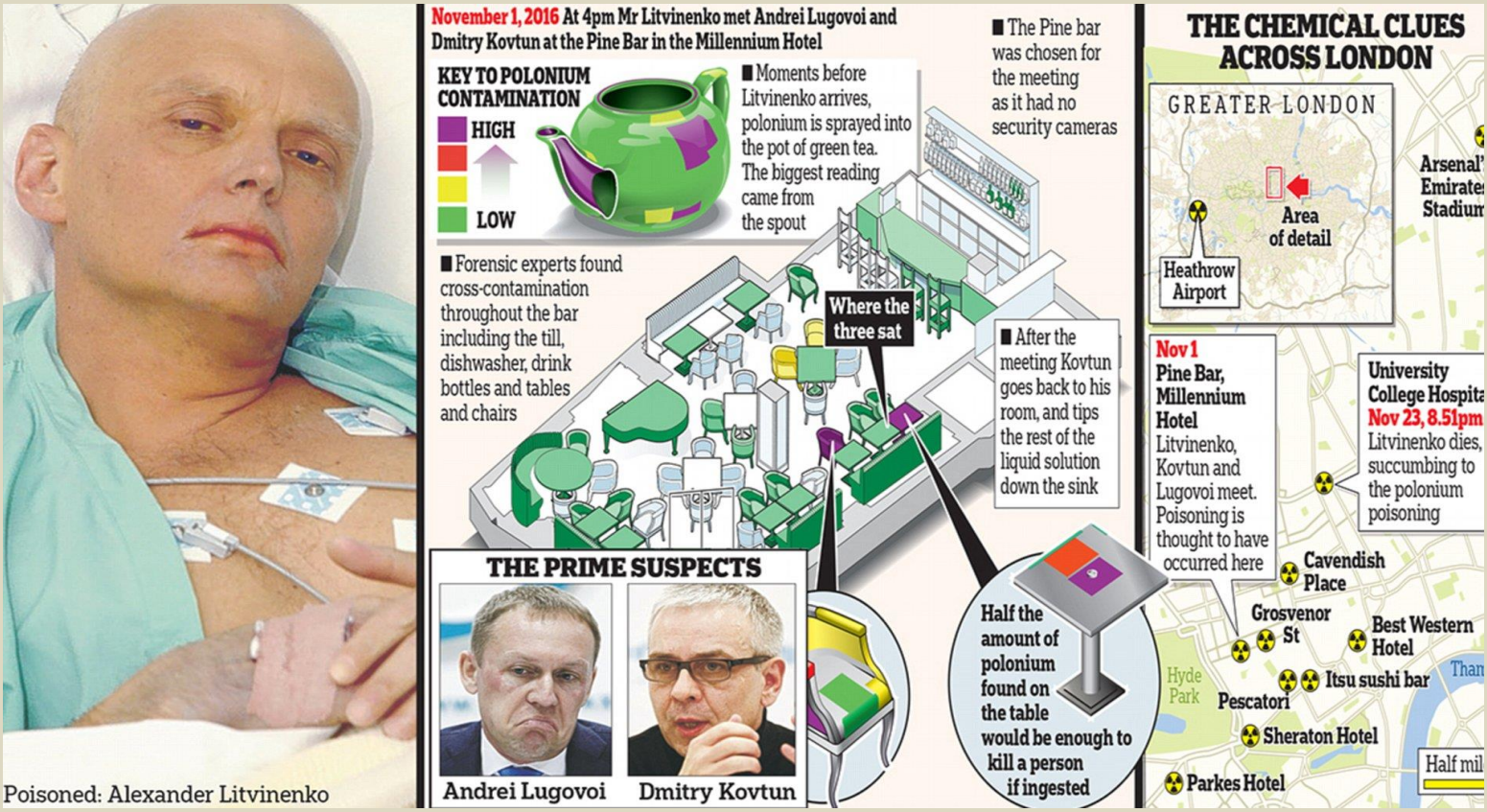
Litvinenko and the perfect radioactive poison: polonium-210

By Steven Pike

Source: https://www.argonelectronics.com/blog/litvinenko-and-the-perfect-radioactive-poison-polonium-210

Fifteen years ago, on November 1, 2006, Alexander Litvinenko was poisoned in London's Millennium Hotel. The murder weapon, disguised in a pot of tea, was polonium-210: an undetectable, tiny, rare radioactive isotope. By the time he had taken the first sip, his demise was already a fait accompli.

Alexander Litvinenko's death by poisoning



Alexander Litvinenko is the unlikely recipient of the Guinness World Record for being the first-ever person murdered by radiation. But he never found out what had killed him—it took until six hours before his death for the lab at the Atomic Weapons Establishment

[2] William Ralph Inge (6 June 1860 – 26 February 1954) was an English author, Anglican priest, professor of divinity at Cambridge, and dean of St Paul's Cathedral, which provided the appellation by which he was widely known, Dean Inge. He was nominated for the Nobel Prize in Literature three times.

to confirm he was contaminated with radioactive polonium. By this time, he was in an induced coma and never again regained consciousness.
Polonium-210 had presumably been chosen as the murder weapon because those responsible believed it would never be detected. And they were almost right. Doctors were initially perplexed about the reason for Litvinenko's sickness. They eventually decided upon a diagnosis of thallium poisoning—but remained unconvinced. Although some of his symptoms fit with thallium, he did not suffer from peripheral neuropathy, leading doctors to eventually discard the diagnosis.
The correct detection of poisoning with radioactive polonium was only made after a collaboration involving a group of medical doctors, SO15 detectives, a scientist from the Atomic Weapons Establishment, and a scientist from Porton Down (home to the Ministry of Defence's Defence Science and Technology Laboratory). The team tested a large urine sample and established the presence of a radioactive isotope.
Subsequent forensic examinations also found polonium-210 in the Millenium Hotel. There were 2,600 counts per second in a toilet cubicle and over 5,000 counts per second on a hand dryer. "Counts per second" is used to measure rates of ionising radiation; to put this measurement in perspective, anything above 150 counts per minute means the substance is dangerously radioactive. The reading in the hotel was off the scale.

What is polonium-210?
Polonium-210 (also known as Po-210, (210)Po, or 210 Po) is a radioactive chemical element (atomic number 84) that was discovered in 1898 by Marie Curie and named after her native Poland.
It is one of the most toxic substances known; the danger comes from when it emits radiation. It is estimated that one gram of polonium-210 is enough to kill 50 million people and sicken another 50 million.
Litvinenko ingested less than a millionth of a gram.
It is one of several radioactive poisons that could have been used as a lethal weapon whilst causing the murderer no harm. If stored in a glass bottle, the radiation cannot pass through the walls— a thin piece of paper is enough to block the radiation. It is not even able to pass through skin.
To prove fatal, polonium-210 must enter the human body via an open wound, be directly inhaled—or ingested. Once inside, it can travel around with ease; the element's particles deposit huge amounts of energy in the form of highly energetic alpha particles. It becomes concentrated in red blood cells and then spreads through organs and tissue to the liver, kidneys, bone marrow, and gastrointestinal tract. Damage to DNA from the alpha particle radiation causes apoptosis, a type of cell death, and the body ceases to function.

Polonium-210: the perfect poison?
In addition to being lethal, polonium is the perfect poison for another reason: the fact it is so hard to detect. Doctors such as the ones caring for Litvinenko in University College Hospital, London, often can mistake it for simpler poisons, which could derail an investigation.
An additional reason to consider polonium-210 the perfect poison is that it can be concealed and transported across borders with ease. Standard radiative materials set off radiation detectors, but polonium-210 does not. So anyone transporting the element can do so without fear of discovery.
Transportation is made even easier as the material can be carried in crystallised or powdered form or diluted in a bottle of liquid. Identifying it as polonium-210 requires a highly-trained lab technician and advanced equipment—both of which are not readily available.

Emergency responses to radioactive sources
Murder using radioactive poison is rare (so rare it has only happened once). But there is still cause for concern as, globally, over the past 25 years, there have been around 3500 incidents. Every year, there is an average of one serious radiation incident. Three hundred and fifty of these involved stolen or misused radioactive sources, including the infamous radiological event in Lilo, Georgia, where sealed radiation sources were abandoned and no safety procedures were followed. Consequently, eleven border guards were exposed to radioactive sources for prolonged periods of time.
Following the correct procedures to store and transport radioactive materials is paramount; however, systems are not fallible, and the sheer number of historical incidents show us that it is important to be aware of how hazardous radioactive materials are.
The first hurdle is to correctly identify a material as radioactive. Whilst this is relatively easy to do if containers are correctly labelled using the trefoil symbol, the problem arises when there is no indication of the type of materials that are being stored.
There are, however, some indicators. Sealed radioactive sources are usually stored in heavy metal containers with shielding made of lead, tungsten, or depleted uranium, which shield

the uranium. Any container that is abnormally dense and heavy must be treated with caution as this is a potential indication that it is being used to shield a radioactive source.

Identifying radioactive materials

Radioactive materials must be identified and recovered as promptly as possible. If the area in which the materials are located is already known, physical and administrative searches can be carried out, but radioactive sites are often undocumented.

According to the Nuclear Threat Initiative:

There are new and innovative methods "such as network analysis, online surveys, and open-source searches utilizing new tools, such as geospatial analysis, aerial images, social media, as well as YouTube videos, can be used to enhance the national regulators' ability to track down and secure orphan or abandoned radioactive sources and prevent them from potentially falling into the hands of terrorists or other nefarious actors."

These novel methods are excellent ways of helping investigators reduce the size of the area that needs to be surveyed. When in the field, investigative teams will need to use detection devices to positively identify and address radiological materials.

The benefits of simulation training for investigators

Using simulation as a training tool is a widely used method of preparing investigators in the field to correctly identify radioactive materials.

Argon Electronics has over 30 years of experience as a global provider of Chemical, Biological, Radiological and Nuclear (CBRN) detector simulators. We have developed strong relationships with many of the leading detector manufacturers, which allows us to create realistic simulators that are almost identical to the real devices.

This allows instructors to create realistic scenarios and train future investigators who will accurately be able to detect radiological threats before they further damage human and environmental life.

Iran admits having 210 kilograms of 20% enriched uranium

Source: https://www.aa.com.tr/en/middle-east/iran-admits-having-210-kilograms-of-20-enriched-uranium/2413398

Nov 06 – Iran said Friday that its stockpile of 20% enriched uranium has reached 210 kilograms (463 pounds).

Iran's semi-official Tasnim and Fars news agencies quoted a spokesman for the country's atomic agency, Behrouz Kamalvandi, who said the quantity is larger than the 120 kilograms at 20% set by parliament to be produced.

Kamalvandi added that the agency produced **25 kilograms of 60% enriched uranium -- a level only countries with nuclear weapons can produce. Uranium enriched to 90% can be used to develop a nuclear weapon** but Iran has repeatedly said its program is for civil purposes.

Under the 2015 nuclear deal between Iran and world powers, Tehran was allowed to enrich uranium to a level not exceeding 3.67%.

In January, a spokesman for Iran's atomic agency said the country was reviewing the need to increase uranium enrichment to a level greater than 20% and stressed Tehran has the capability to enrich uranium to a level that could reach 90%.

The European Union, US and Iran announced Wednesday that nuclear talks will resume Nov. 29 in Vienna.

The talks aim to restore the 2015 nuclear deal which was annulled by former US President Donald Trump in May 2018 as well as to bring Iran in compliance with international commitments regarding its nuclear program.

EDITOR'S COMMENT: It will come a day (soon) that Iran will say "Hey guys! We have two nuclear bombs and there is nothing you can do about it!"

Meet the Saab 36: Sweden's Secret Nuclear Bomber Program

By Caleb Larson

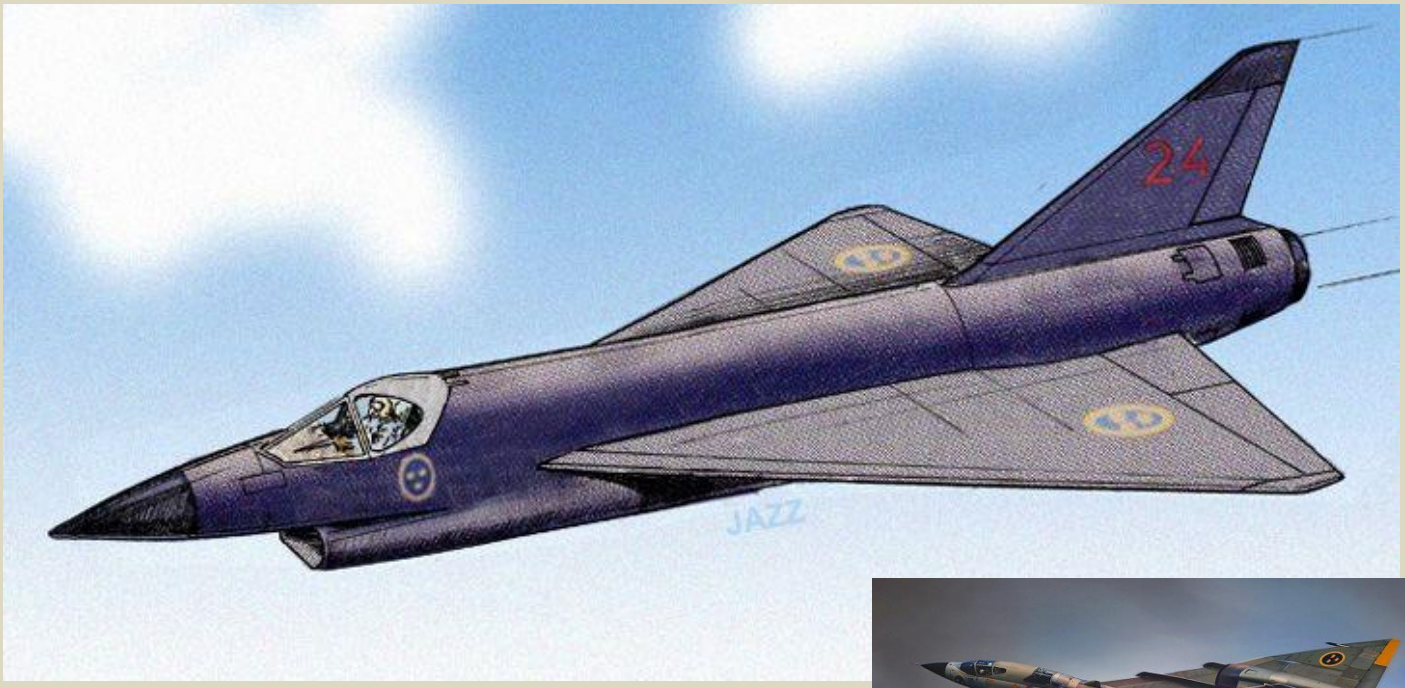
Source: https://nationalinterest.org/blog/buzz/meet-saab-36-swedens-secret-nuclear-bomber-program-146062

After the Second World War, Sweden initiated a clandestine nuclear program — and had plans for a supersonic nuclear bomber.

Atoms for Peace

After World War II, the Soviet specter lay heavily across Europe. Like other post-war countries, Sweden wanted to protect itself from a Soviet invasion — and decided to manufacture nuclear weapons to ensure its security.

Initially, Sweden tried to get nuclear weapons expertise from outside the country. The United States, as the world's first nuclear power and a guarantor of European security, was a logical partner.
In the early days of the Cold War, the United States pursued a strategy of promoting nuclear power for energy production — President Eisenhower's "Atoms for Peace" concept. Nuclear material and nuclear know-how would only be transferred to foreign governments on the condition that the nuclear research and development would only be for peaceful purposes, precluding weapon's research. Sweden declined.
Buying nuclear weapons directly from the United States was also an unattractive option for Sweden most likely impossible.
Luckily for the Swedes, Uranium-containing shale is abundant in Sweden.



Bombs Away
By the mid-1960s, Sweden has enough fissile material to build a bomb in six months. It just needed a platform to deliver nuclear payload — the Saab 36.
The Saab 36 was a twin-engine supersonic bomber. It would have had delta wings, and fly in the Mach 2+ range. Flight ceiling was to be 18,000 meters or 60,000 feet.
Targets of value to Sweden were in the Baltic — the Baltic countries of Latvia, Estonia, and Lithuania are just across the Baltic Sea, and Poland and East Germany are also practically next door to Sweden. (Though the Cold War is over, the Baltic is still an area of concern for Sweden.)
The Saab 36 had to deal with a few design restrictions which would affect its payload.
Designers at Saab were concerned that the weapons externally attached to the fuselage or wings would create drag, degrading the jet's performance. The high Mach 2+ speed would also have generated a large amount of heat that could damage weapons — or worse cause them to "cook-off" or accidentally explode.
Bombs would have to be stored internally in an enclosed weapons bay, farther away from potentially dangerous high temperatures. Internal space would be at a premium, and there would only be space for a single 800 kilogram, or 1,800 pound, free-falling nuclear bomb, reducing the efficacy of the bomber, and limiting its use to a tactical weapon delivery system rather than a strategic deterrent.
The Saab 36 got off the drawing board just as a simple wind tunnel mockup and the design was not finalized. Images online appear to show two different designs, one with a chin-mounted engine intake, and another with two jet engines integrated in the delta wing.

Postscript
Though the bomber never entered serial production, work on the Saab 36 contributed in part to the development of the Saab 37, a strike fighter that was one of the first successful jets that incorporated the delta wing design.

The Swedish Parliament, the Riksdag, would renounce nuclear weapons in 1968, and Sweden would abandon its nuclear ambitions in the early 1970s, shipping fissile material abroad. The Saab 36 would never fly.

***Caleb Larson** is a Defense Writer with The National Interest. He holds a Master of Public Policy and covers U.S. and Russian security, European defense issues, and German politics and culture*.

Results of the 1st International Arabian-Gulf Security Conference at AUE

Drawing a better future for the Arabian-Gulf Security

Source: https://aue.ae/results-of-the-1st-international-arabian-gulf-security-conference-at-aue/

The 1st International Arabian-Gulf Security Conference was organized and hosted successfully by the American University in the Emirates (AUE) over two days Wednesday 10 and Thursday 11 November 2021. The Conference was held under the Patronage of and in the presence of His Excellency Lieutenant-General Dhahi Khalfan Tamim, Deputy Chairman of Dubai Police and General Security in Dubai. The Conference was headed by the honorary Chair Major General Dr. Ahmed Nasser Al Raisi; chaired by Professor Muthanna Abdul Razzaq, President and CEO of the AUE.

Participants hailed the conference's need, topics, timing and reasoning for such an organization. The Conference brought together, academics, researchers, practitioners and experts at the local and international levels to discuss the current status and future relations of Arabian Gulf Security. The conference was organized at an important moment in light of regional challenges yet also opportunities to convene and discuss the importance on peace and resolution of pending or ongoing conflicts.

As a highlight to the Conference, His Excellency Lieutenant-General Dhahi Khalfan Tamim, Deputy Chairman of Dubai Police and General Security in Dubai, stated that "the AUE's

interest in organising an annual security conference and promoting the security culture in society is one of the strategies that people should pay attention to because it is extremely important."

"When a society's security is stable, individuals are able to live better lives, which emphasizes the need of instilling a security culture in society. We observe what has happened and continues to happen in nations where security and security culture are lacking," he added.

Professor Muthanna Abdul Razzaq, President and CEO of the AUE, stated during the Conference that "the Arab Gulf, Arab countries, through which also the Gulf Cooperation Council constitute a particularly crucial region in all respects and circumstances, in addition to its worldwide and not just regional significance. From this standpoint, we took the initiative to hold this Conference in order to explore the region's security challenges from a variety of perspectives that will help up comprehend yet also propose issues for consideration."

US Ambassador Mark Andrew Green CEO and President of the Woodrow Wilson Center from the Washington DC, lauded the AUE Conference, calling it “very crucial” for the region for both the UAE and the region particularly due to its importance in identifying methods and features for a brighter more stable and secure future in the Arabian-Gulf region. Elements achieved through the 1st International Arabian Gulf Security Conference.

Highlighted important personalities and key experts joining the conference include H.E. Major General Ahmed Nasser Al Raisi, Chairman of the Board of Trustees of the AUE, retired US Ambassador Mark Andrew Green, President and CEO of the Woodrow Wilson International Centre for Scholars in Washington, Major General Thani Butti Al Shamsi, Director of the Saif Bin Zayed Academy of Police and Security Sciences, Engineer Anwaar Al Shimmari from the Federal Geographic Information Center - Abu Dhabi, and Vladimir Tomašević from Union Nikola Tesla University School of Engineering - Serbia, participated in the opening session of the Conference.

The Conference is thankful to the collaborating partners of this years’ conference, to include The Hoplite Group, the Federal Authority for Identity and Citizenship, H.E. Sheikh Abdulaziz bin Duaij bin Khalifa al Khalifa Private Office, Expo 2020 Dubai, the International Association for Intelligence Educators (IAFIE), the Center for Sea Power and Strategy At Plymough University UK, The Center for Global Security and Defence Affairs UAE & Egypt, The Center for Global and Strategic Studies Islamabad, the Georgian Center for Strategic Studies and Environmental Research.

During the conference more than 200 papers were submitted and 55 papers were successfully accepted to be presented with 75 authors/co-authors, which included, 4 tracks of presented papers to include security and law affairs, economic warfare and diplomacy and international affairs, peace and conflict resolution and military affairs and technology and cyber-security, on the most recent developments and the future on the security, resilience and growth of the Arabian-Gulf region.

Among others, topics like money laundering and financial crimes in the Middle East and North Africa, comprehension of international alliances in the Gulf and greater MENA region, recommended the way to implementing security convergence management and tackling threats were all covered and reviewed during the Conference sessions.

The importance and role of water security and stadium security was included. Game-changing factors in cyber security were added to the historical development of fake news and its danger to societies, analysis of the phenomenon of conflicts and examining their causes and complexity, biological terrorism threats and ways to address them through strategic foresight were among the topics discussed as well while also methods of peace and conflict resolution.

Moreover, sessions touched on cybercrime and technology, military technology issues such as the utility of drones for the Arabian-Gulf area, and the ramifications for future strategy and tactics. The attendees also considered Gulf security in terms of possibilities for stability and commercial continuity, as well as strategies to strengthen peace between the Arabian Gulf's two shores.

During the opening of our second day of our Conference a highlight included the talk of Major General Abdulla Al Hashmi, Member of the Board of Trustees of the AUE, who inaugurated the second day on UAE's regional concerns and issues and security. Other topics centred on the complexity of the regional security challenges, factors against threats of asymmetrical threats and terror groups, the need for joint collaboration in international governance and cooperation to face current and future challenges.

The 1st International Arabian-Gulf Security Conference, already in its inaugural edition, is seen as a springboard for the second edition, which will take place next year in 2022. This Conference stems from the AUE's keenness to graduate competent and educated leaders and research experts, who make sound and important decisions for society and their nation.

25,000kg consignment of titanium forgings worth RM3.5 million found in Port Klang warehouse

Source: https://www.nst.com.my/news/crime-courts/2021/11/745122/25000kg-consignment-titanium-forgings-worth-rm35-million-found-port

Nov 13 – The Royal Malaysian Customs Department has foiled an attempt to smuggle 'titanium forgings', a possible nuclear weapon material, worth more than RM3.5 million here.

Customs deputy director (enforcement/compliance) Datuk Abdul Wahabi Abdullah said the 25,000kg consignment was on transit in Malaysia and was believed to be on its way to the middle east.

He said 'titanium forgings', which have the dual use of either producing weapons of mass destruction, including nuclear ones; or in making aircraft spare parts, is a prohibited item.

It requires special permit from the Atomic Energy Licencing Board (AELB) and International Trade and Industry Ministry (Miti) before it can be transported through Malaysian ports.

"It is illegal for any person to transport the titanium forgings unless the sender has obtained special permits from the relevant authorities because it is considered highly dangerous and normally used for military purposes only," he said here today.

Wahabi said having acted upon a tip off, an enforcement team from the Federal Territory together with AELB officers and Miti inspected a warehouse in Port Klang on Oct 27, before they discovered the 25,000kg consignment.

"The titanium forgings commonly used to build mass destruction weapons were wrongfully declared and did not have the necessary permits to enter our country as transshipment.

"The shipment is headed to the Middle East from a country in Asia and Malaysia was used as a transit point, before it gets transported to the intended destination," he said when met at Wisma Kastam Selangor in Pulau Indah, this afternoon.

Customs deputy director (enforcement /compliance) Datuk Abdul Wahabi Abdullah said the 25,000kg consignment was on transit in Malaysia and was believed to be on its way to the middle east. - NSTP/ OWEE AH CHUN

Wahabi said the department has opened an investigation into the fraudulent consignment and are in the midst of questioning the shipping agent responsible for its arrival into the country.

He said the consignment breached the requirements of Section 9(1) and Section 9(4) (a) of the Strategic Trade Act 2010.

The Strategic Trade Act 2010 is a law enacted by the Malaysian government in 2010 to control the export of sensitive technology and materials in order to combat terrorism, nuclear proliferation, and the spread of weapons of mass destruction.

"This is the first time we have come across a highly classified consignment such as this and we are investigating the case thoroughly, with the help of Miti, AELB and several other relevant agencies," Wahabi said.

He said authorities are also trying to determine how the consignment made it out of the last port and what's the purpose and source of the transshipment.

Could a Radiation Shield Made of Fungus Keep Astronauts Safe During Space Travel?

Source: https://www.sciencealert.com/could-a-radiation-shield-made-of-fungus-keep-astronauts-safe-during-space-travel

Nov 14 – A lack of effective radiation shielding is one of the biggest challenges still to be overcome if humans are to embark on long-term voyages into deep space.

On Earth, the planet's powerful magnetosphere protects us from the deadliest forms of radiation – those produced by solar flares, and galactic cosmic rays arriving from afar – that stream through the Solar System.

Astronauts on the International Space Station, some 408 kilometers (254 miles) above the Earth, receive elevated levels of radiation but are close enough to Earth that they still receive some shielding, and can stay on orbit for up to a year.

The same can't be said for astronauts traveling further out, to the Moon, for example, or, someday, to Mars. Future deep space voyagers will need to bring their own shielding with them – or, as a new paper suggests – grow it along the way.

According to the paper, published in pre-print format on BioRxiv earlier this month, a special type of fungi that thrives in high radiation environments called ***Cladosporium sphaerospermum*** could form a living shield around astronauts in space.

The fungus not only blocks radiation but actually uses it to grow, through a process call radiosynthesis: It pulls energy from radiation, just as most plants pull energy from sunlight via photosynthesis.

These radiation-loving fungi survive on Earth in extreme places, like the site of the Chernobyl Nuclear Power Plant in Ukraine.

In space, they do just as well. In 2019, researchers flew some of the fungi to the ISS, watching how it grew over a period of 30 days, and measuring the amount of radiation that passed through it, as compared to a control sample with no fungi.

The experiment showed that radiation levels beneath a 1.7-millimeter-thick (0.07 inches) bed of fungus were about 2.17 percent lower than the control.

Not only that, but the fungus grew about 21 percent faster than it does on Earth, meaning that the fungi's ability to act as a protective shield for astronauts could actually grow more robust the longer a mission lasts.

It's too early to get overly excited about the practical applications of this fungus in space travel. The team estimates that on Mars, to bring radiation levels down to Earth-like conditions, a habitat would need to be covered with a 2.3-meter-thick (7.5 feet) layer of radiosynthesizing fungi.

The same effect could be achieved by burying the habitat beneath 3 meters of Martian dirt (regolith). Still, the potential for biological solutions to what are often considered engineering challenges is a unique approach and may prove fruitful.

For the near future, astronauts will rely on more mundane solutions. In the case of solar flare events, contingency plans involve sheltering amidst a spaceship's cargo: the more mass between the astronauts and the incoming radiation, the safer they'll be.

The upcoming uncrewed Artemis 1 mission, due to launch next year, is testing a protective vest designed to minimize the radiation doses received by the wearer.

So far, none of these solutions are ideal. There is a lot of work still to be done to keep future astronauts safe. When the time comes, however, don't be surprised if part of the solution to space radiation involves hiding beneath a thick blanket of friendly fungi.

China's silence on nuclear arms buildup fuels speculation on motives

By Tong Zhao

Source: https://thebulletin.org/2021/11/chinas-silence-on-nuclear-arms-buildup-fuels-speculation-on-motives/

Nov 12 – The US Defense Department released a report this month that spotlights the Chinese military's rapid nuclear modernization efforts. The report follows news earlier this year that China constructed potential intercontinental ballistic missile silos and tested an orbital hypersonic missile system. China has also been at work strengthening its nuclear

triad capability of land, sea, and air missiles. And the country is reportedly experimenting with new and perhaps exotic delivery technologies, while possibly shifting toward a launch on warning posture. World citizens who want to understand the security implications and prospects for future arms control cooperation with China must first try to understand the military rationale behind its nuclear expansion.

Chinese decision makers have never elaborated in public about speeding up China's traditionally modest nuclear modernization program. But their occasionally reported public statements reveal how their thinking has evolved. The current Chinese paramount leader—Xi Jinping—upgraded the Rocket Force of the People's Liberation Army from a military branch to a full military service in 2015. Then, in 2016, he instructed Rocket Force officials to "accelerate the pace of development and make a solid effort to bring strategic capabilities to a high level."

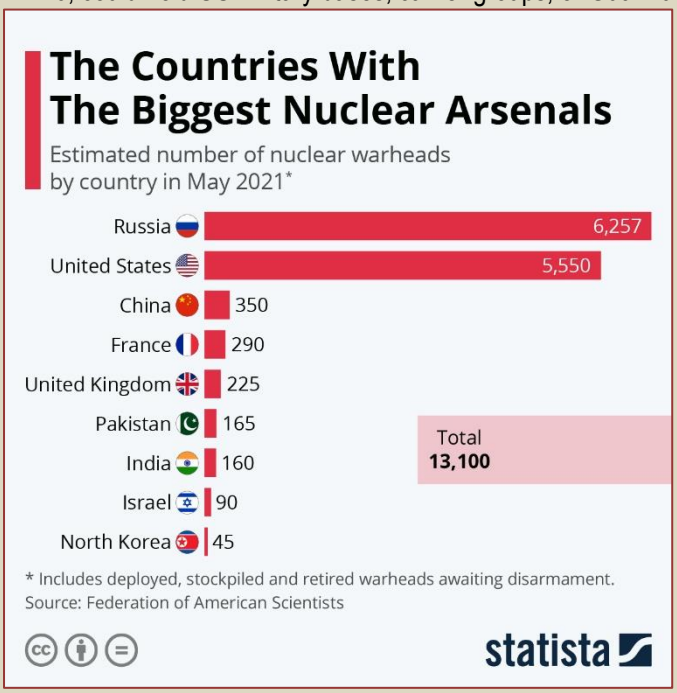
"Our sea-based nuclear capabilities need to massively develop," Xi told naval leaders during a 2018 submarine base inspection. Later, during an important March 2021 political conference, he instructed the military "to accelerate the construction of high-level strategic deterrent" systems as part of China's 14th Five-Year Plan. When the draft of this plan was proposed in 2020, the original wording was "to construct high-level strategic deterrent" systems. The additional emphasis on "accelerate" reveals his urgency to expedite the nuclear modernization process.

What military rationale may have contributed to this development?

On a basic level, China may simply want to further assure its second-strike capability. The country has long relied on an uncertain second-strike capability as a deterrent, according to some Chinese nuclear experts. Beijing may be convinced that its growing strategic rivalry with Washington makes its uncertain second-strike capability insufficient to deter a more hostile United States. However, this does not fully explain the reported scale and speed of China's nuclear expansion.

Even considering Chinese strategists' long-standing distrust of the US military, China's projected nuclear buildup looks excessive for securing a basic second-strike capability. Instead, China may be aiming to achieve some escalation management capabilities.

Since the 1980s, Chinese nuclear strategists have recognized that the threat of massive retaliation lacks credibility and could be considered too escalatory against a limited nuclear attack. Instead, they may have sought more sophisticated nuclear development and employment policies. At the same time, China may be concerned that the US reemphasis on low-yield nuclear weapons in recent years indicates a lower threshold for nuclear use. China could de-escalate a nuclear conflict on its own terms by responding symmetrically or proportionately to limited US nuclear employment. Accurate theater-range nuclear missiles, such as the DF-21 and DF-26, could hold US military bases, carrier groups, or Guam under threat.



Admittedly, such missiles would also give China the capacity to initiate a limited nuclear strike in a regional conventional conflict, such as one over the Taiwan Strait. Yet China's growing conventional military advantages within the First Island Chain could help reduce its incentive to do so. Nevertheless, China may be concerned about US nuclear first use, given the shifting balance of conventional military power in the region. Indeed, many international analysts believe the Chinese paramount leader seeks to achieve national unification with Taiwan by 2049. As part of this effort, the People's Liberation Army has been building up conventional forces to deter and defeat any conventional US military intervention of Chinese efforts to take over Taiwan. If China is capable of conducting proportionate nuclear retaliation at the theater level, it could deter Washington from escalating the conventional war to the nuclear level. Even if deterrence fails, China's accurate theater-range nuclear weapons would increase Beijing's chances of achieving de-escalation on terms favorable to China.

If a regional nuclear conflict further escalates and the United States launches a limited nuclear strike on select military targets in China, Beijing might want to respond with a limited nuclear strike on select military targets on the US homeland. For this, China would need long-range strike capabilities that are accurate, highly effective at penetrating US homeland missile defenses, and incapable of neutralization by US missile defenses. For a limited nuclear strike, China could not simply launch more missiles to saturate US missile defenses, as that would obscure the limited nature and intention of the strike. For this reason, China may be developing a more advanced nuclear force as a means

to acquiring escalation management capabilities. In particular, the reported development of an intercontinental hypersonic glider system could be useful in this regard.

China may have had trouble determining how much nuclear modernization is sufficient for securing a second-strike capability. But it may have had even more trouble deciding how much additional nuclear modernization is sufficient for acquiring a proper escalation management capability. Proper escalation management capability is much more ambiguous than a basic second-strike capability based on massive retaliation. If China is indeed exploring nuclear escalation management options, the already-competitive US-China nuclear relationship would become much more acute. Once both countries seek advantageous capabilities over each other to be able to de-escalate nuclear conflicts on one's own terms, an arms race could ensue.

The new Defense Department report asserts that China "probably seeks to keep at least a portion of its force on a [launch on warning] posture" and "has conducted exercises involving early warning of a nuclear strike and launch on warning responses" since 2017. To acquire a launch on warning capability would enhance the survivability of China's second-strike forces, but it could provide additional military benefits. Specifically, China might worry that Washington could conduct a limited nuclear attack on China, while threatening a more massive nuclear attack should Beijing dare to retaliate with nuclear weapons. Given the US nuclear superiority, Chinese leaders might not be able to respond in kind. But this problem could be mitigated if Beijing publicly adopts launch on warning. Washington would then need to consider the possibility that Chinese leaders could order an immediate nuclear retaliation within minutes of detecting incoming US missiles and before any US threat of follow-on nuclear attack could be issued. In this regard, China's growing interest in launch on warning capabilities might strengthen its de-escalation capacity by weakening the US capacity to de-escalate.

As a Chinese and world citizen, I am not alone in speculating about the Chinese government's nuclear thinking. Senior Chinese diplomats in charge of relevant policy issues are not necessarily informed about the People's Liberation Army's nuclear capability development and policy deliberation. Most Chinese nuclear policy experts appear cut out of internal policy deliberations and instead rely on open-source research by foreign counterparts to understand their own country's capabilities and motivations. The internal coherence and overall rationality of China's new nuclear capabilities and posture is shrouded in secrecy and lacks domestic checks and balances. If Beijing elaborated on the military rationale behind China's nuclear expansion, it would help mitigate international anxieties.

***Tong Zhao** is an associate at the Carnegie–Tsinghua Center for Global Policy. His research focuses on strategic security issues, including nuclear arms control, nonproliferation, missile defense, strategic stability, and China's security and foreign policy. Zhao received his PhD in science, technology, and international affairs from Georgia Institute of Technology. He holds a Bachelor's in physics and a Master's in international relations from Tsinghua University.*

FW de Klerk, who ended South African apartheid, leaves another legacy: nuclear disarmament

By Robin Ephraim Möser

Source: https://thebulletin.org/2021/11/fw-de-klerk-who-ended-south-african-apartheid-leaves-another-legacy-nuclear-disarmament/

Nov 12 – Almost nothing suggested that former South African president Frederik Willem de Klerk would be the one to dismantle apartheid. He was born into a family of politicians of the nascent apartheid state, became a member of Parliament in 1972, and was complicit in—even supportive of—all the evil committed under apartheid during numerous ministerial posts. But while serving as president, de Klerk stunned the world in February 1990 when he removed the ban on opposition political movements, including the African National Congress, and released political prisoners, including the individual with whom he would later share the Nobel Peace Prize—Nelson Mandela.

De Klerk's death at the age of 85 this week has been widely reported in the *New York Times*, the *BBC*, *der Spiegel*, the *Daily Maverick*, and other international media. Yet none mention that, under his leadership in 1991, South Africa joined the Nuclear Non-Proliferation Treaty and fully dismantled the country's nuclear weapons arsenal.

De Klerk believed that nuclear weapons, having lost their deterrence value following the end of the regional conflicts, would subsequently burden his government. Two weeks after assuming the presidency, he held a top-secret meeting of advisors in which he requested a plan to rid the country of nuclear weapons. Those who attended agreed, though some rather grudgingly, as he recounted in my 2017 interview with him.

South African Deputy President FW de Klerk and South African President Nelson Mandela pose with their Nobel Peace Prize Gold Medals and Diplomas in Oslo on December 10, 1993 [File: AP Photo]

A president in favor of nuclear disarmament

Though de Klerk apologized for his complicity and support for the evil committed under apartheid in his last public message, he will never be acquitted. He benefitted from the racially discriminating structures, while serving as an instrument that perpetuated the system—at least until he negotiated the Afrikaners out of power. But when he had the chance to terminate the nuclear program, he did so with expediency and conviction.

Was de Klerk's anti-nuclear stance born from strategic foresight, distaste for the nuclear warheads, or opportunistic awareness of the necessity? The world may never know. Still, unlike his predecessor, PW Botha, he had the courage to act on a nuclear disarmament opportunity when he saw it.

The Cold War was winding down by the time de Klerk took over the presidency. He made sense of international political events like the fall of the Berlin Wall and Soviet Perestroika in terms of realpolitik—politics based on practical rather than ideological considerations. In the nuclear realm, he displayed an inner certainty that moved him to act. He sought to reduce South Africa's isolation that resulted from its Cold War nuclear ambiguity. If Pretoria—the city where the country's executive branch sits—dissolved its nuclear arsenal, South Africa would regain respect in the global community of states.

An international and domestic balancing act

When de Klerk ordered the disarmament in early 1990, the South African government was not yet on a clear path towards democratic majority rule. On the international stage, UK

Prime Minister Margaret Thatcher and US President George H.W. Bush courted de Klerk. Meanwhile, the Conservative Party—a looming right-wing threat emanating from paramilitary groups and white extremists—exerted pressure at home. Opposition to the government's reform plans risked a coup.

The newly elected de Klerk wanted a quick return to normal political relations with other states. While the world would be reassured if Pretoria renounced nuclear weapons, saying as much would have had disastrous domestic political repercussions. Still, soon after taking office, de Klerk issued secret orders to dismantle South Africa's six nuclear warheads and a seventh then under construction. He waited to announce the historic decision until March 1993.

Almost three decades later, in my 2017 interview with him, de Klerk revealed that his distaste for nuclear weapons preceded his presidency. He had decided that if ever he became president, he would review South Africa's nuclear weapons program. He had that chance by 1990—and seized the denuclearization opportunity.

De Klerk's nuclear rollback was complete and verifiable. Not only was South Africa free of nuclear weapons, but the development served as a catalyst for Africa as a nuclear-weapon-free zone. In 1995, President Nelson Mandela and other African heads of state signed the Treaty of Pelindaba, which forbade atomic bomb testing and banned nuclear weapons from the African continent.

South Africa remains the only country to have gone full circle on nuclear weapons. The South African National Party politicians initiated a nuclear weapons program during the 1970s and de Klerk ended it in 1989. De Klerk expressed the hope that South Africa's example might inspire the nine leaders of other nuclear weapons states—the United States, the United Kingdom, Russia, France, China, India, Pakistan, Israel, and North Korea—to eliminate their arsenals. The world can only hope that, over time, they do.

Robin Ephraim Möser, PhD, *is a researcher associated with the Global and European Studies Institute (GESI) at the University of Leipzig, Germany. His forthcoming book,* Disarming Apartheid, *explores the political history of South Africa's nuclear disarmament and the multilateral negotiations preceding the accession to the Nuclear Non-Proliferation Treaty.*

Russia threatens Europe and NATO

Source: https://www.thesun.ie/news/7893408/us-nuclear-germany-eagle-hypersonic-missiles-moscow/

Nov 10 – The United States has reactivated a nuclear unit in Germany for the first time since the Cold War and is armed with "Dark Eagle" long-range hypersonic missiles. When fully developed and deployed the rockets will be capable of travelling 4,000mph and could blitz Russia in just 21 minutes and 30 seconds.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

EXPLOSIVE NEWS

The Importance of Humanitarian Underwater Demining

By Mr. Veselin Mijajlovic
Director of Regional Center for Divers Training and Underwater Demining, Montenegro
NCT Magazine | October 2021
Source: https://nct-magazine.com/nct-magazine-october/the-importance-of-humanitarian-underwater-demining/

The RCUD is a governmental organization from Montenegro, the sole civilian one of its kind in Europe, performing underwater demining and related divers training. The problem of underwater UXOs, leftover from the World Wars, represented a big problem for Montenegro. The RCUD successfully removed tens of tons of unexploded ordnances from the former military bases located within the Montenegro territory, gaining invaluable experience that then deployed them in underwater demining missions around the world. Such humanitarian underwater demining missions present some vital security and strategic aspects.

New analysis puts more accurate figure on size of last year's Beirut blast

By Rebecca Trager (US correspondent, Chemistry World)
Source: https://www.chemistryworld.com/news/new-analysis-puts-more-accurate-figure-on-size-of-last-years-beirut-blast/4014586.article

Oct 19 – New light has been shed on the size of the explosion in Beirut, Lebanon in August 2020 that killed more than 200 people and injured thousands more. Estimate of the explosive yield of the blast, which resulted from the detonation of thousands of tonnes of improperly stored ammonium nitrate and damaged more than half the city, have varied widely. In some cases, these figures were inconsistent with what would be expected based on the amount of ammonium nitrate stored at the

harbour, as well as the crater size, seismic magnitude and mushroom cloud height, according to researchers from Lawrence Livermore National Laboratory (LLNL) in California.
Official records indicate that roughly 2700 tonnes of ammonium nitrate were stored at the Beirut harbour warehouse that blew up. The detonation – one of the largest non-nuclear explosions in history – created a large crater, and seismic measurements suggested that the yield was anywhere from a few kilotonnes of TNT to much more. But other estimates suggest that the explosion was significantly smaller, maybe as little as half a kilotonne. Now, new analysis by LLNL physicist Peter Goldstein has assessed the crater dimensions, seismic magnitude estimates and the cloud height of the explosion, and concluded that all the data are consistent with **a yield of around a kilotonne**.

By comparison the largest non-nuclear explosion occurred in Halifax, Canada in 1917 when a transport ship carrying picric acid, TNT and fuel collided with another ship. The resulting explosion has been estimated at 2.9 kilotonnes of TNT.

Goldstein and his team determined the yield by using crater-size observations from satellite imagery and empirical data for scaled crater radii from past chemical and nuclear explosions. 'The evidence suggests that the relatively large crater radius is due to a high degree of saturation of the ground beneath the explosion,' he explained. 'It is likely that this saturation increased coupling of shock wave energy to the surrounding material and reduced the effective stress/strength of the material.'
Other measures, including the maximum debris cloud height and the observed crater depth, corroborated the estimates based on crater radius.
Effective emergency response planning to address potential consequences from accidents like the Beirut explosion, or deliberate attacks with weapons like improvised nuclear devices and radioactive dispersal devices, requires these models to be trustworthy.
The new LLNL research also has implications for nuclear explosions, indicating that environmental features can substantially affect shock and blast waves, seismic motions and crater formation, as well as fallout. The effects also feed into things like the yield estimate, Goldstein noted. He said he expects features like water close to the site of the explosion to have a significant effect on other explosion phenomena, including the transport of radiation and the formation of post-detonation debris.

On October 28, Abbas Ahmed Mazloum, 38, a father of five died of wounds sustained in the Beirut port blast where he was working, 15 months after the catastrophic explosion.

China Hypersonic Test "Has All of Our Attention": Gen. Milley

Source: https://www.homelandsecuritynewswire.com/dr20211028-china-hypersonic-test-has-all-of-our-attention-gen-milley

Oct 28 – China's efforts to surpass the United States as the world's foremost military power are making significant progress, based on a July test of a hypersonic weapons system.
The top U.S. military officer confirmed Beijing's July 27 test of a high-speed system that orbits Earth to better evade U.S. missile defense systems, calling the development "very concerning."
"What we saw was a very significant event of a test of a hypersonic weapon system," General Mark Milley, chairman of the Joint Chiefs of Staff, told Bloomberg Television on Wednesday.
"I don't know if it's quite a Sputnik moment, but I think it's very close to that," he added, referring to Russia's launch of the world's first artificial satellite in the 1950s, which sparked the space race that dominated the next several decades. "It has all of our attention."

A Surprise, Report Says
Until now, U.S. officials have declined to speak publicly about the Chinese weapons test, first reported by the *Financial Times*, which said it took U.S. intelligence officials by surprise.
The *Financial Times* also reported that while the Chinese weapon missed its target by several kilometers, the test marked the first time any country had sent a hypersonic weapon fully around Earth.
For years, U.S. military officials have warned about the dangers of hypersonic weapons, which travel faster than five times the speed of sound and are capable of carrying nuclear payloads.
In 2018, General John Hyten, vice chairman of the Joint Chiefs of Staff, cautioned that Washington's best defense against hypersonic weapons was to be able to mount similar offensive capabilities.
"We don't have any defense that could deny the deployment of such a weapon against us," said Hyten, then the commander of U.S. Strategic Command.
Since then, U.S. military officials have made the development of hypersonic weapons a priority, boosting research following a Russian test of a nuclear-capable hypersonic glider in 2018.

Last week, the U.S. Army and Navy announced several tests of hypersonic weapons components, describing them as successful. But concerns about hypersonic weapons persist.
"We just don't know how we can defend against that type of technology," Ambassador Robert Wood, the top U.S. arms control official, told reporters in Geneva last week, when asked about the reported Chinese test.
"Neither does China or Russia," Wood added.
For its part, China has denied it carried out a hypersonic missile test, saying it actually tested a reusable spacecraft.
But U.S. officials said Wednesday that in any case, China's military trajectory is worrying.
"They continue to pursue capabilities that increase tensions in the region, and we continue to have concerns about that," White House press secretary Jen Psaki said, declining to comment directly on Beijing's hypersonic test.
The Pentagon also refused to comment directly on the test, saying only that the development "reinforces for us the need to continue to treat the PRC [People's Republic of China] as our No. 1 challenge."
"We are laser focused on making sure that we have the operational concepts, the capabilities, the resources that we need to deal with this pacing challenge," Pentagon press secretary John Kirby said during a briefing, in response to a question from VOA.
"They have a global reach that we have to be careful about." he said.

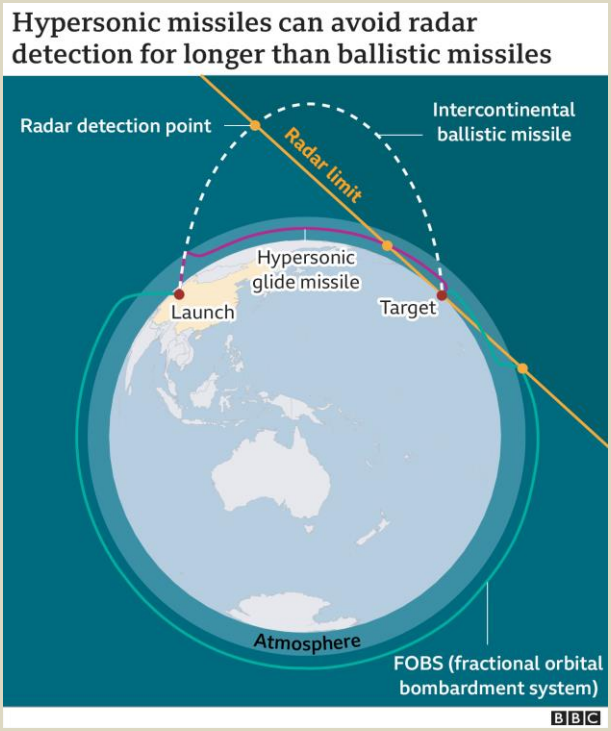
Can U.S. Missile-Defense Systems Handle China's New Missiles?

By Malcolm Davis
Source: https://www.homelandsecuritynewswire.com/dr20211028-can-u-s-missiledefense-systems-handle-china-s-new-missiles

Oct 28 – A pair of reports in the *Financial Times* have set the defense community abuzz with the suggestion that China has tested a new hypersonic glide vehicle, possibly with a fractional orbital bombardment system, or FOBS. Two possible tests—one potentially as early as 27 July and a second on 13 August—involved a Chinese Long March 2C orbital launch vehicle blasting off and flying a south polar trajectory into low-earth orbit. The rocket released a hypersonic glide vehicle that circled the globe in low polar orbit before de-orbiting and landing several kilometers from its target. China claims that it was a test of a spaceplane under its Tengyun program, but the nominated date of 16 July doesn't match up with the launch activity observed later that month and in August.
FOBS is not a new idea. The Soviet Union explored the possibility of firing ballistic missiles over Antarctica to attack the United States from the south, rather than from the north over the Arctic, during the Cold War. An early system was deployed but soon withdrawn from service when Soviet efforts turned to modernizing their intercontinental ballistic missile force and introducing independently manoeuvring multiple warheads, or MIRVs, to complicate U.S. defensive measures. The U.S. considered the idea, but never deployed a FOBS capability, and has always favored traditional ICBMs that fly over the Arctic.
But FOBS might be back. The Russians have suggested a FOBS capability for the SS-28 Sarmat heavy ICBM that will replace the SS-18 Satan, and now it looks like China may be

pursuing a FOBS too, though one that replaces traditional MIRVs with hypersonic glide vehicles. It's the FOBS–HGV combination that's new and has led to a lot of guessing by China watchers and arms-control advocates about what the test entailed and what China's intent is in pursuing such a capability.

A FOBS capability, especially if combined with a highly manoeuverable hypersonic glide vehicle, would enable the Chinese to circumvent existing and likely planned U.S. missile-defense and early warning systems. They would go through the back door, rather than try to bash down the defended and watched front door. Understanding the architecture of U.S. early warning and defense systems helps illuminate why China would test a FOBS–HGV capability now.



U.S. missile early warning starts with a network of infrared satellites that can detect a launch of an ICBM and track it through its flight. At the same time, upgraded early warning radars at Beale Air Force base in California, Fylingdales in the UK and Thule in Greenland, along with the Cobra Dane phased-array radar in Alaska and a range of other sensors, give radar tracks that cue missile interceptors for a mid-course intercept.

The U.S. national missile defense system currently consists of 40 ground-based interceptors at Fort Greely in Alaska and four at Vandenburg Air Force Base in California, with 20 more to be deployed by 2023. The system is designed to defeat a limited raid from North Korean ICBMs, not a large-scale Chinese or Russian nuclear attack. However, Beijing is clearly anxious about U.S. defensive measures.

For China, the concern driving a FOBS–HGV capability must be that U.S. missile defense will expand and become more effective over time, particularly if an expanded ground-based interceptor force were to be combined with ship-based SM-3 interceptors.

China's nuclear arsenal is small in comparison with the U.S.'s, though the recent discovery of large fields of missile silos under construction in Xinjiang and Inner Mongolia suggests that China is moving away from a 'minimum deterrent' posture and might be debating caveats on its no-first-use policy. Greater numbers of both silo-based and road-mobile ICBMs, if combined with a niche FOBS-HGV component that can strike the U.S. from the south, would certainly overwhelm any likely U.S. missile defense architecture. That would strengthen Chinese deterrence against U.S. non-nuclear strikes against China's nuclear forces, demonstrating that even an expanded U.S. capability to counter any residual Chinese nuclear retaliation wouldn't prevent a Chinese retaliation from inflicting massive damage. Of course, even a limited nuclear capability such as the one being developed by the North Korea changes decision-making, so the perceived need for Chinese nuclear expansion is less rational.

Despite hyperbolic headlines in the media, suggesting that this was a 'Sputnik moment', a Chinese FOBS capability isn't a fundamental game-changer in nuclear stability. Yet it's not unimportant or irrelevant either. The U.S. will need to respond to this increased threat.

President Joe Biden and his administration would be very unwise to now adopt a nuclear no-first-use posture, or a 'sole purpose' declaration as part of its nuclear posture review to be released in 2022. Such a stance would dramatically weaken extended nuclear deterrence, and if such a step were made against a backdrop of Chinese (and Russian) nuclear build-up and force posture changes, it would send the wrong signal to allies looking for U.S. leadership and resolve, especially after the debacle of the Afghanistan withdrawal.

Nor should the Biden administration cancel the ground-based strategic deterrent program that would replace ageing Minuteman ICBMs. Any rush to scrap ICBMs and turn the U.S. nuclear triad into a dyad would only make it easier for an adversary to deliver a decisive nuclear blow in a crisis, even if it couldn't deliver a knockout punch due to U.S. Navy ballistic missile submarines.

The U.S. should look at options for expanding its missile early warning and missile tracking coverage to deal with hypersonic glide vehicles and threats such as FOBS. Continued development of infrared surveillance satellites will be important, including the 'next-generation overhead persistent infrared' (known as 'Next Gen OPIR') constellation that will eventually complement the current space-based infrared system. Ground-based sensors such as the upgraded early warning radar network could also be expanded to cover southern launch trajectories from China and Russia.

The FOBS–HGV test presents a challenge but also an opportunity for AUKUS. The projected orbital path from China to the U.S. passes very close to the west coast of Australia. One step that Canberra could take would be to offer to host a U.S. enhanced early warning radar in Western Australia as a joint facility to allow Australia to play an even greater role in

supporting U.S. deterrence. Such a facility could complement the Jindalee over-the-horizon radar network and be a key sensor in the Defense Department's integrated air and missile defense project (AIR 6500 Phase 2). But the challenge would be for Australia to act quickly to establish such a facility, rather than make it a decades-long process that renders such a move irrelevant.
In considering how to proceed with AIR 6500 Phase 2, it's clear that having a resilient space-based sensor layer is vital to track fast-moving missile threats, especially those heading in Australia's direction. Another good move that could be done via AUKU.S. would be for Australia to work with the U.S. on Next Gen OPIR capabilities, including through sovereign satellite manufacture and launch to augment and reconstitute lost capability in a crisis. Such steps would be early and highly visible achievements for AUKU.S., reinforcing the relevance of the new agreement, which is currently struggling with the question of how to facilitate Australia's acquisition of nuclear-powered submarines.

***Malcolm Davis** is a senior analyst at ASPI.*

▶▶ **Read also:** Hypersonic Weapons: Fast, Furious…and Futile? (RUSI, UK)

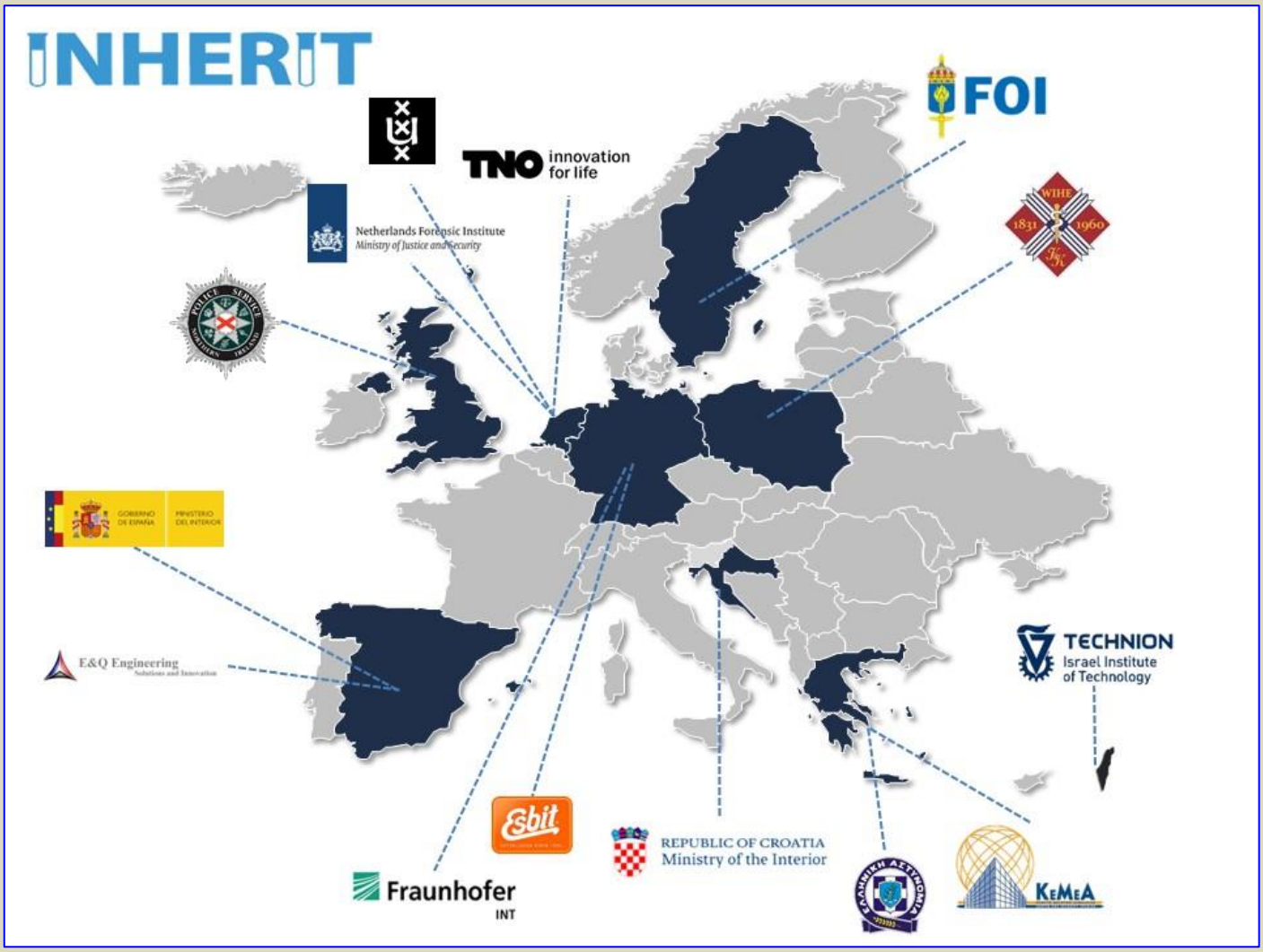
EU INHERIT Project

Source: https://h2020-inherit.eu/

The terrorism timeline consists of multiple stages. Each stage possesses vulnerabilities that can be used to disrupt a planned attack. Due to the large diversity in precursors, there is no universal approach yet that can be taken to keep a terrorist from using them to make explosives. INHERIT (INHibitors, Explosives and pRecursor InvesTigation) proposes to develop a multi-disciplined approach

to intervene across multiple stages of the terrorism timeline. INHERIT has assembled a multi-faceted team with experience of all aspects of four important steps in this timeline. With a focus on explosive precursor chemicals, the team will work to develop technologies directed towards thwarting the ability of terrorists to exploit these materials for production of explosives. Methodologies to render chemicals inert, more readily detectable and capable of yielding greater forensic value will all be pursued. Collaboration between the diverse teams developing these interventions will ensure a coordinated holistic approach across all threat materials identified. This holistic approach will also be applicable in the struggle against emerging and future HME threats. The knowledge and insight resulting from INHERIT testing and analysis will be fed to targeted authorities, legislators, and organisations through a dissemination process which will include meetings, workshops and conferences conducted at appropriate security levels.
INHERIT is funded by the European Union's Horizon 2020-Research & Innovation Framework Programme, under GA no 101021330 (1 June 2021 - 31 May 2024).

Partners



NHERIT objectives

1. To disrupt or prevent the production of HMEs
2. To disrupt or prevent the use of HMEs by markers and their detection
3. To tie a perpetrator to the crime by forensics, where the crime is in the preparatory phase
4. To assess the countermeasures and further exploit the results

A Closer Look at China's Missile Silo Construction

By Matt Korda and Hans Kristensen

Source: https://fas.org/blogs/security/2021/11/a-closer-look-at-chinas-missile-silo-construction/

Nov 02 – After the discovery during the summer of what appears to be at least three vast missile silo fields under construction near Yumen, Hami, and Ordos in north-central China, new commercial satellite images show significant progress at the three sites as well as at the People's Liberation Army Rocket Force (PLARF)'s training site near Jilantai.

The images provide a vivid and rare public look into what is otherwise a top-secret and highly sensitive construction program. The Chinese government has still not officially confirmed or denied that the facilities under construction are silos intended for missiles and there are many uncertainties and unknowns about the nature and role of the facilities.

In this article we use words like suspected, apparent, and probable to remind the reader of that fact.

Yet our analysis of hundreds of satellite images over the past three years of the suspected missile silo fields and the different facilities that are under construction at each of them have

increased our confidence that they are indeed related to the PLARF's modernization program. In recent analysis of new satellite images obtained from Planet Labs and Maxar Technologies, we have observed almost weekly progress in construction of suspected silos as well as discovered unique facilities that appear intended to support missile operations once the silo fields become operational. In this article we describe the progress we have observed. We first describe the shelters, then what we see under the shelters, unique support facilities, and end with overall observations.

▶▶ Read the full article with many sat photos at the source's URL.

Matt Korda *is a Senior Research Associate and Project Manager for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the Nuclear Notebook—an authoritative open-source estimate of global nuclear forces and trends. Matt is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Matt is also the co-director of Foreign Policy Generation—a group of young people working to develop a progressive foreign policy for the next generation. He received his MA in International Peace & Security from the Department of War Studies at King's College London, where he subsequently worked as a Research Assistant on nuclear deterrence and strategic stability. He also completed an internship with the Verification, Training and Information Centre (VERTIC) in London, where he focused on nuclear security and safeguards.*

Hans M. Kristensen *is director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons. He specializes in using the Freedom of Information Act (FOIA) in his research and is a frequent consultant to and is widely referenced in the news media on the role and status of nuclear weapons. His collaboration with researchers at NRDC in 2010 resulted in an estimate of the size of the U.S. nuclear weapons stockpile that was only 13 weapons off the actual number declassified by the U.S. government. Kristensen is co-author of the Nuclear Notebook column in the Bulletin of the Atomic Scientists and the World Nuclear Forces overview in the SIPRI Yearbook.*

EOD Soldiers field test Next Generation Advanced Bomb Suit

Source:https://www.army.mil/article/251848/explosive_ordnance_disposal_soldiers_field_test_next_generation_advanced_bomb_suit

Nov 09 – U.S. Army Explosive Ordnance Disposal Soldiers field tested the Next Generation Advanced Bomb Suit on Fort Campbell, Kentucky.

Army EOD Soldiers from the 184th Ordnance Battalion (EOD) put the new bomb suits through a series of tests at ranges on Fort Campbell over the last two weeks.

The 184th EOD Battalion is part of the 52nd EOD Group and 20th Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Command.

From 19 bases in 16 states, Soldiers and civilians from the Aberdeen Proving Ground, Maryland-headquartered 20th CBRNE Command take on the world's most dangerous threats and hazards in support of military operations and civil authorities.

The deployable command is home to 75 percent of the active U.S. Army's Explosive Ordnance Disposal technicians and Chemical, Biological, Radiological and Nuclear specialists, as well as the 1st Area Medical Laboratory, CBRNE Analytical and Remediation Activity, five Weapons of Mass Destruction Teams and three Nuclear Disablement Teams.

Staff Sgt. Gregory D. Meckel, one of the participants in the testing from the 49th EOD Company, said the Next Generation Advanced Bomb Suit has a number of advantages.

"These include improved range of motion, weight reduction and better center of gravity due to the Modular Scalable Vest, increased capabilities in a number of areas, improved helmet comfort and stability, better air flow and built in lighting capabilities," said Meckel.

Bomb suits are designed to protect EOD technicians as they accomplish their high stakes mission in support of combat operations around the world and explosive mitigation missions at home.

A New Braunfels, Texas, native who has deployed to Afghanistan and Iraq, Meckel said the new suit is an improvement over the previous suit.

"The NGABS provides greater comfort and mobility for EOD personnel when mitigating explosive threats," said Meckel.

Modern Warfare: "Precision" Missiles Will Not Stop Civilian Deaths – Here's Why

By Peter Lee

Source: https://www.homelandsecuritynewswire.com/dr20211119-modern-warfare-precision-missiles-will-not-stop-civilian-deaths-here-s-why

Nov 19 – Modern guided missiles and bombs are capable of incredible, almost science-fiction-like precision. To research my book, Reaper Force, about the lives of drone operators, I was allowed to watch RAF MQ-9 Reaper drones in real-time action in Syria. I sat with a three-person crew at a ground-control station in Creech Air Force Base in Nevada as they killed an Islamic State fighter with a Hellfire precision-guided missile. The Reaper drone being piloted was flying 20,000 feet above its target. He was on a moving motorcycle when the missile hit him.

Missile accuracy is judged by how close it gets to its aiming point. Precision refers to the size and predictability of the explosive blast. The strike I watched was accurate and precise and no civilians were hurt.

Degrees of Precision

Air-launched missile technology continues to advance rapidly. The 100-pound Hellfire missile was developed to destroy armored tanks, and its laser targeting is the most accurate system in regular use. It included 20 pounds of explosive charge, though recent versions use less explosives to reduce the risk of collateral damage and civilian deaths.

Having said that, precision can only take you so far: governments do not publish lethal blast-radius information, but a video released by the UK's Ministry of Defense shows a Hellfire blast radius of several meters. Blast is also affected by the angle at which a missile hits a target, the local topography and any nearby structures which might absorb some of the explosion. Also, even light clouds can disrupt the laser beams that laser-guided missiles like the Hellfire rely on to hit their targets accurately.

This is still much more accurate than more traditional bombs, though these are being improved for accuracy too. Traditional unguided 500-pound, 1,000-pound and 2,000-pound

"dumb" bombs are being converted into "smart" Guided Bomb Units (GBU) by attaching a Joint Direct Attack Munition (JDAM) guidance tail kit.
The JDAM contains inertial navigation – an internal computer and gyroscopes to ensure it flies straight – as well as global positioning-system guidance capabilities. They can only hit coordinates and can't "see" or avoid civilians, though unlike the Hellfire missiles, they are not affected by cloud cover. The 2,000-pound version can be lethal up to several hundred meters away but the guidance kit enables them to strike between [10 and 30 meters] of their targets.

Danger to Civilians
The development of more precise missiles and guided bombs does not automatically mean a reduction in civilian deaths. For one thing, "precision" is not about protecting civilians so much as making these weapons "more lethal".
A whole range of factors affect the civilian risk during a "precision" attack. These include the size and explosive yield of the missile or bomb; the training and experience of the aircrew involved; the quality of the military intelligence; and the operational environment in which the attack is made.
Political implications for the countries involved are also a factor. The British government, for example, has faced public scrutiny for civilian deaths in air strikes in a way that, say, the Russian president, Vladimir Putin, has not.
Much also depends on the rules of engagement – or legal guidance, because they will set out how many civilians a government is prepared, or not, to allow its air force to kill in pursuit of its military campaign objectives.

Law of War
The law of war – which includes the Geneva Conventions – requires civilians to be protected in war and not attacked. But – and this is not commonly understood – the law allows civilians to be legally killed in some circumstances: where the number of deaths is judged by the attacker not to be "excessive in relation to the concrete and [direct military advantage] anticipated". So if a target is judged to be valuable enough, and the military advantage important enough, civilians can and will be killed.
On August 29 2021, ten Afghan civilians were killed by a Hellfire missile from a US Reaper drone. The precision of the missile did not save them. The crew responsible made the mistake through a combination of human error, miscommunication and the fact that the family's Toyota Corolla had been wrongly identified as the car of an important ISIS target.
Lieutenant General Sami Said, the US air force inspector general, described it as "an honest mistake". His enquiry also found that the crew had not broken the law of war.

Sometimes Harming Civilians Is the Point
Sometimes air power is also used to directly target or coerce civilian populations. For example, in 2016 Amnesty International reported air attacks by Russian forces on Syrian hospitals. Six hospitals or medical facilities were bombed in three months in areas controlled by forces opposed to the Syrian government. Dozens of civilians were killed or injured. This, despite hospitals being explicitly protected under international humanitarian law.
Direct hits on all of those hospitals indicate the operational effectiveness of the aircraft and weapons involved. Russia was open about its use of "precision" weapons by its air force in Syria at the time. Putin spoke of Russia acting in Syria in support of its government within "the norms of international law". When he referred to Russian strike aircraft producing "positive results," it was about keeping Syria's government in power, not protecting civilians.

What Does the Future Hold?
As aerial firepower has become more sophisticated, the risks of civilian deaths also rise for other reasons. For example, IS has repeatedly demonstrated effective methods of reducing its enemy's aerial advantage, such as resorting to urban warfare and creating a network of tunnels under cities such as Mosul and Fallujah in Iraq.
In urban warfare it is impossible to avoid all civilian deaths. A camera in the sky cannot tell if there are civilians out of sight behind walls, in buildings, under trees or in tunnels. Choosing not to shoot is the only sure protection for civilians in unclear circumstances.
For all these reasons, no degree of missile precision will stop the tragedy of civilian deaths in war. And wars show no sign of ending. Perhaps it is time for a more honest dialogue about the limits of technology and the human costs involved.

Peter Lee *is Professor of Applied Ethics and Director, Security and Risk Research, University of Portsmouth.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

CYBER NEWS

C2BRNE DIARY

Facebook is changing its name to Meta as it focuses on the virtual world

Source: https://www.washingtonpost.com/technology/2021/10/28/facebook-meta-name-change/

Oct 29 – Facebook changed its corporate name to Meta on Thursday, moving aggressively to distance itself from a social-media business embroiled in crisis and rebrand itself as a forward-looking creator of a new digital world known as the "metaverse."

In a 75-minute online presentation, CEO Mark Zuckerberg urged users to adjust their thinking about the company, which he said had outgrown its ubiquitous and problematic social media app — a platform that will continue to be known as Facebook. Instead, he said, the company plans to focus on what Zuckerberg described as the next wave of computing: a virtual universe where people will roam freely as avatars, attending virtual business meetings, shopping in virtual stores and socializing at virtual get-togethers.

"From now on, we're going to be the metaverse first. Not Facebook first," Zuckerberg said at Connect, the company's annual event focused on virtual and augmented reality. "Facebook is one of the most-used products in the world. But increasingly, it doesn't encompass everything that we do. Right now, our brand is so tightly linked to one product that it can't possibly represent everything we are doing."

The move comes as Facebook is mired in controversy over allegations that it has privately and meticulously tracked real-world harms exacerbated by its platforms, ignored warnings from its employees about the risks of their design decisions and exposed vulnerable communities around the world to a cocktail of dangerous content. After a whistleblower this month turned over tens of thousands of internal company documents to Congress and the U.S. Securities and Exchange Commission, lawmakers and critics have called for urgent action to rein in the tech giant.

The revelations by whistleblower Frances Haugen represent arguably the most profound challenge yet to Zuckerberg and his company, which ranks as the largest social media platform in the world. Critics swiftly criticized the move, comparing it to the crisis strategy employed by tobacco company Phillip Morris when it became clear that the company had long known that cigarettes damage human health.

"Don't forget that when Phillip Morris changed [its] name to Altria it was still selling cigarettes that caused cancer," tweeted Democratic lawyer Marc Elias.

Zuckerberg said the rebrand would heed the "lessons" of the past, noting in a blog post that privacy and safety would be built into the new generation of products "from Day One" — a clear nod to Facebook's record of eroding trust. In his keynote address, he also nodded to Facebook's problems, saying, "The last few years have been humbling for me and my company in a lot of ways."

But Facebook's trust deficit is real. The crisis brought on by the Facebook Papers, which were provided to Congress and the Securities and Exchange Commission in response to a whistleblower lawsuit, follows other scandals in recent years, such as Russian disinformation surrounding the 2016 presidential election and the Cambridge Analytica crisis that highlighted the improper sharing of personal data.

The current crisis is more existential for the company, because the harm comes from within rather than from an outsider abusing the service. The Facebook Papers also touch every aspect of the service, exposing fundamental flaws in the architecture of its algorithms, the design of the platform, and its policies, while the harms exposed around mental health and polarization hit close to home for many Americans.

The Facebook Papers were obtained by a consortium of news organizations, including The Washington Post. Facebook has called them a "coordinated effort to selectively use leaked documents to paint a false picture of our company."

One of the major allegations of the Facebook Papers is that the company built and deployed social media technology without having a grasp of its harmful effects. Critics fear the same problems would plague the metaverse — only the stakes could be higher, as Zuckerberg pitched that people would essentially live part of their lives in his virtual world.

He sought to offset potential criticism by saying in his presentation that the next generation of Internet services would be built with greater "humility and openness," and take the "lessons" of the past into account. But critics and some former insiders questioned that commitment.

"I was thinking during the keynote, who will be the cops in the metaverse?" said Katie Harbath, founder and CEO of consultancy Anchor Change and former Facebook public policy director. "The first few years may seem great because not that many people are on the service, but the more that come on, the more bad actors. And then the company plays catch-up."

Harbath noted that roughly every five years, the company has announced a big directional change amid a bad press cycle. In 2012, the company pivoted to mobile while getting

attacked for a poor performance during its public offering. In 2017, it announced a shift to focus on communities and groups — bringing the world together — after the controversies over Russian disinformation during the previous year's presidential election.
For the time being, Facebook's name change seems aspirational. A company that Zuckerberg launched from a college dorm room 17 years ago has become a conglomerate encompassing WhatsApp, Instagram, Messenger and a nascent payments and hardware business, leading some experts and insiders to say that the company was long overdue for a name change.
But virtually all of Facebook's revenue — $29 billion in the third quarter — comes from online advertising produced by the core blue Facebook app, meaning that any transition to virtual reality focused on the sale of hardware would take enormous investment and many years.
"While the name change indicates a larger vision, that transformation is not yet a reality and will be a years-long investment," eMarketer analyst Audrey Schomer said in an email.
Zuckerberg and Facebook have acknowledged that. Zuckerberg said in his keynote that the process to become a metaverse company would take a "decade" and that his goal was for it to "reach a billion people" over that time. On Monday, the company said its investments in the metaverse — which include a commitment to hiring 10,000 new people in hardware jobs — will shave $10 billion off its 2021 profits.
Zuckerberg's keynote was filled with a dizzying array of scenes that showcased the company's vision for the metaverse. It included Zuckerberg doing his favorite water sport, hydrofoiling, with friends in a virtual environment, and then jumping into work meetings from a virtual home office, boxing with virtual avatars and working out on a virtual lily pad.
In a letter on the company's website posted shortly after the keynote, Zuckerberg said that the future would be "an embodied internet where you're in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build."
Zuckerberg began talking about how the company would transition to a new identity this summer. He subsequently announced a smart-glasses partnership with Ray-Ban and a plan to use its virtual reality headsets for work-related videoconferencing. He promoted a longtime friend who heads the hardware division, Andrew Bosworth, to become the company's new chief technology officer.
The political dimension of the rebrand also began months before Haugen emerged with the Facebook Papers. Facebook executives spent parts of the summer introducing the metaverse idea to experts in Washington think tanks and planning outreach to federal agencies that might regulate its hardware, The Post previously reported. Zuckerberg has told colleagues that he no longer wants to be the face of the company's headaches in Washington and elsewhere.
The term "metaverse" comes from science fiction and has been popularized by venture capitalists in recent years as a way to talk about interconnected services.
Facebook also isn't the first Silicon Valley company to rebrand itself. Google changed its parent company's name to Alphabet in 2015 in an attempt to unify a corporate behemoth that encompassed not only search-and-display advertising but also driverless cars and a life-sciences division. Snapchat changed its name to Snap Inc. in an attempt to rebrand itself as a camera company.
Zuckerberg said that the name "meta" was inspired by his love of the classics, and that it comes from the Greek word "beyond."
"For me, it symbolizes that there is always more to build, and there is always a next chapter to the story."

EDITOR'S COMMENT: Since the word "meta" is of Greek origin (μετά meaning beyond") the tone should be on "a" and not on "e". When you borrow something you do it as a whole and not as you like or how it sounds better. New FB is **Metá** (even if is sounds a bit French 😊)

Targeted: Masterminds of Global Ransomware Attacks Against Critical Infrastructure

Source: https://www.homelandsecuritynewswire.com/dr20211029-targeted-masterminds-of-global-ransomware-attacks-against-critical-infrastructure

Oct 29 – Twelve individuals who were wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries.
These attacks are believed to have affected over 1,800 victims in 71 countries. These cyber actors are known for specifically targeting large corporations, effectively bringing their business to a standstill.
The actions took place in the early hours of 26 October in Ukraine and Switzerland. Most of these suspects are considered high-value targets because they are being investigated in multiple high-profile cases in different jurisdictions.

As the result of the action day, over $52,000 in cash was seized, alongside 5 luxury vehicles. A number of electronic devices are currently being forensically examined to secure evidence and identify new investigative leads.

The Ticking Time Bomb of Undetected Malware

The targeted suspects all had different roles in these professional, highly organized criminal organizations. Some of these criminals were dealing with the penetration effort, using multiple mechanisms to compromise IT networks, including brute force attacks, SQL injections, stolen credentials and phishing emails with malicious attachments.

Once on the network, some of these cyber actors would focus on moving laterally, deploying malware such as Trickbot, or post-exploitation frameworks such as Cobalt Strike or PowerShell Empire, to stay undetected and gain further access.

The criminals would then lay undetected in the compromised systems, sometimes for months, probing for more weaknesses in the IT networks before moving on to monetizing the infection by deploying a ransomware. These cyber actors are known to have deployed LockerGoga, MegaCortex and Dharma ransomware, among others.

The effects of the ransomware attacks were devastating as the criminals had had the time to explore the IT networks undetected. A ransom note was then presented to the victim, which demanded the victim pay the attackers in Bitcoin in exchange for decryption keys.

A number of the individuals interrogated are suspected of being in charge of laundering the ransom payments: they would funnel the Bitcoin ransom payments through mixing services, before cashing out the ill-gotten gains.

International Cooperation

International cooperation coordinated by Europol and Eurojust was central in identifying these threat actors as the victims were located in different geographical locations around the world.

Initiated by the French authorities, a joint investigation team (JIT) was set up in September 2019 between Norway, France, the United Kingdom and Ukraine with financial support of Eurojust and assistance of both Agencies. The partners in the JIT have since been working closely together, in parallel with the independent investigations of the Dutch and U.S. authorities, to uncover the actual magnitude and complexity of the criminal activities of these cyber actors to establish a joint strategy.

Eurojust established a coordination center to facilitate cross-border judicial cooperation during the action day. In preparation of this, seven coordination meetings were held.

Europol's European Cybercrime Centre (EC3) hosted operational meetings, provided digital forensic, cryptocurrency and malware support and facilitated the information exchange in the framework of the Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol's headquarters in The Hague.

More than 50 foreign investigators, including six Europol specialists, were deployed to Ukraine for the action day to assist the National Police with conducting jointly investigative measures. A Ukrainian cyber police officer was also seconded to Europol for two months to prepare for the action day.

This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

Hackers-for-Hire Drive Evolution of Threat Landscape

Source: https://www.homelandsecuritynewswire.com/dr20211101-hackersforhire-drive-evolution-of-threat-landscape

Nov 01 – The ENISA Threat Landscape 2021 (ETL) report is the annual report of the EU Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape. The 9th edition covers a period of reporting starting from April 2020 up to July 2021.

ENISA says that cybersecurity threats are on the rise. Ransomware ranks as a prime threat for the reporting period. For each of the identified threats, attack techniques, notable incidents and trends are identified alongside recommendations. The new report also features a list of trends concerning threat actors.

The cybersecurity threat landscape has grown in terms of sophistication of attacks, complexity and impact. Such a trend is spurred by an ever-growing online presence, the transitioning of traditional infrastructures to online solutions, advanced interconnectivity and the exploitation of new features of emerging technologies.

Without surprise, supply-chains attacks rank highly among prime threats because of the significant potential they have in inducing catastrophic cascading effects. The risk is such that ENISA recently produced a dedicated threat landscape report for this specific category of threat.

The 9 Top Threats

Nine threat groups were identified due to their prominent materialization over the reporting period.

1. Ransomware;
2. Malware;
3. Cryptojacking;
4. E-mail related threats;
5. Threats against data;
6. Threats against availability and integrity;
7. Disinformation – misinformation;
8. Non-malicious threats;
9. Supply-chain attacks.

Key Trends

The COVID-19 crisis has created possibilities for adversaries who used the pandemic as a dominant lure in campaigns for email attacks for instance. Monetization appears to be the main driver of such activities.

The techniques that threat actors are resorting to are numerous. The non-exhaustive list below presents some of the most prevalent ones identified in the report, across all threats:

- Ransomware as a Service (RaaS)-type business models;
- Multiple extortion ransomware schemes;
- Business Email Compromise (BEC);
- Phishing-as-a-service (PhaaS);
- Disinformation-as-a-Service (DaaS) business model; etc.

Focus on three threats

Ransomware

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Ransomware has been the prime threat during the reporting period, with several high profile and highly publicized incidents. The significance and impact of the threat of ransomware is also evidenced by a series of related policy initiatives in the European Union (EU) and worldwide.

Compromise through phishing e-mails and brute-forcing on Remote Desktop Protocol (RDP) services remain the two most common infection vectors. The occurrence of triple extortion schemes also increased strongly during 2021 and cryptocurrency remains the most common pay-out method for threat actors.

Cryptojacking infections

Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. With the proliferation of cryptocurrencies and their ever-increasing uptake by the wider public, an increase in corresponding cybersecurity incidents has been observed. Cryptocurrency remains the most common pay-out method for threat actors.

Misinformation and disinformation

This type of threats makes its first appearance in the ENISA threat landscape report.

Disinformation and misinformation campaigns are on the rise as a result of the increased online presence due to the COVID-19 pandemic logically leading to an overuse of social media platforms and online media.

Such threats are of paramount importance in the cyber world. Disinformation and misinformation campaigns are frequently used in hybrid attacks to foster doubt or create confusion, therefore reducing the overall perception of trust as a consequence and damaging this major proponent of cybersecurity in the process.

Threat Actors: Who Are They?

Cyber threat actors are an integral component of the threat landscape. They are entities aiming to carry out a malicious act by taking advantage of existing vulnerabilities, with the intent to do harm to their victims. Understanding how threat actors think and act, what their motivations and goals are, is an important step towards a stronger cyber incident response. Monitoring the latest developments with respect to the tactics and techniques used by threat actors to achieve their objectives is crucial for an efficient defense in today's cybersecurity ecosystem. Such threat assessment allows us to prioritize security controls and devise an adequate strategy based on the potential impact and likelihood of threat materialization.

For the purposes of the ETL 2021, focus was given to four categories of cybersecurity threat actors: state-sponsored, cybercrime, hacker-for-hire actors and hacktivists.

Background

The ETL report maps the cyber threat landscape in a means to help decision-makers, policy-makers and security specialists define strategies to defend citizens, organizations and cyberspace.

This work is part of the EU Agency for Cybersecurity's annual work program to provide strategic intelligence to its stakeholders.

The report's content is gathered from open sources such as media articles, expert opinions, intelligence reports, incident analysis and security research reports; as well as through interviews with members of the ENISA Cyber Threat Landscapes Working Group (CTL working group).

The Three Horsemen of Cyber Risks: Misinformation, Disinformation, and Fake News

Source: https://www.homelandsecuritynewswire.com/dr20211101-the-three-horsemen-of-cyber-risks-misinformation-disinformation-and-fake-news

Nov 01 – Misleading information has emerged as one of the leading cyber risks in our society, affecting political leaders, nations, and people's lives, with the COVID-19 pandemic having only made it worse. However, it also affects something we rarely stop to consider: business. But how do organizations prepare against such threats? A new study, in *Business Horizons*, published by Elsevier, maps out the risk factors associated with misinformation, disinformation and fake news—proposing practical ways to manage risks in the parlance of business.

Industry 4.0 has brought about a metamorphosis in the world of business. The new revolution demands the integration of physical, biological and digital systems under one roof. Such a transformation, however, comes with its own set of risks. Misleading information, including misinformation, disinformation and fake news, often has damaging effects on the public image of political leaders and, as the COVID-19 crisis has clearly shown, on the general public and the economy. However, the consequences of misinformation on business organizations have been far less explored.

"Information has always played an irrefutable role in economics," said **Dr. Pythagoras N. Petratos of Coventry University's Business School**, whose research, examines the various forms of misleading information, identifying the cyber threats associated with them, and providing recommendations on tackling such risks. "We need to pay attention to the quality of information disseminated into the world, now more than ever, as spreading misinformation has become a lot easier with the advent of digital transformation.

"My research attempts to bridge the divide between academic research and real-world practice of cyber risk management."

The fake news "infodemic" that spread alongside the COVID-19 pandemic also affected the finance sector. For instance, during the lockdown period of 2020, there was a huge surge in fake news and illegal activity related to the financial and other markets. Financial firms had to train their staff to deal with fraudulent online schemes and reports.

Deliberate spreading of disinformation has also been responsible for swaying the outcome of elections. Cyber attackers have used misleading information on social media for procuring campaign finances as well as personal and financial information of people and corporations. These actions undermine a nation's security and make them vulnerable to geopolitical risks.

To deal with these cyber risks, businesses and authorities need to establish cybersecurity practices and policies that can evolve and adapt to the multifaceted cyberthreats. Executives and leaders should be trained to recognize cyber threats when they see one. To enable faster recognition, firms need to embrace modern computing software that fits their work criteria and can detect, report, and effectively manage cyber threats.

Anti-misinformation strategies such as having human fact-checkers for websites or artificial intelligence for bot detection on social media could be used to prevent the damage caused by propagation of misleading information. Partnerships between private and public sectors can also mitigate cyber risks by forming a united front with better cyber defenses and funds to invest in cyber security technologies.

All in all, the study provides a primer on the risks associated with misleading information in the sphere of business and the ways to avoid them, highlighting the fact that businesses are not immune to them either.

"Fake news is not a new phenomenon, but the COVID-19 pandemic, the ongoing digital transformations, and advances in big data have exacerbated it. Business executives and leaders across an array of industries, organizations, and nations, as well as the public, need to become aware of such risks and find innovative ways to manage them," concludes Dr. Petratos.

Israeli Cyber Experts: What's Behind the Cyberattack on Iran?

Source: https://i-hls.com/archives/111327

Oct 27 – A cyberattack on Iran has disrupted the sale of subsidized fuel in Iran on October 26, causing the shutting down of a government system managing fuel subsidies, state media reported.

The attack, that has caused long queues at gas stations across the country comes weeks before the anniversary of 2019 street protests that followed fuel price hikes.

Who could have been behind the attack and what was it trying to gain? "I think that the attack was perpetrated by a state actor and not by some kind of a small group," claims Guy Mizrahi, a serial entrepreneur and a cyber expert, in a special interview with iHLS. "The reason is we are talking about a multidisciplinary attack, involving both IT capabilities and capabilities that have consequences on OT and SCADA products".

"I find it most interesting to ask why a state actor would want to perpetrate such attack when it actually didn't cause economic damage to the Iranian state, but rather to citizens' resentment against the establishment," Mizrahi asks. "The question arises why the attacking body will decide to burn capacity for gaining a profit that is confined to psychological warfare?"

Is it possible that this is a matter of making war on Iranian public opinion a high priority? The question remains open to interpretation. Can an attack of this magnitude occur against Israel? Mizrahi estimates that "in Israel, the situation is different since the fuel market is distributed among several companies and is not concentrated in one place as in Iran. In order to achieve a significant effect in Israel, an attack on port facilities and refineries is required."

Another aspect of the attack is the ongoing cyber conflict in the Middle East, says Boaz Dolev, CEO, Clearsky, a cyber intelligence company operating in Israel during the last decade. "The assailants in this conflict come not only from the Middle East but also from the US, China, and Russia."

Why did the attackers choose this mode of operation? Dolev believes that the attack on the refueling cards in Iran was intended to create deterrence and send a hint to the Iranians. "We discovered a Telegram channel that relates to the attack and claims responsibility. Moreover, it appears that emergency organizations in Iran had been alerted to refuel their vehicles before the attack, apparently in order to refrain from risking human lives. This may prove that the attack was perpetrated by a state actor and not by criminals. However, we do not have the means to trace the attack to a specific actor."

During the last three years, there has been an ongoing conflict between Israel and Iran in the cyber arena. Dolev believes that the recent attack should be seen over the backdrop of Iranian attacks against Israel in the last several weeks. "The attack may have been a signal to the Iranians that they had crossed the line". "In any event, Israel's cyber capabilities are far more powerful than Iran's capabilities," Dolev concludes.

Interpol Unveils Emerging Cyberthreats

Source: https://www.homelandsecuritynewswire.com/dr20211112-interpol-unveils-emerging-cyberthreats

Nov 12 – The accelerated digitalization related to the COVID-19 pandemic has significantly influenced the development of a number of cyber threats, according to the new edition of Europol's Internet Organised Crime Threat Assessment. Criminals have been quick to abuse the current circumstances to increase profits, spreading their tentacles to various areas and exposing vulnerabilities, connected to systems, hospitals or individuals. While ransomware groups have taken advantage of widespread teleworking, scammers have abused COVID-19 fears and the fruitless search for cures online to defraud victims or gain access to their bank accounts. The increase of online shopping in general has attracted more fraudsters. With children spending a lot more time online, especially during lockdowns, grooming and dissemination of self-produced explicit material have increased significantly. Grey infrastructure, including services offering end-to-end encryption, VPNs and cryptocurrencies continue to be abused for the facilitation and proliferation of a large range of criminal activities. This has resulted in significant challenges for the investigation of criminal activities and the protection of victims of crime.

In addition to expanding the efforts to tackle these threats from a law enforcement perspective, it is crucial to add another level of protection in terms of cybersecurity. The implementation of measures such as multi-factor authentication and vulnerability management are of utmost importance to decrease the possible exposure to cyber

threats. Awareness raising and prevention are key components in reducing the effectiveness of cyberattacks and other cyber enabled criminal activities.

The Key Threats

- Ransomware affiliate programs enable a larger group of criminals to attack big corporations and public institutions by threatening them with multi-layered extortion methods such as DDoS attacks.
- Mobile malware evolves with criminals trying to circumvent additional security measures such as two-factor authentication.
- Online shopping has led to a steep increase in online fraud.
- Explicit self-generated material is an increasing concern and is also distributed for profit.
- Criminals continue to abuse legitimate services such as VPNs, encrypted communication services and cryptocurrencies.

The new edition of Europol's Internet Organized Crime Threat Assessment, launched today, looks into the (r)evolutionary development of these trends, catalyzed by the expanded digitalization of recent years. The report was presented during the Europol-INTERPOL Cybercrime Conference. The conference gathered about 100 experts together to share their insights into the latest cybercrime trends and threats and to discuss how innovation is essential in countering cybercrime acceleration.

High Value Targets: The New Victims of Malware Attacks

Ransomware groups have used the pandemic to their advantage to launch more sophisticated and targeted attacks. While mass distributed ransomware seems to be in decline, cybercrime groups and their affiliates opt for well-orchestrated manual attacks against large corporations and government institutions. Always driven by opportunities for larger profits, in the past criminals have targeted companies which have both the financial capability to pay large ransoms and the need to rapidly resume operations in case of a successful cyberattack, which affects their main activities. The attacks on Kaseya and SolarWinds show how criminals have realized the potential in attacking digital supply chains, often going for the 'weakest link'. However, many of the most infamous groups have reduced the attacks on governments and social services in an attempt to limit the attention of law enforcement on them. DDoS attacks have re-emerged and are targeting service providers, financial institutions and businesses. Claiming to be part of two well-known threat groups, they have asked for significant ransoms. The pandemic has also facilitated the breakthrough of other threats, which were already making significant attempts to penetrate the cyberspace. Mobile malware and specifically banking Trojans have also been equipped with capabilities to intercept text messages on Android devices, compromising the two-factor authentication security protocols.

Alarming Rise of Self-Produced Explicit Materia

Child abusers have exploited the increased, unsupervised presence of children online during the pandemic in order to increase their grooming activities. The acceleration of production and dissemination of child sexual exploitation material is also fueled by the proliferation of encrypted messaging applications and social media platforms. Online gaming and communication, the reduction of real-life social activities and the normalization of sexual behavior online are circumstances, which are abused by predators to target a larger number of victims. These factors create conditions for the victimization of children online during a longer period. A key threat is the production of self-generated material, an alarming trend, which younger children are also exposed to. Lured by offenders using fake identities on gaming platforms and social media, more and more young children are falling into the trap of producing and sharing explicit material. Recording without the knowledge of the victims and the further dissemination of live-streamed sexual material is another alarming threat, referred to as 'capping'. Peer-to-peer networks remain a key channel for the exchange of child abuse material, along with the Dark Web.

Semper Wi-Fi: Marine Corps launches into cyberwar with 4 new jobs for Marines

Source: https://taskandpurpose.com/news/marine-corps-cyber-warfare-jobs/

Aug 05 – The Marine Corps is adding four new jobs for those hoping to fight on the front lines with ones and zeros.

On Tuesday, the service announced it was creating four new military occupational specialties: 1712, Interactive On-Net Operator; 1713, Exploitation Analyst; 1722, Host Analyst; and 1723, Network Analyst, according to an administrative message released by the deputy commandant for information. The Corps also updated its specialty of cyber warfare operator (1721) and ditched the role of offensive cyberspace operator (1711) entirely.

The changes are the latest effort by the Corps to build a "professional cyber workforce" after debuting the new '17XX' cyberspace occupation field in September 2018 and later deploying

"tactical cyber teams" alongside the Navy in the Pacific. Notably, the new roles essentially create a well-rounded Marine hacker force to defend U.S. military networks and attack the networks of adversaries like China and Russia.

Marines from lance corporal to gunnery sergeant can now take on the primary military occupational specialty of Cyber Warfare Operator (1721) who "employ offensive and defensive cyber tools, tactics, techniques, and procedures," according to the job summary, which suggests they can hack in support of strategic, operational, and tactical objectives.

U.S. Marines serve as the "Red Team" for Cyber Yankee at Joint Base Cape Cod, MA, June 14-18, 2021. Cyber Yankee is a regional cybersecurity exercise designed to promote interoperability of National Guard cyber operators among the New England states and build readiness to respond to network attacks.

Operators will also be trained to "emulate" the tricks of the other side to help find vulnerabilities in Department of Defense networks.

The three other professions are called "necessary" military occupational specialties as they allow for additional training to complement a primary job. Marines in several intelligence and cyber fields can pick up additional training as an interactive on-net operator, or 1712, which are described as "technical experts in defensive and offensive cyber operations" whose duties will vary as they advance in rank from lance corporal to master gunnery sergeant. But they can likely expect to probe enemy networks and work to develop stealthy ways to get inside, according to the Army's description of a similar job.

Marine exploitation analysts (1713) will require "advanced cyber analytical training" since they are primarily tasked with developing exploits to take over an adversary computer system. "Analysts must be experts with adversary systems, networks, technologies, tools, techniques, and procedures," says the summary for the job, meaning that analysts will be trained to find ways to manipulate, disrupt, or destroy enemy networks.

U.S. Marine Corps Sgt. Che McReynolds, a satellite chief with General Support Company, 8th Communication Battalion, conducts signal connectivity on a Very Small Aperture Terminal Large during Exercise Cyber Fury 21, at Camp Lejeune, North Carolina, July 26, 2021. The VSAT-Large enables command and control by pushing critical C2 infrastructure to the furthest edge of the battlespace. Cyber Space 21 is the third iteration of this exercise designed to enhance the capabilities of Delta Company by simulating a series of cyberspace attacks in order to sharpen and hone cyberspace defensive countermeasures. McReynolds is a native of Decatur, Illinois. (U.S. Marine Corps photo by Cpl. Armando Elizalde)

Marine network analysts with the 1723 specialty appear to be defensive roles responsible for analyzing network traffic on U.S. military networks to "discover anomalies" long before adversary hackers gain full access and potentially steal sensitive data. Their cohorts in the 1722 specialty, host analysts, will need to possess "advanced knowledge" of services on the Windows, Unix and Linux operating systems.

The addition of new roles in the Marine Corps' growing cyber force comes several years after then-Marine Commandant Gen. Robert Neller laid out his vision for recruiting the right people to take on emerging threats that are vulnerable to digital attacks, such as drones and enemy communications nodes.

In a 2018 speech at the Naval War College in Newport, Rhode Island, Neller said the Corps needed to be "more flexible" in order to retain cyber warriors and offer them a career trajectory that will keep them in uniform, according to a Fifth Domain report.

"If you get qualified as a cyber Marine, you ain't ever leaving, unless you want to," Neller said, portraying the Corps as already being in the middle of a digital battle, according to the site, which quoted Neller as saying the Corps was in "phase 2.5 against potential countries and adversaries," an apparent reference to the five stages of military operations.

Weeks after Neller's speech, the Corps released its 87-page manual on cyberspace training and readiness, which established standards for how cyber Marines would operate. The core "mission-essential" tasks for the new force included planning, directing, and conducting both offensive and defensive cyberspace operations. The Corps stood up its first defensive cyber company the following month.

More recently, the Corps created a voluntary "cyber auxiliary" force to help with cyber and IT issues in February 2020 and deployed defensive cyber operators aboard the USS America in April 2020, according to Fifth Domain. Marines on the flagship were focused on "proactively" defending the networks of the America Expeditionary Strike Group.

The strike group and its embarked Marines from 1st Battalion, 7th Marine Regiment is currently underway in the South Pacific, according to the U.S. Naval Institute.

"We need to educate and train to the constant changes and advancements to our communication infrastructure in today's world," said Capt. Neal McGaughey, a cyberspace warfare development officer, in October 2020. "The enemy is developing new strategies to achieve dominance in the information environment. The Marine Corps has proven our adaptability to always remain the most effective and lethal force in the world; this applies to the information domain as well."

Experts call for 'Geneva Convention' for cybersecurity at Abu Dhabi Strategic Debate

Source: https://theshillongtimes.com/2021/11/15/experts-call-for-geneva-convention-for-cybersecurity-at-abu-dhabi-strategic-debate/

Nov 15 – Emerging disruptive technologies are changing the rules of the game as they are too complex to manage and collaborative effort is needed to tackle cybersecurity threats, top experts said at an event in Abu Dhabi on Sunday. "Cybersecurity cannot be impacted by a single entity. It needs to be a collaborative effort and we need to have a 'Geneva Convention' for cybersecurity," Dr. Mohamed Hamad Al Kuwaiti, Head, Cybersecurity in the United Arab Emirates Government, said during a panel discussion of the Abu Dhabi Strategic Debate (ADSD). Dr. Fabio Rugge, Head, the Centre on Cybersecurity of the Italian Institute for International Political Studies (ISPI), said events like the ADSD create awareness about the importance of cybersecurity. "Cybersecurity is a team sport. We need to involve academics, governments and ordinary citizens to create a culture of security and develop norms of cybersecurity. Cyberspace has become a critical element of national security and is the domain of ambiguity. We are witnessing a security paradox in which everyone is engaged in reinforcing their own security but we are actually becoming less secure," he said during a panel on 'Technology, Cybersecurity, and the Future of Global Politics'. Al Kuwaiti added that cyber-attacks are happening every moment and there was a need for effective rules. "Data is the next oil, and private companies own a lot of the infrastructure and they play with this data, therefore rules need to be laid down. No one nation can deal with cybersecurity ambiguity, it needs collaboration." Jean-Marc Rickli, Head, Global and Emerging Risks at the Geneva Centre for Security Policy (GCSP), said the convergence of power today is not witnessed in history. "Once technology is developed, the rate of proliferation is enormous, which has security implications," he said, citing the example of deep fake, which did not exist before 2014. "Increasingly, with the development of technology, we will be able to tap directly into human brains, and we may see brain-computer interfaces. With the rapid rise of new technologies, we are seeing a convergence of power and wealth into the hands of a few companies and individuals that we have not seen before." Dr. Hadi Saleh, Associate Professor of the School of Software Engineering, Higher School of Economics (HSE), Moscow, and Lead Solution Architect, said artificial intelligence has become an essential part of our everyday lives and entities cannot use traditional methods to tackle attacks anymore.

"We need to provide more training in cybersecurity for employees, and introduce it into our schools and universities for ordinary people. Cybersecurity needs to become part of our culture. The gap between hackers and government capabilities in cybersecurity is becoming smaller by the day." Saleh added that artificial intelligence enhances accuracy in detecting and improving the response system. The two-day Abu Dhabi Strategic Debate brings together top decision-makers, strategic studies experts, and scholars from all over the world to focus on the regional and international environments in the post-Covid era.

EU Agency Reports 47% Rise in Cybersecurity Incidents in the Health Sector in 2020

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/eu-agency-reports-47-rise-in-cybersecurity-incidents-in-the-health-sector-in-2020/

Nov 15 – The European Union Agency for Cybersecurity (ENISA) says cyber-attacks on the health sector have risen by almost 50%.

In 2020, ENISA received a total of 742 reports about cybersecurity incidents with a significant impact on critical infrastructure under the Directive on security of network and information systems (NIS Directive). The health sector saw an increase of 47% of such incidents in 2020 compared to the previous year.

Cybersecurity attacks on healthcare can threaten lives and affect the entire health supply chain with damaging consequences for all stakeholders concerned such as citizens, public authorities, regulators, professional associations, industries, small and medium enterprises.

The number of cyber threats over the years is now rising proportionally to the growing popularity of emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), big data, cloud computing and the multiplicity of connected devices, among others.

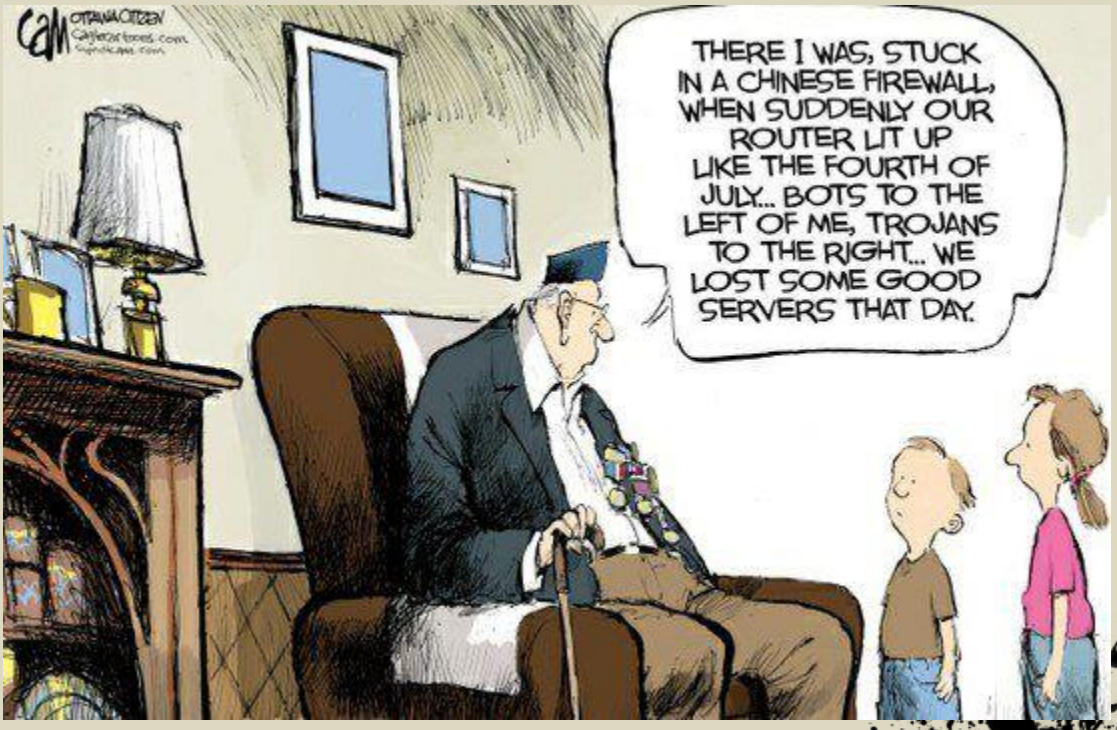
It is the role of Computer Security Incident Response Teams (CSIRTs) to develop the capabilities needed to address such issues and implement the NIS Directive provisions.National CSIRTs are the entities in charge of incident response in the health sector. Although dedicated health sector CSIRTs are still the exception in the Member States, sector specific CSIRT cooperation is developing.

ENISA says there is a lack of security culture among Operators of Essential Services within the EU. Because the pace of updates quickly outruns the pace of IT technology evolution when healthcare equipment usually has a lifetime of 15 years on average, vulnerabilities tend to accumulate with the obsolescence of the IT layer through the lifecycle of hardware and digital devices. Another challenge the healthcare sector is faced with is the complexity of systems due to the increased number of connected devices leading to an extension of the potential attack surface.

The key force driving the development of incident response capabilities of CSIRTs is the information related to security requirements and responsibilities of organizations for each sector. Shared frameworks for incident classification and threat modelling, education activities and a network allowing communication between incident response actors constitute the main resources and tools currently supporting the development of incident response capabilities.

National health sectoral CSIRTs tend to provide services better suited to the sector. Because sectoral health CSIRTs remain scarce in an environment where specialized support is needed to develop incident response activities, ENISA recommends aiding the creation of health sector CISRTs by allowing easy access to funding, and promoting capacity building activities.

The health CSIRTs could then assist Operators of Essential Services to develop their incident response capabilities, ENISA says, by establishing sector-specific regulations, cooperation agreements, communication channels, and public-private partnerships.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

The Technical Obstacles to Afghan Drone War

By Sarah Kreps and Paul Lushenko (Brookings)

Following the U.S. withdrawal from Afghanistan, the Biden administration appears to be embracing an "over-the-horizon" strategy of carrying out drone strikes against terrorist targets in Afghanistan. This relies on what one analyst describes as "cooperation with local partners and selective interventions of air power, U.S. special operations forces, and intelligence, economic, and political support from regional bases outside of Afghanistan for the narrow purpose of counterterrorism." This strategy assumes, however, that the U.S. has the requisite technical infrastructure and intelligence sharing agreements in place to enable the targeting of high-value terrorists in Afghanistan.

DroneWISE

Source: https://dronewise-project.eu/

DroneWISE recognizes that the illegal use of UAVs is now a serious security concern across the world as terrorists, activists and criminals are adopting drone technology and developing new, creative and sophisticated ways in which to commit crime, terrorism and invade the privacy of citizens. The adoption of drones as a tactical attack planning option for terrorists to cause mass disruption, damage economic stability and directly threaten EU security and the safety of its citizens is a chilling reminder of the clear and present danger from contemporary terrorism. Reinforcing this new and emerging threat, during August 2019, EU Security Commissioner Julian King warned that drones could be used for acts of terrorism stating that: "Drones are becoming more and more powerful and smarter which makes them more and more attractive for legitimate use, but also for hostile acts." The warning followed the publication of a secret report issued in December 2018 from France's Anti-Terrorism Unit (UCLAT) to the country's Special Committee on Terrorism. The report warned of "a possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents." To address these current vulnerabilities, **DroneWISE will develop a holistic first-responder agency command, control and coordination strategy, underpinned by evidence-based training for the counter-terrorism protection of public spaces. DroneWISE will serve to increase the preparedness of first-responder agencies to better coordinate their efforts, significantly improving the protection of public spaces and coordinated response to a terrorist attack using UAVs**.

Consortium

DroneWISE is constituted of 6 partners representing 5 member states including Bulgaria (European Institute Foundation), Croatia (University of Applied Sciences Velika Gorica | RiniGARD d.o.o.), Estonia (Saher [Europe] OU), Germany (University of Applied Sciences for Public Service in Bavaria) and Greece (Center for Security Studies – KEMEA), bringing forward a broad European perspective.

DroneWISE presented at seminar CEPOL drone event

DroneWISE partner SAHER (Europe) presented at the CEPOL Unmanned Aerial Vehicles – Threats & Opportunities for Law Enforcement event, hosted by the Estonian Academy of Security Studies, 19-22nd October in Tallinn.

Attended by Law Enforcement Agency officers representing 21 EU member states, including representation of drone and counter-drone represenatatives from Europol, Frontex, European Commission DG Home and the United Nations Office for Drugs and Crime (UNODC), the diverse 4-day training programme covered police operations, legislation, drone capabilities, field tests and virtual reality exercises.

Andrew Staniforth, Director of Innovation at SAHER (Europe) stated: "The CEPOL event provided an excellent opportunity to share lessons learned from the DroneWISE project, particularly in the domain of drone threat assessments and the impact of the weaponisation for drones and actors with hostile intentions. We were delighted to contribute to this event which had gathered together an excellent group pf police drone pilots, technicians and senior leaders from across the EU to share knowledge and expertise on the police use of drones and their efforts to counter drone threats."

CSS Analyses in Security Policy
No. 292, October 2021
CSS ETH Zürich

Dominika Kunertova

From Robots to Warbots: Reality Meets Science Fiction

The ongoing robotization of armed forces raises concerns about the desirability of autonomous systems with lethal capacity. In contrast, unarmed military robots have already improved and supplied capabilities unconstrained by human physical limitations. But despite the long-term efforts to develop fully autonomous systems, no military robot can lift the fog of war.

Dominika Kunertova *is a Senior Researcher in the Global Security Team at the Center for Security Studies (CSS) at ETH Zürich*

The Future of the Global Drone Market Will Not Be 'Made in Europe'

Dominika Kunertova | Monday, Oct. 4, 2021

A Eurodrone, produced by Airbus, Dassault and Leonardo, June 18, 2019 (photo by Anna Zvereva).

Europe's efforts to build its own unmanned aerial vehicle, known as the Eurodrone, got a boost with new funding from the European Union this summer, but that will not save the project from obsolescence. Large drones are going global, rapidly becoming more weaponized and diverse, but European countries are still muddling through with the development of their own indigenous, long-endurance drone.

Even with the additional $115 million that was announced in June through the EU's European Defense Fund, the large, fully European-made surveillance drones will only be available for delivery to customers by 2029. That is almost 35 years after the first deployment of U.S.-made Predator drones in the early 1990s. ...

Likely Drone Attack On U.S. Power Grid Revealed In New Intelligence Report

By Joseph Trevithick

Source: https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report

Nov 04 – U.S. officials believe that a DJI Mavic 2, a small quadcopter-type drone, with a thick copper wire attached underneath it via nylon cords was likely at the center of an attempted attack on a power substation in Pennsylvania last year. An internal U.S. government report issued last month says this is the first time such an incident has been officially assessed as a possible drone attack on energy infrastructure in the United States, but that this is likely to become more commonplace as time goes on. This is a reality *The War Zone*

has sounded the alarm about in the past, including when we were first to report on a still-unexplained series of drone flights near the Palo Verde nuclear powerplant in Arizona in 2019.

ABC News was first to report on the Joint Intelligence Bulletin (JIB) covering the incident in Pennsylvania last year, which the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) published on Oct. 28, 2021. The document, which *ABC* obtained a copy of — but released only a small portion of — is marked unclassified, but some parts are labeled Law Enforcement Sensitive (LES) and For Official Use Only (FOUO). Other outlets have

since obtained copies of this document, which reportedly says this likely attack took place on July 16, 2020, but it does not identify where the substation in question was located.

A portion of an annotated satellite image from a US Joint Intelligence Bulletin regarding a likely attempted drone attack on a power substation in Pennsylvania in 2020.

"This is the first known instance of a modified UAS [unmanned aerial system] likely being used in the United States to specifically target energy infrastructure," the JIB states. "We assess that a UAS recovered near an electrical substation was likely intended to disrupt operations by creating a short circuit to cause damage to transformers or distribution lines, based on the design and recovery location."

ABC and other outlets have reported that the JIB says that this assessment is based in part on other unspecified incidents involving drones dating back to 2017. As already noted, *The War Zone* previously reported on another worrisome set of incidents in 2019 around Arizona's Palo Verde Generating Station, the largest nuclear power plant in the United States in terms of its electrical output. In the process of reporting that story, we uncovered other reported drone flights that prompted security concerns near the Limerick Generating Station nuclear power plant in Pennsylvania earlier that year.

A low-quality image showing the drone recovered after the likely attempted attack in Pennsylvania. The green lines are the nylon cables. A copper wire was attached to the bottom ends of both lines.

"To date, no operator has been identified and we are producing this assessment now to expand awareness of this event to federal, state, local, tribal, and territorial law enforcement and security partners who may encounter similarly modified UAS," the JIB adds.

Beyond the copper wire strung up underneath it, the drone reportedly had its camera and internal memory card removed. Efforts were taken to remove any identifying markings, indicating efforts by the operator or operators to conceal the identifies and otherwise make it difficult to trace the drone's origins.

It's unclear how much of a threat this particular drone posed in its modified configuration. The apparent intended method of attack would appear to be grounded, at least to some degree, in actual science. The U.S. military employed Tomahawk cruise missiles loaded with spools of highly-conductive carbon fiber wire against power infrastructure to create blackouts in Iraq during the first Gulf War in 1991. F-117 Nighthawk stealth combat jets dropped cluster bombs loaded with BLU-114/B submunitions packed with graphite filament over Serbia to the same effect in 1999.

Regardless, the incident only underscores the ever-growing risks that small drones pose to critical infrastructure, as well as other civilian *and* military targets, in the United States. If this modified drone did pose a real risk, it would also highlight the low barrier to entry to at least attempt to carry out such attacks. New DJI Mavic 2s can be purchased online right now for between $2,000 and $4,000.

The technology is so readily available that non-state actors around the world, from terrorists in the Middle East to drug cartels in Mexico, are already employing commercial quad and hexacopter-type drones armed with improvised explosive payloads on a variety of targets on and off more traditional battlefields. This includes attempted assassinations of high-profile individuals.

The U.S. government is *finally* coming to terms with these threats and there are certainly some steps being taken, at least at the federal level, to protect domestic civilian and military facilities against small drones. At the same time, it is equally clear there is still much work to be done.

This particular incident in Pennsylvania last year highlights separate security concerns relating to Chinese-made small drones that are now widely available in the United States and are even in use within the U.S. government. DJI, or Da Jiang Innovations, is by far the largest Chinese drone maker selling products commercially in the United States today, and it has been at the center of these debates in recent years.

Whether or not the modified Mavic 2 posed a real danger in this instance or if this was truly the first-ever attempted drone attack on energy infrastructure in the United States, it definitely reflects threats are real now and will only become more dangerous as time goes on.

UPDATED: A reader has been able to identify the location of the electrical substation and where the drone was recovered based on the partial map from JIB. The substation and adjacent building are across the way from the Hershey Company's old chocolate factory in Hershey, Pennsylvania. This is also relatively close to the Hersheypark amusement park.

A satellite image showing the old Hershey chocolate factory in Hershey, Pennsylvania, and the substation to the immediate northeast.

A closer view of the substation and adjacent building where the drone was recovered last year.

The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant

Source: https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

The mysterious case of mass drone incursions over America's most powerful nuclear power plant that only resulted in more questions and no changes.

New Tech for Underground Screening

Source [+video]: https://i-hls.com/archives/111463

Nov 05 – A ground-penetrating radar integrated into a drone is expected to provide a solution for industrial, hydrographic, urban, and environmental data collection with the use of a GPR, magnetometers, methane detectors, and more.
SPH Engineering and Hexadrone partner to integrate **TUNDRA drone** with ground-penetrating radar.

A recent test flight conducted in Latvia confirmed the compatibility of the drone with a GPR sensor to perform near surface surveys.
Main advantages of the Tundra drone include a modular and multipurpose body that can be integrated with almost any payloads, accessories, and modules available on the market or in development.
Available in different configurations, it can fly up to 1 hour without payload, 50 minutes with a 1,5kg payload, and 30 minutes with the max payload – 4kg, according to the company.
The solution consists of UgCS software for mission-planning, UgCS SkyHub hardware (on-board computer) for data accumulation, Radar Systems Zond Aero GPR, and Hexadrone TUNDRA drone.

Gremlin drone recovered in mid-air for the first time

Source: https://newatlas.com/drones/gremlin-drone-recovery-mid-air/

Nov 08 – Although drones certainly *can* replace crewed aircraft, DARPA's Gremlins program instead aims to equip military planes *with* drones that can be deployed and then retrieved for reuse. Now, for the first time ever, one of the drones has been recovered in mid-air.
The basic idea behind the Gremlins program is that instead of risking the lives of human pilots and their expensive aircraft, those planes would stay safely out of reach of enemy forces, releasing swarms of autonomous fixed-wing drones to do the dangerous work. Those drones are being developed by aerospace company Dynetics.

An X-61 Gremlin Air Vehicle (GAV) engages the "recovery bullet" of a C-130 Hercules aircraft (DARPA)

Once each drone's mission was complete, it would then fly up to a safe altitude, where it would be recovered by another human- piloted aircraft. Within 24 hours, that drone could be refurbished by a ground crew and then deployed on another mission – this process could be repeated up to 20 times per drone.

In tests conducted last December, a C-130 Hercules transport plane failed to retrieve three of the drones, which subsequently had to parachute to the ground. According to DARPA, the aerodynamics in flight were more complicated than expected, causing the tests to fail at the moment of engagement. Last month, however, a C-130 *did* successfully recovery an X-61 Gremlin drone in mid-air. The test flight was conducted at the Dugway Proving Ground in Utah, and actually involved two of the drones – although one was recovered, the other ended up being destroyed. Crews refurbished the recovered drone, then used it in another test flight within 24 working hours. "Airborne recovery is complex," says Gremlins project manager Lt. Col. Paul Calhoun. "We will take some time to enjoy the success of this deployment, then get back to work further analyzing the data and determining next steps for the Gremlins technology."

Could the Next 9/11 Be Caused By Drones?

By Tom O'Connor and Naveed Jamali

Source: https://www.newsweek.com/could-next-9-11-caused-drones-1647249

Sept 09 – Twenty years after the worst attack to ever occur on U.S. soil, it's not just large, populated passenger planes that keep officials and experts up at night, but also the threat of smaller, readily available unmanned aerial systems capable of carrying deadly payloads through the skies of an unsuspecting nation.

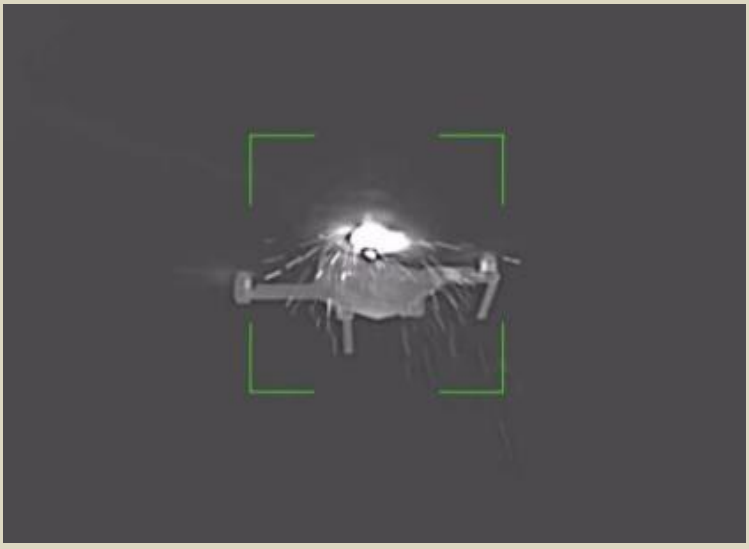
Drones are not tomorrow's weapons of mass destruction. They're here today, and the technology required to fashion such a device is only getting cheaper, smarter and more accessible.
One U.S. military official who requested anonymity paints a potential nightmare scenario involving small drones, referred to as unmanned aerial systems, unmanned aircraft systems, or simply, UAS.
"I kind of wonder what could you do if you had a couple of small UAS and you flew into a crowded stadium," the U.S. military official told *Newsweek*. "That could cause a lot of damage and it's a scenario that could potentially be in play."
While "no specific knowledge" of an active threat was discussed, the U.S. military official said that "there is concern given the proliferation of small, portable drones, that explosive drones could cause a mass casualty event."
It wouldn't be the first time the nation had been caught off guard by a possible danger looming right in front of authorities.
"It's just like I had no specific knowledge before 9/11 that people could hijack planes and crash into buildings, but Tom Clancy wrote a book about it," the U.S. military official said.
When the political thriller "Debt of Honor" was released in 1994 depicting a hijacked airliner targeting the U.S. Capitol, the concept of an aerial suicide raid had largely been confined in the national consciousness to the experience of Japanese kamikaze pilots in World War II. It wasn't until nearly 3,000 were killed on September 11, 2001 that what had been an eventuality became a reality.
But when it comes to UAS, the age of tactical drone warfare is already upon us. Shortly after 9/11, the United States became the first country to truly weaponize drones, fitting them with precision missiles that became a staple of the "War on Terror."
In the years since, drones have evolved from a high-end military technology to a commercial hobby flown by enthusiasts across the globe and sold by a multitude of companies on the civilian market. With the explosion of this seemingly innocent innovation has come a rise in nefarious usage that the U.S. military official with whom *Newsweek* spoke described as "an emergent threat" already demonstrated in several high-profile events.

A picture taken on March 14, 2017 in the northern Iraqi city of Mosul shows a drone carrying two 40-mm grenades flying in a test flight by Iraqi forces that aim to use it against ISIS fighters, which employed similar tactics against Iraqi, Syrian, U.S. and Kurdish forces during the multinational effort to defeat the jihadis. ARIS MESSINIS/AFP/Getty Images

One such event came just last weekend when three explosive-laden UAS, believed to be simple quadcopter models, targeted the residence of Iraqi Prime Minister Mustafa al-Kadhimi in an assassination attempt. Kadhimi lived, but photos released of his home revealed the destructive capabilities of such devices.
Kadhimi was not the first world leader to be preyed upon by bomb-rigged UAS. In August 2018, two drones carrying explosives detonated in an apparent failed attempt to take out Venezuelan President Nicolás Maduro during a military parade in Caracas. He also escaped with his life.
Prior to these incidents, militants and militias had already managed to utilize such technology, giving non-state actors a sort of rudimentary yet deadly air force to take on better-equipped foes. In Iraq and Syria, U.S. troops have been targeted from above by both the Islamic State militant group (ISIS) and Iran-aligned paramilitary forces.
Even more destructive platforms have seen action on the battlefield in the form of what's known as loitering munitions, or suicide drones. Last year, Azerbaijani forces demonstrated a deadly edge over Armenian rivals during a brief but bloody war over the disputed Nagorno-Karabakh territory through their use.

"They're relatively small, inexpensive drones, but they kind of cross that boundary between a drone and guided missile," the U.S. military official said.
This point was echoed by a security official from Israel, a country that produced some of the loitering munitions employed by Azerbaijani forces with substantial effect and now prove a potential concern for Iran as tensions simmer between the neighbors.
"This tool today is so easy, and small drones, you just really order them in and you've got yourself like a guided precision missile," the Israeli security official told *Newsweek*.
The Israeli security official noted that even with their current destructive potential, the munitions attached to such UAS today are in their relative infancy, not yet on a scale that any one of them alone could replicate a 9/11-style attack.
But their potential is already rapidly growing.
"They are becoming much more accurate in their capabilities of navigation," the Israeli security official said. "I think where we will be seeing things is that the amount of explosives will get bigger now."
Smaller commercial UAS have another unique advantage over traditional aircraft and missile platforms: They have no launch signature, making them far more difficult to detect. Used in greater numbers, known as a swarm, they're also harder to intercept.
"If you need to intercept a dozen, an F-16 payload, if it's only doing air-to-air would be about six different air-to-air missiles, or similar to an F-35," the Israeli security official said. "So that already means that you need a few airplanes, and you need the time if you're looking at interception."
Israel was among the first nations to refine wartime drone technology, and it continues to field various platforms for covert missions. But its rivals have also demonstrated an early prowess for such technology, as proven by the Lebanese Hezbollah, the Palestinian Hamas, and their supporter, Iran.
Iran has developed an extensive arsenal of drones, including suicide drones capable of flying beyond 2,000 kilometers, exceeding 1,240 miles. Israel and the U.S. have both accused Iran of directly supplying UAS technology to partnered militias across the region, an allegation denied by the Islamic Republic.
"I think Tehran has its own independent defense program based on its defense needs and can define its efforts to counter the threats by strengthening its defense capabilities," an Iranian official told *Newsweek*.
China has also excelled in UAS technology, and Russia has developed high-end systems of its own as well.
The Israeli security official noted another trend that could prove deeply problematic to the safety of the region and beyond, a trend linked to Israel's ally, the U.S., and the withdrawal from a 20-year war in Afghanistan, where ISIS has sought to stage a comeback in a country the U.S. first entered in response to 9/11.
"We see another rise of terror, and I'll say, being both humble and appreciative to the U.S., but after Afghanistan, we do see a rise in what potentially could come again with the terror activities and the kind of backing that some of the terror organizations feel stronger and maybe even more courageous," the Israeli security official said. "This tool of drones can definitely be something that we might be seeing more."
One man who has written and spoken extensively on the potential impact of drones in the wrong hands is Zachary Kallenborn.
Kallenborn is a policy fellow at George Mason University's Schar School of Policy and Government and a research affiliate with the University of Maryland's Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism. He has also served as a national security consultant and contributed to the U.S. Army as part of its Mad Scientist Laboratory.
"Drones are definitely capable of causing mass casualties," Kallenborn told *Newsweek*.
Echoing the example put forth by the U.S. military official with whom *Newsweek* spoke, he imagines a crowded event as a potential target.
"Growing drone technology also increasingly allows drones to be flown autonomously or in collaborative swarms," Kallenborn said. "That increases the damage potential significantly. Imagine a terrorist air raid: a group of drones dropping bombs on a concert or stadium crowd."
Even more damaging, attackers could vastly multiply casualties by employing weapons of mass destruction, Kallenborn warned.
"Drones would be highly effective delivery systems for chemical, biological, radiological, and nuclear weapons," he said. "Drones could, say, spray the agent right over a crowded area."
Kallenborn said he was "also quite concerned about drone attacks on airplanes, because aircraft engines and wings are not designed to survive drone strikes."
But he notes that "who the attacker is matters a lot," adding that "a big limiter" for the worst-case scenarios "is the ability of terrorists to acquire the chemical, biological, radiological, or nuclear agent, which they have historically struggled with."
He pointed out the difficulty of a militant group acquiring both the material and manpower to fly a larger swarm-sized fleet while avoiding detection.

"But that limitation is not an issue for state militaries," Kallenborn said. "Militaries have the resources and technology to make truly massive swarms that could rival the harm of traditional weapons of mass destruction, including small nuclear weapons."
"Not only is such a weapon massively powerful, it would be quite difficult to control," he added. "If you have 1,000 drones working together without human control, that's 1,000 opportunities for failure. And even more, because in a true drone swarm, the drones talk. As we've seen with COVID vaccine paranoia, misinformation can spread easily even among beings far smarter than an algorithm-guided drone."
As humans and machines are wont to err, so are defenses, and drones add a new level of difficulty in their ability to conduct random, difficult-to-detect operations. The U.S. military official with whom *Newsweek* spoke expressed a level of skepticism regarding existing defenses being acquired by the Department of Defense.
"The DOD is pouring a lot of money and effort into counter-UAS technology, but I think the DOD's PR exceeds the actual capability of these devices," the U.S. military official said.
One of the agencies keeping an eye out for UAS and drone activity on the domestic side is the Federal Aviation Authority. An FAA spokesperson told *Newsweek* that "the FAA is tasked with ensuring the safety of the National Airspace System (NAS) as well as people and property on the ground."
"When criminal activity is suspected, we work with our federal, state, and local law enforcement partners by providing them assistance with their investigations and prosecutions," the spokesperson said.
One way in which the FAA is seeking to improve the ability for authorities to determine potential problems posed by UAS is by enforcing remote identification, through which drones would be required to provide key information such as identity, altitude and current location as well as the location of its operator and take-off point.
"Remote identification requirements for all UAS operators, when combined with our current registration requirement, will enable more effective detection and identification," the FAA spokesperson said. "This will also help law enforcement to connect an unauthorized drone with its operator. Remote identification will help law enforcement determine if a drone poses an actual threat that needs to be mitigated, or if it's an errant drone that got away from someone but means no harm."



U.S. Marines in an undisclosed location within the U.S. Central Command area of operations train on the Compact Laser Weapon System (CLaWS), taking down an unmanned aerial vehicle mid-flight in this video published January 1. U.S. forces have faced small drone attacks from both ISIS and Iran-aligned militias. U.S. Marine Corps Forces Central Command

The rise of the drone threat has given birth to a booming new industry of counter-drone technologies. Among the leading companies in this field is DroneShield, an Australian firm that has supplied cutting-edge tools to the likes of the NATO military alliance and the United Nations.
DroneShield CEO Oleg Vernik shared Kallenborn's concerns about WMD-strapped UAS in large numbers.
"Small UAS can be seen as a highly effective and cheap platform for surveillance and payload delivery," Vernik told *Newsweek*. "For payload delivery, a small UAS can easily carry up to a few pounds of weight — this is a lot of explosive or biological or chemical weapons."
"What's more," he added, "at $1,000-$2,000 per UAS, and swarming technologies available today (think of giant figures in the sky or fireworks, all generated by choreographed drones), this can be easily in 100s of drones, each carrying a dangerous substance."
These figures may seem high, but Vernik argued that the general lack of oversight would make it hard to track acquisition. And even if suggested controls were put in place, he said, the threat would only partially be addressed.
"UAS can be purchased today in a completely unrestricted way, being considered toys, essentially. Registration would solve some of the issue, but consider how many unregistered firearms get used for terrorism," Vernik said. "The pilot of the drone would also be invisible/difficult to catch in an attack, making it more appealing to use"
In addition to the kinetic threat, he warned of potential cyber attacks employing UAS.
"Call it a conspiracy, but we received reports that the Ever Given container ship (yes, the one that blocked Suez Canal and stopped much of sea traffic) was due to a cyber hacking

from a drone, when a request for ransom was denied," Vernik said. "We are now hearing of this commonly from ship customers, especially in areas close to the better-known rogue states."
Last week, DroneShield released the 6th edition of its C-UAS, or counter-UAS, factbook, which details the scope of potential threats posed by small drones.
The guide covers recent events in drone warfare, including the Nagorno-Karabakh conflict and the 2019 attacks on Saudi Aramco oil sites, claimed by Yemen's Ansar Allah, or Houthi, movement but blamed by Saudi Arabia and the U.S. on Iran. It also gives examples of the latest innovations by China and Russia, and identifies some of the most popular heavy-lifting UAS that could be used even more discretely than their larger cousins.
The report provides potential solutions as well, including a range of detection capabilities such as radio frequency, radar, acoustic, optics and multi-sensor systems. It also lists neutralizing assets including radio frequency jammers, GPS jammers, cyber tactics, directed energy attacks, counter-UAS drones and kinetic systems capable of blasting UAS out of the sky.
"Without dedicated C-UAS system (for detection and defeat of such UAS)," Vernik said, "there would be no warning and no time to react, until it is too late and the damage is done."
As to whether such tools and methods would be employed before the next attack, he has expressed a note of skepticism.
"We live in a reactive society," Vernik said. "Boulders across the pathways have only started to be placed after terrorists used vehicles to bulldoze through crowds, as an example."
He warned that governments and their law enforcement and security agencies must start setting up systems now to defend against UAS attacks.
"We need to be more proactive in setting up UAS detection and defeat systems across areas where large gatherings of people are likely, the high profile places, sort of areas which would be terror sweet spots," Vernik said. "Law enforcement and homeland security personnel need to be trained for this threat, much like more conventional attacks."

***Tom O'Connor** is an award-winning senior writer of foreign policy at Newsweek, where he specializes in the Middle East, North Korea and other areas of international affairs and conflict. He has previously written for International Business Times, the New York Post, the Daily Star (Lebanon) and Staten Island Advance.*
***Naveed Jamali** is a Newsweek editor at large and a former FBI double agent and the author of "How to Catch a Russian Spy"*

First Drone Attack on US Energy Infrastructure Unveiled

Source: https://i-hls.com/archives/111495

Nov 08 – Critical infrastructure is often protected by fences and other barriers, but are these sufficient against drones?
US officials believe that a **DJI Mavic 2**, a small quadcopter-type drone, with a thick copper wire attached underneath it via nylon cords was likely at the center of an attempted attack on a power substation in Pennsylvania last year.
If the wire had come into contact with high-voltage equipment it could have caused a short circuit, equipment failures and possibly fires.
This has been revealed in an internal report from the FBI, Department of Homeland Security and National Counterterrorism Center. According to the report, cited by newscientist.com, the incident is the first known use of a drone to target energy infrastructure in the US. The drone crashed without causing damage. The device is similar in concept to "**blackout bombs**" used by the US Air Force, which have no explosive but scatter masses of conductive filaments over electrical equipment. These were used to shut down **70 percent of Serbia's electricity generation capacity in 1999 during the Kosovo war**.
The report assesses that such incidents are likely to become more commonplace as time goes on.

Unveiling the Scorpius Electronic Warfare System

The world's first EW system to detect and disrupt multiple threats simultaneously

Source: https://www.iai.co.il/unveiling-scorpius-electronic-warfare-system

Nov 11 – Israel Aerospace Industries (IAI) is excited to unveil the **Scorpius** family of Electronic Warfare (EW) systems. Scorpius is the first electronic warfare (EW) system in the world capable of simultaneously targeting multiple threats, across frequencies and in different directions.

Scorpius is based on the Active Electronically Scanned Array (AESA) technology, which provides a breakthrough in EW performance – enabling a new generation of electronic warfare capabilities.

With AESA's multi-beam capability, Scorpius can simultaneously scan the entire surrounding region for targets, and deploy narrowly focused beams to interfere with multiple threats across the electromagnetic spectrum. The system is able to target a range of threats, including: UAVs, ships, missiles, communication links, low probability of interception (LPOI) radars, and more. Scorpius effectively disrupts the operation of their electromagnetic systems, including radar and electronic sensors, navigation, and data communications.

Scorpius' technological breakthrough is characterized by unprecedented receiver sensitivity and transmission power (ERP), far exceeding those of legacy EW systems. This allows Scorpius to detect multiple threats, of different kinds, simultaneously, from dramatically increased distances, and to address each threat with a customized response.

Scorpius is available across multiple domains:

- **Ground**: Scorpius-G (ground) is a ground-based EW system designed to detect and disrupt ground- and airborne threats. Scorpius-G is a mobile system, and can be quickly deployed by vehicle. Scorpius G represents a new category of air defense systems: "Soft-kill" air defense, which creates an electronic dome of protection above a wide geographic sector to neutralize a broad range of modern threats.
- **Naval**: Scorpius-N (naval) is an EW system dedicated to defending ships against advanced threats in the marine arena, including: Over-the-Horizon Anti-Ship Cruise Missiles, Unmanned Combat Aerial Vehicles (UCAV) and airborne imaging radars. Scorpius' extremely high range provides early detection and targeting of threats, which is essential for effective protection in the naval domain.

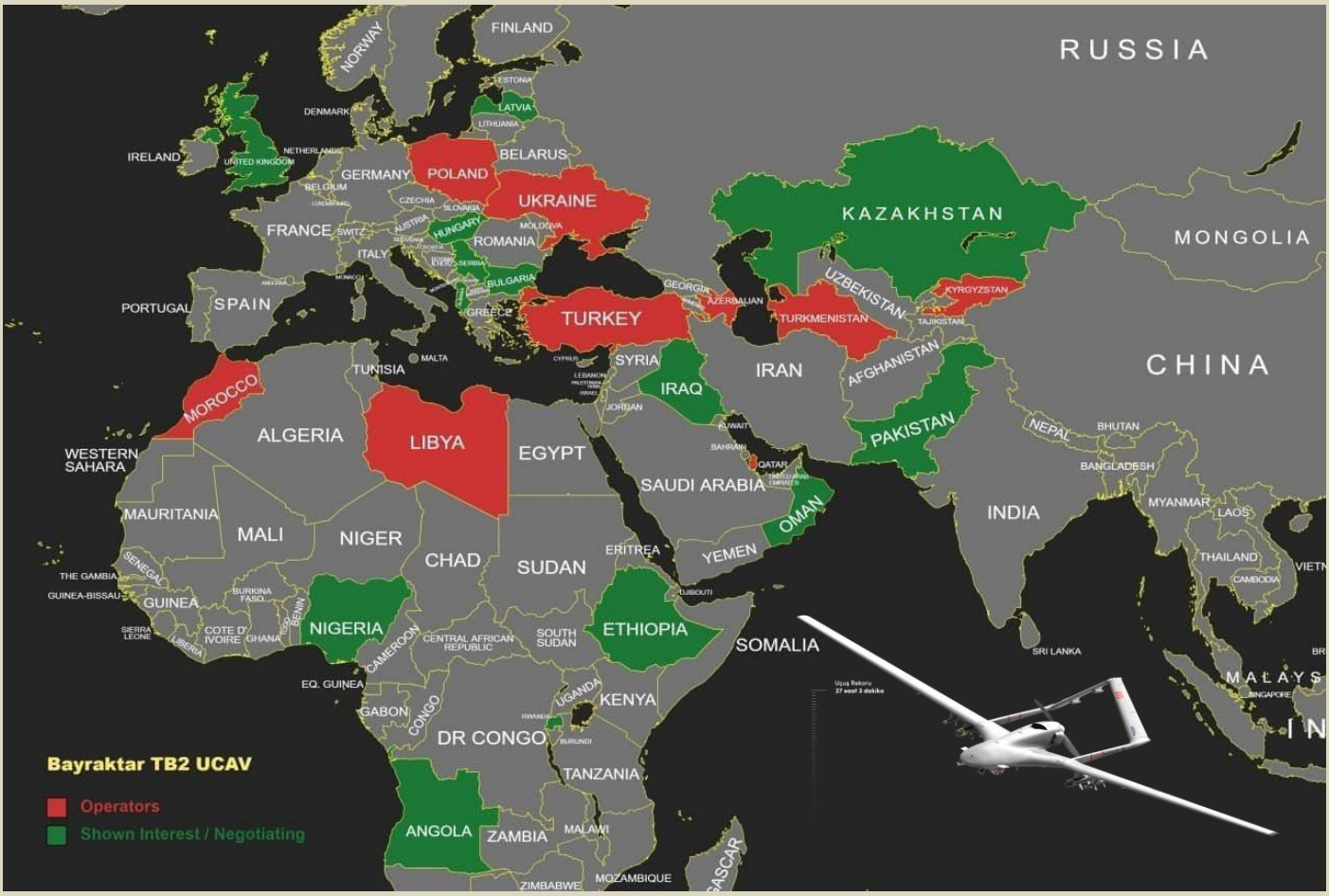
- **Air**: Scorpius SP, a self-protection pod for combat aircraft, and the Scorpius SJ, a standoff jammer that disrupts enemy aerial and ground-based electromagnetic operations across a vast sector.

- **Training**: Scorpius-T (training), unveiled last month, provides EW training for pilots. Scorpius-T can emulate a variety of modern air-defense systems, simultaneously, from a single platform. Its advanced emulation capabilities support training for fifth-generation aircraft. Scorpius T made its debut during the international air force exercise **Blue Flag 2021**.[3]

Adi Dulberg, General Manager, Intelligence Division, IAI**:** "The modern battlefield depends on the electromagnetic domain for sensing, communications, and navigation. Protecting the use of the electromagnetic domain for our forces, while denying its use by the enemy, have become mission-critical for success in combat and for ensuring the superiority of our forces in the field. The new technology, developed by IAI's talented engineers, tips the scale of electronic warfare, providing world-first breakthrough capabilities for electronic defense and disrupting enemy systems".

[3] Participating aircraft included Israeli F-35Is, F-15Ds and F-16Cs; French Rafales; U.K. Typhoons; Italian F-35s and G550 early warning aircraft; German Typhoons; Greek F-16s; and Indian Mirage 2000s.

Updated map of Turkish Bayraktar drone acquisition (red) and interest (green)



EDITOR'S COMMENT: What a coincidence that **almost** all customers are involved in wars or conflicts!


International
CBRNE
INSTITUTE
C2BRNE
DIARY
CBRNE-Terrorism
Newsletter
W
M
O
D
HOTZONE
SOLUTIONS
GROUP
EMERGENCY
RESPONSE

DMORT Teams and Their Role in MFIs

By Frank P. Saul

Source: https://www.domesticpreparedness.com/healthcare/dmort-teams-and-their-role-in-mfis/

Disaster strikes – and there are more fatalities than local resources can manage. An operational definition of a Mass Fatality Incident (MFI) is "one more than local authorities can handle." The specific death tolls in MFIs that the nation's Disaster Mortuary Operational Response Teams (DMORTs) have responded to since 1993 range from 11 fatalities to almost 3,000.

Fortunately, DMORTs are now available to assist local authorities as part of the National Disaster Medical System (NDMS) of the U.S. Department of Health and Human Services (DHHS). When deployed, a DMORT works for the local coroner/medical examiner. Public concerns and expectations following mass-fatality incidents – whether due to accidents, natural disasters, or terrorist activity – have resulted in the increasing application of forensically based multidisciplinary approaches to managing victim identification and other aspects of the incident, including evidence recovery.

That change is reflected in the composition and organization of the ten U.S. regional DMORT teams, which provide varying levels of assistance to local coroners/medical examiners – who still possess legal responsibility for control of the victims' remains. Typical DMORT teams are composed of forensic anthropologists, odontologists and pathologists, medicolegal investigators, computer specialists, and other support personnel, in addition to the morticians who first voiced concern about the proper care of victims, and who serve as the organizational backbone of the DMORT concept.

DMORT team members are intermittent federal employees who leave their "day jobs" when activated during MFIs. The types and numbers of personnel deployed to a specific MFI vary with the availability of local resources and the number of victims. The basic approach to handling an MFI is likely to be similar, however, starting with:

- The recognition, recovery, and documentation of victim remains and associated evidence at the scene of the incident. These scenes have varied from rural flooded cemeteries to airplane crashes; from fields, forests, and tropical Pacific settings to both the Atlantic and Pacific Oceans; from an Amtrak train crash in a small town to large regional areas devastated by natural disasters including tornadoes and

hurricanes (Katrina, for example); and, of course, to terrorist incidents, large and small, involving such sites as the Murrah Federal Building in Oklahoma City, and New York City's World Trade Center – the latter immediately becoming the largest crime scene in U.S. history. Climatic circumstances also have ranged widely, from a wind-chill temperature of 48 degrees below zero Fahrenheit with snow and ice in Monroe, Michigan, to over 100 degrees Fahrenheit combined with "super typhoons" on Guam.

- The selection of a site for, and establishment of, a Family Assistance Center (FAC) to aid in the acquisition of victim antemortem information, while also providing progress reports for victims' families. Hotels where out of town kin can be housed while receiving and providing information have been very useful for this purpose.
- The setting up and staffing of an Information Resource Center (IRC) to receive, process, and manage the antemortem and postmortem victim data. The latter usually is obtained by forensic specialists from the remains themselves at the morgue. DMORT computer programs are used for data processing. Forensic specialists will attempt to positively identify the victims by comparing the morgue data with the computer data.
- The selection of a site for, and establishment of, a temporary Incident Morgue (IM) for the processing and identification of recovered remains. Local authorities have sometimes made use of school facilities, but this should be avoided, because such locations are likely to become "tainted" in the eyes of local residents. Medical-examiner offices, military facilities, airport hangars, and warehouses also have been used, and rented tent-like structures with appropriate utility attachments have shown great potential for future use.

DPMUs, the Disaster Scene, and NTSB Involvement

The work at each of the above locations is facilitated by the use of what are called Disaster Portable Morgue Units (DPMUs). The typical DPMU is stocked with a broad spectrum of supplies and equipment including gurneys, personal protective equipment, remains examination tools, and computers as well as digital full-body and dental x-ray equipment. All DPMU equipment owned by the federal government is palletized and ready for immediate deployment, by air or overland transport, to incident locations. There are presently one DPMU on each coast, and one in Texas. Specially trained personnel travel with the DPMU to set up, maintain, and later return the DPMU to its point of origin.

Team members often aid in the recognition and recovery of remains and associated evidence while also documenting their location. However, as mentioned above, the disaster scene itself remains under the control of the pertinent local, state, or federal jurisdiction. Many disaster scenes also are considered crime scenes, and thorough documentation – followed by continuing documentation when the remains are processed at the morgue – avoids the types of mistakes that may hamper criminal and/or civil proceedings. Documentation has become even more important in recent years because of concerns about possible terrorist activity. The FBI's Evidence Response Teams (ERTs) also have become increasingly involved.

While emphasizing the forensic aspects of documentation it should not be forgotten that the National Transportation Safety Board (NTSB) and other agencies are charged with determining what specifically went wrong in accidents involving aircraft and/or other modes of transportation so that, in addition to helping to assign legal responsibility, those agencies also are involved in the effort to prevent future accidents.

An Inside Look at the Family Assistance Center

The Family Assistance Center (FAC) is an integral part of any mass-fatality response. The FAC serves several purposes. It serves, for example, as: (a) A central location where family members of the deceased can provide antemortem information on the victim, such as a detailed physical description, dental records, medical information, and DNA reference samples; and (b) A convenient meeting place where the families of victims can receive accurate, timely information regarding victim identification – and have their own questions answered.

In the case of aircraft accidents, the Aviation Disaster Family Assistance Act (the legislative "bible" for such accidents) places responsibility for running the Family Assistance Centers on the National Transportation Safety Board itself – which has available a small cadre of well trained DMORT members to help provide FAC support.
Family members can assist in the identification of their loved ones at the FAC by providing information about the victims. Antemortem information about clothing, jewelry, physical characteristics, medical and dental procedures, and health history is collected for comparison with similar postmortem information derived from the victims' remains. The FAC is usually where the process of locating and obtaining victim antemortem dental and medical radiographs and related information is initiated. It is also where family members usually are interviewed – by funeral directors who are accustomed to working with grieving families.
Many of the interviewers also have backgrounds in mental health and/or social work. DMORT has recognized the important nature of this work by forming a Family Assistance Center Team (FACT) that provides a cadre of highly trained and experienced interviewers.

Information Resource Centers & the Incident Morgue

The Information Resource Center (IRC) uses a software Victim identification Program (VIP) that has evolved in relation to each incident. The IRC usually will be set up in an area with close access to the morgue work area, and a separate data-entry area may be set up at the FAC for the input of antemortem data; the data gathered is then electronically transferred to the IRC. After all antemortem data has been collected and entered, a careful search of the accumulated data is carried out, using the postmortem data points as the primary basis for the searches. Under no circumstances, it should be emphasized, does the VIP program make an identification per se; what it does do, and very competently, is narrow the number of possible matches that must be checked scientifically.
The other important piece of software that will be running in the IRC is the WinID program, which is used to match dentition in the Dental Section.
The Incident Morgue (IM) is used for all postmortem examinations. Morgue operations are modular in organization and can be modified to address the needs that become obvious

during and after a specific disaster. The morgue layout is standardized, though, with an organized flow of the remains from initial documentation to postmortem examination to identification to release.
After being taken into the morgue, victims' remains pass through a triage process to remove: (a) unidentifiable material; and (b) material considered to be unsuitable for DNA testing. The remains of each victim are assigned both a number and an escort person – to ensure continuity of both the evidence chain and the documentation of victim remains and personal effects. The documentation includes both photographic and radiographic recording of the remains. All remains also are photographed before they move through the morgue process.

Pathology and Other Medical Specialties

Immediate incident-scene radiographic documentation is needed to locate airplane parts as well as other foreign objects that may be a hazard to personnel and/or be needed by the NTSB or FBI for their analyses. Radiographs also are used to record loose teeth, medical/surgical devices, and unusual or otherwise distinctive characteristics of the remains that may aid in identification. Customary clinical views of the remains are taken for comparison with any antemortem radiographs.
As in normal practice, pathologists attempt to determine the cause and manner of death. The latter may seem simple in transportation and natural disaster incidents, but homicides *not* related to the crash or flood have been found by careful examination of the remains. Also, improvements in safety have come about as a consequence of determining the actual cause of death. For instance, the fact that death in some crashes was due to smoke inhalation rather than to the blunt force associated with impact has resulted in the use of fire-resistant materials for seating and interiors. Moreover, the notation of injury patterns can lead to design changes that can reduce future injuries and save lives.
In addition, pathologists describe remains and, if and when the condition of the remains allows, pathologists: (a) note the victim's sex (based on examination of the body's external and/or internal soft tissues); (b) make a rough estimate of the victim's age (as suggested by internal organs); and (c) record the presence of moles, scars (and their significance), tattoos, medical devices, etc. In a transportation accident, the pathologist is also required to take samples from specified crew members (of the aircraft or locomotive, for example) for analysis.
Other medical specialists contribute significantly to development of the overall postmortem process. A basic contribution of the forensic *anthropologist*, for example, in the standard forensic setting (coroner/medical examiner office) is to create a biographic profile based on a skeletal assessment of sex, age, ancestry, stature, etc. for the unidentified individual so that appropriate antemortem dental and medical radiographs can be obtained from a variably sized pool of missing persons for comparison. The biographic profiles also may include fleshed characteristics, if and when available.
In an MFI, the immediate need is to create biographic profiles for each set of remains, whether an intact body or a body fragment, so that when (and if) the antemortem radiographs arrive, potentially matching postmortem radiographs can quickly be made available for comparison.
The specific anatomical structure present (useful in re-associating separate units and called for in DNA protocols) and other descriptive information are also documented.
Antemortem and postmortem clinical-view radiograph comparisons are usually carried out by anthropologists – who also may use antemortem photographs of distinctive body features (i.e., ear form) in the same fashion, after first matching biographic profiles.
Forensic *odontologists* (dentists) locate and radiographically record the teeth, restorations, and other dental characteristics present in the remains. This information is compared to the antemortem dental radiographs (written records may not be accurate) obtained through the FAC. (Historically, dental identifications have accounted for a majority of identifications of disaster victims.)

Fingerprinting, DNA, and Returning the Remains

When available, fingerprints are usually handled by specialists from the FBI Disaster Squad. DNA evidence also has become an important tool for both positive identification and the re-association of remains. Just as in other identification methods, DNA requires the use of postmortem samples and antemortem or family reference samples. DMORT has adopted the protocols of the Armed Forces DNA identification Laboratory (AFDIL) for collection of postmortem DNA samples and victim and family reference samples. DMORT collects family and victim reference samples through the FACT.
After passing through the above stations – and others if and when required by special circumstances – the remains are stored in refrigerated trucks awaiting additional identification information and eventual release to the families. After a positive identification has been recommended by the forensic team, the final determination is made by the local coroner/medical examiner. The remains may then be embalmed by DMORT morticians prior to returning them to the next of kin, or they may be embalmed by local morticians selected by the next of kin. The process of releasing the correct remains to the proper funeral home is an exceptionally critical process demanding thorough documentation.

As the general public (specifically including victims' families) has become more sophisticated and knowledgeable about the forensic sciences – in part, undoubtedly, because of the popularity of several television programs focused on the forensic sciences – expectations have been heightened concerning the positive identification of victims in Mass Fatality Incidents. The role of DMORT, and its forensic scientists and support personnel, has probably for that reason alone become more important than ever before in responding to the needs of the victims' families.

Dr. Frank P. Saul *is Associate Dean and Professor Emeritus, Anatomy, of the Medical College of Ohio, and also serves as commander, Region V Disaster Mortuary Operational Team (DMORT), of the National Disaster Medical System. Dr. Saul is also a forensic anthropology consultant to coroner/medical examiner offices in Toledo, Ohio, Detroit, Michigan, and other cities, as well as to the Cleveland (Ohio) FBI Evidence Response Team.*

HOTZONE SOLUTIONS GROUP

"The world's most practice oriented provider of Hazardous Substances Management Solutions"

https://hotzonesolutions.org/

+31(0)70 262 97 04 | Prinsessegracht 6, 2514 AN, The Hague, The Netherlands