

08\23

I
C
I

IC² CBRNE



August 2023

*Dedicated to Global
First Responders*

DIARY



**AQ experimented
with CWAs**

PART A



**CBRN challenges
in floating cities**



**Enjoy
Summer
2023**



An International CBRNE Institute publication

C²BRNE DIARY-2023[©]

August 2023

Website: www.cbrne-terrorism-newsletter.com

Editor-in-Chief

BrigGEN (ret.) Ioannis Galatas MD, MSc, MC (Army)

Ph.D. cand

Consultant in Allergy & Clinical Immunology

Medical/Hospital CBRNE Planner & Instructor

Senior Asymmetric Threats Analyst

Manager, CBRN Knowledge Center @ International CBRNE Institute (BE)

Athens, Greece

➔ Contact e-mail: igalatas@yahoo.com

Editorial Team

- **Bellanca Giada, MD, MSc (Italy)**
- **Bossis Mary, Ph.D. Intern/EU Studies (Greece)**
- **Hopmeier Michael, BSc/MSc MechEngin (USA)**
- **Kiourktsoglou George, BSc, Dipl, MSc, MBA, PhD (UK)**
- **Photiou Steve, MD, MSc EmDisaster (Italy)**
- **Tarlow Peter, Ph.D. Sociol (USA)**

International CBRNE Institute

Rue des Vignes, 2
B5060 SAMBREVILLE (Tamines)
BELGIUM

Email: info@ici-belgium.be

Web: www.ici-belgium.be

ICI
International
CBRNE
INSTITUTE



DISCLAIMER: The C²BRNE DIARY[®] (*former CBRNE-Terrorism Newsletter*), is a **free** online monthly publication for fellow civilian/military CBRNE First Responders worldwide. The Diary is a collection of papers and articles related to the stated thematology. Relevant sources/authors are included and all info provided herein is from **open** Internet sources. Opinions and comments from the Editor, the Editorial Team, or the authors publishing in the Diary **do not** necessarily represent those of the International CBRNE Institute (BE).

●▶ Occasional advertisements are free of charge.

ICI
International
CBRNE
INSTITUTE



Topics that attracted attention!

EDITOR'S CORNER





Editorial

Brig Gen (ret.) Ioannis Galatas, MD, MSc, MC (Army)

Editor-in-Chief
ICI C²BRNE Diary



Dear Colleagues,

The situation remains the same: the proxy war continues; a second one is in the next corner – the pandemic ended but the virus does not agree – AI is fighting AI – global stupidity refuses peace and progress blaming the climate crisis for everything.

The World: As if we don't have enough of the conflict in Ukraine, the dangerous tension in the Middle East and the Taiwan Straits, the war against Nature, which accelerates climate catastrophe and brings the end of humanity closer, we don't have enough of the explosive state of a planet of unprecedented inequality, half of whose inhabitants do not have food, now the serious possibility of a war that threatens to embrace all of sub-Saharan Africa, the famous Sahel, and also involve forces outside the region has come to be added... After all, this war started with economic means with the savage sanctions imposed by the French and their minions on Africa, at the expense of Burkina Faso and Niger, with the latter cutting off, literally, Nigeria's electricity. Since we are talking about the poorest countries in the world, one can easily understand the results of such "agricultural" but completely common measures in the history of Western colonialism. The reason this is happening is a series of four nationalist military movements that challenge the region's neo-colonial ties to the old colonial power France. The most advanced of these is the movement in Burkina Faso, which means "Land of Intact People", whose president is inspired by Thomas Sankara, his murdered predecessor and considered the "Che Guevara" of Africa. Such a war - in which the Americans are pushing the French and the French are pushing the countries of the region led by Nigeria, a war for which the black mercenaries of the Foreign Legion are already preparing, but perhaps also ISIS, probably controlled by services of the "collective West", will blow up all the balances of Africa by pushing this continent into chaos, it risks causing a major humanitarian crisis, disrupting the export of energy and raw materials to Europe and causing a huge wave of refugees (towards EU).

Africa: France and the USA are losing one of the last French bastions and therefore friendly to the Americans in an Africa that is turning in favor of the Russians and the Chinese. It should be noted that Algeria is one of the main suppliers of natural gas in Europe. Niger has already stopped exporting gold and uranium to France. The Niger coup is about to ignite a new war in Africa and, as always Western fingers are involved – France, UK, US. The new government of Niger has signed an agreement with the Russian volunteer corps of Wagner, to offer its services in the defense of the country. Al-Qaeda is reported to have attacked Wagner forces that have arrived in Niger.

Quran burning: The EU's foreign policy chief Josef Borrell condemned recent Quran burnings in Denmark and Sweden. Burning the Islamic holy book "is offensive, disrespectful, and a clear provocation," Borrell said in a statement. What is wrong with Denmark and Sweden? Seven opposition parties in Denmark today objected to government efforts to make it illegal to burn copies of the Koran, arguing that such legislation would constitute an unacceptable restriction on freedom of expression. There will be a day that, after a terrorist attack, we will say "They asked for it?"



ICI C²BRNE DIARY – August 2023

Taliban: Best candidacy for the Global Stupidity Award 2023! Taliban religious police reportedly burned many musical instruments in Afghanistan's western province of Herat. Sheikh Aziz al-Rahman al-Muhajir, the provincial head of the Ministry of Promotion of Virtue and the Prevention of Vice, said music led to "misguidance of the youth and the destruction of society."

Illegal Immigration: New (?) modus operandi for human traffickers invading Greek sea territories. When they see the patrol vessel coming towards their boat, they through the engine into the sea and tear the boat apart to sink it. As a result, the civilized Greek Coast Guard will save them and transfer them to shore to apply for asylum! What if the next time they do that, the patrol vessel will turn around and go back to its port? What would be the impact on those using women and children to blackmail illegal entry to another country?

Proxy War: John Sopko, Inspector General of the United States Reconstruction Agency in Afghanistan, said the amount of money the US will spend by the end of 2023 will exceed the money spent on the entire Marshall Plan. He also pointed out how Ukraine is a country that is almost as corrupt as Afghanistan "We are spending more money in Ukraine now in one year than we spent in about 12 years in Afghanistan, and by the end of 2023, we will spend more money in Ukraine than we spent to prepare the entire Marshall Plan after World War II" ... No problem, as long as Ukrainians keep on killing Russians. According to a CNN poll, 55% say the US Congress should not authorize additional funding to support Ukraine vs. 45% who say Congress should authorize such funding. And 51% say that the US has already done enough to help Ukraine while 48% say it should do more. Next step if immorality: Denmark and The Netherlands will provide 61 F-16 to Ukraine after short training of the pilots! France might follow with Mirage-2000!

Pyroterrorism: So many wildfires in such a short period in so many different locations near or inside inhabitant areas and military installation without apparent cause, constitute the definition of a "pyroterrorism" attack against Greece!

The Editor-in-Chief



Wildfire attacking the city of Alexandroupolis, Northern Greece | August 2023



On Tuesday, July 25, 2023, at 14:52, a CL-215 aircraft, with a crew of two Airmen, of the 355th Tactical Transport Squadron of the 112th Fighter Wing, crashed during aerial firefighting in Platanistos, Evia.



Rest in Peace!

Surveillance Plans for the 2024 Paris Olympics Raise Concerns

Source: <https://i-hls.com/archives/120026>



July 24 – In an attempt to control the crowds arriving for the 2024 Paris Olympics next summer, the authorities plan to use real-time cameras and artificial intelligence to detect suspicious activity, but **civil rights groups say the technology is a threat to civilian rights.** PARIS 2024

According to BBC News, a recent law dictates that police will be able to use CCTV algorithms to pick up a bnormalities like crowd rushes, fights or unattended bags, and explicitly rules out using facial recognition technology, as was adopted by China, for example, in order to trace “suspicious” individuals.

Despite this disclaimer, opposers claim that this is a very thin line that is easily crossed, and fear that the French government’s real intention is to make the new security provisions permanent.

“We’ve seen this before at previous Olympic Games like in Japan, Brazil, and Greece. What were supposed to be special security arrangements for the special circumstances of the games, ended up being normalized,” says Noémie Levain, of the digital rights campaign group La Quadrature du Net (Squaring the Web).

According to French officials, the AI system monitors all the cameras and raises an alert when detecting something it’s been told to look out for. It is then up to the human police officers to examine the situation and make an action plan.

The AI algorithm was trained by a huge bank of images of lone bags on the street, but unattended luggage is easy to detect- a person with malicious intentions is way harder to spot in a crowd.

This is where the XXII group comes in. It is a French start-up that specializes in computer vision software and is currently waiting for further specifications from the French government before fine-tuning its bid for part of the Olympics video surveillance contract.

The XXII group and other developers are aware of the criticism regarding this new so-called “unaccepted level of state surveillance”, but they insistently claim they have safeguards set in place, saying they cannot by law provide facial recognition.

Nevertheless, according to the digital rights activist Noémie Levain, this is only a “narrative”.

“They say it makes all the difference that here there will be no facial recognition. We say it is essentially the same,” she says. “AI video monitoring is a surveillance tool which allows the state to analyze our bodies, our behavior, and decide whether it is normal or suspicious. Even without facial recognition, it enables mass control.

“We see it as just as scary as what is happening in China. It’s the same principle of losing the right to be anonymous, the right to act how we want to act in public, the right not to be watched.”

This information was provided by BBC News.

EDITOR’S COMMENT: These “civil rights” groups oppose CCTVs but agree to 600.000 spectators on both banks of the River Seine for the opening ceremony. I think the “f” word is appropriate for the occasion – if I may say.

The Mythical Tie Between Immigration and Crime

By Krysten Crawford

Source: <https://www.homelandsecuritynewswire.com/dr20230726-the-mythical-tie-between-immigration-and-crime>

July 26 – Opponents of immigration often argue that immigrants drive up crime rates. But newly released research from Stanford economist [Ran Abramitzky](#) and his co-authors finds that hasn’t been the **case in America for the last 140 years.**

[The study](#) reveals that first-generation immigrants have not been more likely to be imprisoned than people born in the United States since 1880.

Today, immigrants are 30 percent less likely to be incarcerated than are U.S.-born individuals who are white, the study finds. And when the analysis is expanded to include Black Americans — whose prison rates are higher than the general population — the likelihood of an immigrant being incarcerated is 60 percent lower than of people born in the United States.

While other research has also debunked claims that immigration leads to more crime, this study of incarceration rates provides the broadest historical look at the relationship between immigration and crime across the country and over time, says author Abramitzky. Abramitzky is the Stanford Federal Credit Union Professor of Economics and senior associate dean of social sciences in the School of Humanities and Sciences, as well as a senior fellow at the Stanford Institute for Economic Policy Research (SIEPR). The study is detailed in a working paper released by the National Bureau of Economic Research. Using U.S. Census Bureau data, it focuses on immigrants present in the Census regardless of their legal status and on men between the ages of 18 and 40.



“From Henry Cabot Lodge in the late 19th century to Donald Trump, anti-immigration politicians have repeatedly tried to link immigrants to crime, but our research confirms that this is a myth and not based on fact,” says Abramitzky, whose 2022 book, [Streets of Gold: America’s Untold Story of Immigrant Success](#), examines the many misconceptions around immigration.

In their analysis of Census data from 1850 to 2020, Abramitzky and his co-authors find that, compared to U.S.-born individuals, immigrants as a group had higher incarceration rates before 1870 and similar rates between 1880 and 1950. Since 1960, however, immigrants have been less likely to be incarcerated than have the U.S.-born.

According to the study, this is the case for almost every region in the world that is a major source of immigrants to the United States.

As of 2019, immigrants from China and eastern and southern Europe were committing the fewest number of crimes — as measured by incarceration rates — relative to U.S.-born individuals.

The exception is Mexican and Central American immigrants, but the higher incarceration rates for this group since 2005 is largely attributed to the fact that the Census data combines incarceration for criminal acts with detentions for immigration-related offenses, the researchers say in the paper. Incarceration rates among Mexican and Central American immigrants were similar to those of U.S.-born individuals between 1980 and 2005.

What’s more, comparing the imprisonment of Mexican and Central American immigrants to that of white males born in the United States based on education tells a different story, according to Abramitzky. Men without a high school degree are the group most likely to be incarcerated for criminal activity. “But Mexican and Central American immigrants with low levels of education, which comprise a large share of immigrants from this region, are significantly less likely to be incarcerated than U.S.-born men with similarly low levels of education,” he says.

Abramitzky’s co-authors include Leah Platt Boustan, an economics professor at Princeton and co-author of *Streets of Gold*; Elisa Jácome, an assistant professor of economics at Northwestern and a former SIEPR postdoctoral fellow; Santiago Pérez, an associate professor of economics at the University of California, Davis; and Juan David Torres, a Stanford PhD student in economics and former predoctoral fellow at SIEPR.

Immigrants vs. U.S.-Born: Different Economic Forces

In setting out to compare criminality over time, the researchers took on a big challenge: Finding credible evidence of a connection between immigration and crime — and over a long time period — is extremely difficult. Other studies have relied on arrests records, but those do not include immigration status or birthplace. They also include arrests for minor infractions, which can reflect police bias more than actual crimes.

Instead, Abramitzky and his collaborators chose to analyze incarceration rates, which they say are better indicators of serious crime because they often require a conviction. As their primary data source, they turned to decennial censuses and surveys from the U.S. Census Bureau, which include information on individuals in correctional facilities and their birthplace — thereby allowing the researchers to build what they say is the first nationally representative dataset of incarceration rates for immigrants and the U.S.-born going back 170 years.

The researchers say it’s not entirely clear why the data show that immigrants have been imprisoned at increasingly lower rates than U.S.-born males since 1960.

“Many of the explanations we had in mind turned out to NOT be right when we looked at the data,” Abramitzky says. For example, examining differences in age, marital status, or education levels among immigrants didn’t provide a clue. Nor did changes in immigration policy or the states in which immigrants settled.

It is also unlikely, he says, that deportations contributed to the relatively lower rates of immigrant incarcerations.

The researchers conclude the likely explanation is that first-generation immigrants are faring better overall (and not just with respect to incarceration rates) than are U.S.-born men — especially compared to those without a high school diploma.

Globalization and advances in technology have hit white males hard, especially those who were born in the United States and who didn’t finish high school. Compared to immigrants, they are much more likely to be unemployed, unmarried, and in poor health — and perhaps more prone to commit crimes as a result, Abramitzky says.

The manual jobs that immigrants typically take on have been stable by comparison. Other studies have shown that immigrants also are, among other characteristics, highly adaptable and resilient.

“Recent waves of immigrants are more likely to be employed, married with children, and in good health,” Abramitzky says. “Far from the rapists and drug dealers that anti-immigrant politicians claim them to be, immigrants today are doing relatively well and have largely been shielded from the social and economic forces that have negatively affected low-educated U.S.-born men.”

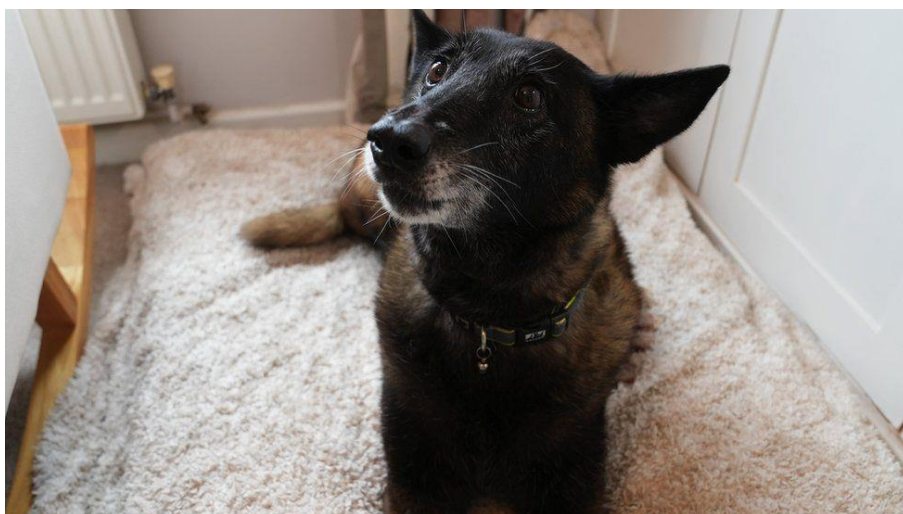


Krysten Crawford writes about the research and work of the Stanford Institute for Economic Policy Research (SIEPR) affiliates as well as the institute's programs and initiatives.

EDITOR'S COMMENT: The title of the article needs slight modification. Either omit the word "mythical" or add at the end "in the United States". Because the situation is not like this in the rest of the world affected by illegal immigration. In addition, the study states that immigrants from China and eastern and southern Europe were committing the fewest number of crimes – areas with higher levels of education and working dexterities compared with the masses from Africa and Asia that usually do not seek employment in hosting countries preferring the benefits generously offered and petty crime while many are incorporated in organized crime as well.

Army dogs should be better protected, says former handler

Source: <https://www.bbc.com/news/uk-wales-66292235>



Ara worked with special forces in Afghanistan and saved many lives, according to her owner

July 25 – Dogs who have served in the military should have equal status to human veterans and receive better aftercare, a former Army handler has said.

Canines can be the first to be sent into the most dangerous situations.

And dog charity Hero Paws said they should be treated equally to people once their time on the frontline is over.

The Army said it provided "the highest standards of welfare and care" for animals.

Charlie Cridland, from Bridgend, was a dog

handler in the Royal Army Veterinary Corps. When he retired he took his two dogs, Ara and Mo, with him.

Ara, a 12-year-old Belgian Malinois, worked with special forces in Afghanistan and was sent into dangerous situations before soldiers to hunt for improvised explosive devices (IEDs). She was trained to detect parts of explosives no bigger than a grain of sand.

Charlie Cridland and his dog, Mo, when they were both serving in the Army

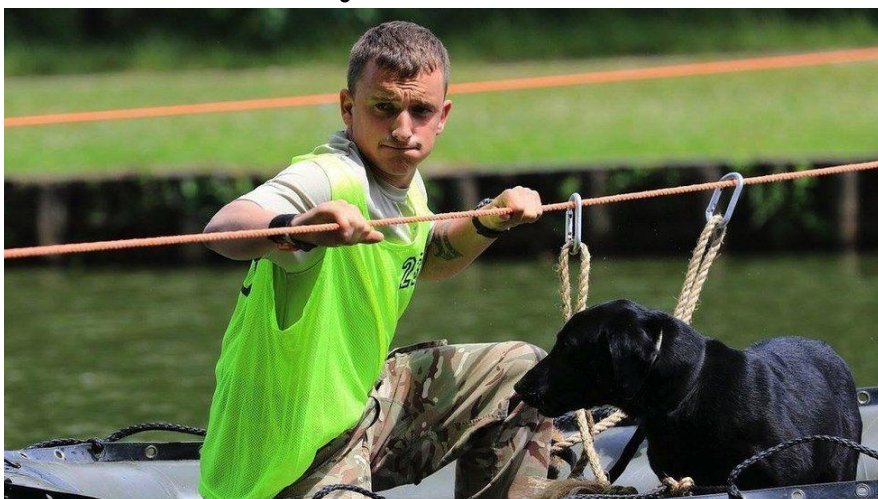
'They are saving lives'

Despite being well cared for in the military, Ara did not have the same status or protections as humans.

Mr Cridland said he believed that should change given how many lives Ara, and other dogs like her, had saved.

He said: "Her work in particular was up there with the most dangerous. IEDs were the biggest killer throughout Afghanistan.

"They are saving lives, and you could make the argument that there is a risk to human life by not protecting the asset that you have got. "So, Mo for example, who could be working a hundred metres away from me,



ICI C²BRNE DIARY – August 2023

if somebody was trying to harm her or put her life in jeopardy, under the rules of engagement, I would not have been allowed to return fire." The British military has nearly 1,000 working dogs.

Each one has a name, service number, health and training record and an assigned military veterinarian.

Lt Col Mike Robinson, commanding officer of the Defence Animal Training Regiment, said all military animals were considered "sentient beings and fall between people and equipment".

"We put, in defence, animals in harm's way I suppose, because of the nature of what we do.

"I know the public care, but our soldiers care, the people who use them care, they are an amazing asset to have in defence," he said.

"Sadly, some dogs do get injured but ultimately dogs also save huge numbers of lives and prevent injuries in their duty," he added.

When someone re-homes a military dog, the new owner becomes responsible for any ongoing veterinary bills.

The charity [Hero Paws](#), which works to re-home service dogs, wants them to be given equal status to people and better aftercare.

Samantha James, a trustee at the charity, was an Army dog handler for five years.

She did a tour of Afghanistan in 2012 with search dog Stikky, who she later re-homed.

"I'm lucky enough with Stikky, I've not had too many veterinary issues, but I know a lot of people do come to Hero Paws for support, financially, because the Army won't pay for it or the military won't pay for it and insurance won't cover it," Ms James said.

The British Army said it tries to treat any condition a dog has before it is re-homed and provides treatment for up to six months after retirement.

EDITOR'S COMMENT: The military's attitude is the same worldwide. When you stop serving all the benefits are postponed and all the services provided are forgotten. The number of legs is not important!

First Responders' Automatic CPR Device 'Doesn't Get Tired'

Source: <https://www.govtech.com/em/first-responders-automatic-cpr-device-doesnt-get-tired>



July 26 – Improved technology that automatically does CPR will take some of the burden off first responders and likely save lives.

The device, called LUCAS 3, is portable and consists of a compression unit that goes on the patient's chest and a plate placed under their back that then performs chest compressions.

The device gives [first responders](#) a chance to rest and help calm a chaotic scene while it does the work.

"The main thing about it is it's consistent and it doesn't get tired," Tom Barsi, education manager for Orchard Park, N.Y., Fire District EMS, told the *Buffalo News*. "If somebody is doing manual CPR and they're pushing on someone's chest with their hands, they can do it for a period of time. You need to perform 100 to 120 compressions a minute. You can do it for a little bit, but you get tired."



ICI C²BRNE DIARY – August 2023

Orchard Park Fire District EMS obtained the devices from the Erie County Health Department on a loan. The health department wants to see how they work in the field, as it plans to use the devices as part of an ambulance service.

The devices cost \$16,000 to \$20,000 each and reportedly are not as user-friendly as an automatic external defibrillator. However, they are better than the first-generation models that came out in the early 2000s and had challenges with power and batteries that didn't last very long. They are not supposed to replace manual CPR, but supplement it. It's also important that the [first person on the scene](#) begins manual CPR as soon as possible, before the first responders arrive. "It's very helpful when we have low manpower," said Chris Richardson, a member of the Lake View, N.Y., Fire District. "It is a really huge asset to have, and since we've been using it, it's been quite successful."



Russia accused of releasing fake German anti-Zelensky advert



EDITOR'S COMMENT: When a fake video talks the truth!

What Is LIDAR?

Source: <https://www.sciencealert.com/what-is-lidar>

LIDAR stands for **Light Detection and Ranging**. Much like sound-based echolocation technologies such as [sonar](#), this popular ranging method uses the time it takes for a focused, coherent wave of light to travel towards a surface and back again to calculate distances.

[First used in the 1960s](#) for military targeting, the technology has since been adapted to make use of advances in satellite-based radio-navigation systems and rapid computer processing to become a high-precision mapping tool.

How does LIDAR work?

As light of different energies reflects from different substances in specific ways, the intensity of an electromagnetic 'echo' can convey a lot of information about layers of material.





An Amazonian archeological site revealed by LIDAR. ([Prümers et al., Nature, 2022](#))

Different wavelengths of laser emission are today used to probe through foliage and water columns to construct highly detailed topographical [layouts of landscapes](#) and [seafloors](#). Emitted into the sky, LIDAR can [study the atmosphere](#) to profile clouds, measure wind speeds, and analyze the makeup of gases and particulates.

With technology dropping in price, we might see its application in even more fields. Many brands of mass-market autonomous vehicles, for example, [are exploring the use of LIDAR](#) as a means of allowing cars to 'see' the environment. The [latest generations](#) in smart personal technology are also putting LIDAR to good use as a way to scan surroundings in 3D.

LIDAR is undoubtedly a tool we'll be seeing a lot more of in the future.

What's the difference between RADAR and LIDAR?

Both RADAR (which is now more commonly known as radar) and LIDAR bounce waves of electromagnetic radiation off objects to measure how far away it is from the light source. Where they differ is primarily in the wavelengths they occupy.

Radar (Radio Detection and Ranging) was developed from research into the reflections of radio waves in the late 19th century. [By the Second World War](#), radio frequency-based ranging technology was being used in military applications for detecting incoming enemy attacks.

These low-frequency radio waves are ideal for traveling great distances through dense fog and cloud cover. Unfortunately, those long waves reduce the resolution of any objects being measured. At a [distance of just 100 meters](#) (328 feet), the smallest details detectable by radar have to be a few meters across.

Development of the [ruby laser](#) in the 1960s opened the way for higher frequency electromagnetic radiation sources to be used. Numerous pulses of laser light in the infrared, visible, or ultraviolet parts of the spectrum provide much tighter resolution at higher ranges, allowing LIDAR to reveal details a radar's wavelength would never see.

Four out of 10 Swedes want ban on Quran burning stunts

Source: <https://dohanews.co/four-out-of-10-swedes-want-ban-on-quran-burning-stunts/>

Aug 02 – Doha has adopted an unwavering stance in the face of Islamophobia globally, being one of the few to stand with utmost intolerance towards anti-religious hate crimes.

Almost 38% of Swedes want the burning of the Holy Quran to be banned in Sweden, according to a fresh research report.

Almost four out of 10 of Swedes support prohibiting the burning of the Swedish flag and the sacred texts of the three major world religions. However, around 50% of Swedes (every second Swede) are opposed to such a ban, research company [Novus](#) gathered. Through the report, Novus aimed to examine the number of Swedes who perceive burning the Quran as a means to sabotage NATO membership. This perception was influenced partly by Turkish President Recep Tayyip Erdogan's statement linking it to membership requirements and also by the very belief that it serves as a reason.

The report also gathered that there seems to be a perception that Russia actively influences such actions to undermine Sweden's application to NATO.





One in every four Swedes believes that burning the Quran is primarily meant to hinder Sweden's NATO membership, however a majority of 59% believe it is to provoke and protest against Islam.

96% of Swedes believe it is crucial to protect freedom of expression in Sweden, with 68% considering it highly important and 28% considering it somewhat important.

The hesitancy likely arises from the question of whether burning the Quran should be permissible under the banner of freedom of expression.

Regarding Quran burning, 38% of Swedes want it to be prohibited. Similarly, the same proportion of people want to ban burning the Swedish flag, the Torah, and the Bible. This shows that there is no significant difference in support for prohibiting the burning of various religious texts as the level of support remains consistent, the report said.

An interesting national difference exists between the Moderate Party (M), the Sweden Democrats (SD), and other parties. SD and M supporters are more inclined to ban the burning of the Swedish flag, while followers of other parties are more likely to advocate for banning the burning of religious texts.

Muslim world reacts

The report comes amid a score of calls from Muslim countries calling on the Swedish government to hold the perpetrators accountable.

Qatar, among other countries, has condemned the incidents and slammed them as a provocation of the feelings of millions of Muslims around the world. Top Qatari officials have come out to speak on the double standard approach towards Islamophobia in Europe. Qatar's outspoken Minister of State for International Cooperation [Lolwah Al Khater](#) pointed towards the "puzzling" lack of accountability regarding religion-based hate speech, especially against Muslims, despite legislations in favour of other minorities being easily approved.

"We remain puzzled by the opposition that some countries expressed to stopping religion-based hate speech especially against Muslims, while they themselves introduce new legislations and statements every day defending new self-defined minorities," maintained [Al Khater](#).



“By the same token STOP ISLAMOPHOBIA.”

The stances of certain European governments in allowing and enabling the repetition of such incidents based on legal arguments surrounding freedom of speech and individual rights has prompted many to point out the double standard approach to state condemnation of religious hate crimes.

The [Organization of Islamic Cooperation \(OIC\)](#) renewed calls on Denmark to take measures to halt repeated Quran burnings on Sunday as Danish authorities vowed to explore “legal” measures against such stunts.

The Danish government announced on the same day that it is proposing new measures against cultural and religious-based attacks in an OIC meeting on Monday.

Denmark’s latest statement said Quran burning incidents on its lands “have reached a level” where the European country is seen as a facilitator “of insult and denigration” of cultures and religions.

“The Danish government has clearly distanced itself from and condemned the burnings of the holy Quran. The burnings are deeply offensive and reckless acts committed by few individuals. These few individuals do not represent the values the Danish society is built on,” the statement stressed.

Denmark also said the actions “play into the hands of extremists” and spread divisions at critical times.

Last month, Iraqi migrant Salwan Momika staged a provocative move in Sweden with the permission of Swedish authorities, followed by another incident on 20 July in which he stepped on the holy scripture.

The OIC had responded to the move by suspending the status of Sweden’s special envoy to the bloc as Iraq expelled the Swedish ambassador in Baghdad. Qatar had also summoned the Swedish ambassador in protest of the burning of the Quran.

The Gulf state was also among a list of countries that voted in favour of a United Nations’ motion that called on nations to step up their efforts to combat religious hatred.

The vote drew 12 rejections, the majority of which were European states, all of which were accused by activists of taking a double-standard approach in addressing hate speech.

Since the start of the year, far-right leaders in Europe – Denmark, the Netherlands and Sweden – have launched provocative Quran burning stunts that have triggered global outrage and drew condemnation from Muslim countries, including Qatar.

EDITOR’S COMMENT: What happened to Swedes? Once upon a time they used to love and support all the people worldwide. Why did they change their status? They do not like what Sweden became. It is a good opportunity to study Ancient Greece mythology – the one with Aeolus and its bags.

What is Optical Camouflage?

By Michael Anissimov

Source: <https://www.allthescience.org/what-is-optical-camouflage.htm>

Aug 01 – Optical camouflage is a hypothetical type of active camouflage currently only in a very primitive stage of development. The idea is relatively straightforward: to create the illusion of invisibility by covering an object with something that projects the scene directly behind that object.

Although *optical* is a term that technically refers to all forms of light, most proposed forms of optical camouflage would only provide invisibility in the visible portion of the spectrum. [Prototype](#) examples and proposed designs of optical camouflage devices range back to the late eighties at least, and the concept began to appear in fiction in the late nineties.

The most intriguing prototypes of optical camouflage yet have been created by the Tachi Lab at the University of Tokyo, under the supervision of professors Susumu Tachi, Masahiko Inami and Naoki Kawakami. Their prototype uses an external camera placed behind the cloaked object to record a scene, which it then transmits to a computer for [image processing](#). The computer feeds the image into an external projector which projects the image onto a person wearing a special retroreflective coat. This can lead to different results depending on the quality of the camera, the projector, and the coat, but by the late nineties, convincing illusions were created. The downside is the large amount of external hardware required, along with the fact that the illusion is only convincing when viewed from a certain angle.

Creating complete optical camouflage across the visible light spectrum would require a coating or suit covered in tiny cameras and projectors, programmed to gather visual data from a multitude of different angles and project the gathered images outwards in an equally large number of different directions to give the illusion of invisibility from all angles. For a surface subject to bending like a flexible suit, a massive amount of computing power and embedded sensors would be necessary to continuously project the correct images in all directions. This would almost certainly



require sophisticated [nanotechnology](#), as our computers, projectors, and cameras are not yet miniaturized enough to meet these conditions.



Although the suit described above would provide a convincing illusion to the naked eye of a human observer, more sophisticated machinery would be necessary to create perfect illusions in other electromagnetic bands, such as the [infrared](#) band. Sophisticated target-tracking software could ensure that the majority of computing power is focused on projecting false images in those directions where observers are most likely to be present, creating the most realistic illusion possible.

Creating a truly realistic optical illusion would likely require Phase Array Optics, which would project light of a specific amplitude and phase and therefore provide even greater levels of invisibility. We may end up finding optical camouflage to

be most useful in the environment of space, where any given background is generally less complex than earthly backdrops and therefore easier to record, process, and project.

●► Read also: <https://www.ijert.org/research/optical-camouflage-technology-IJERTV2IS110327.pdf>

Why Did the United States Invade Iraq? The Debate at 20 Years

By Joseph Stieb

The Scholar | Vol 6, Iss 3 Summer 2023 | 11-28

Source: <https://tnsr.org/2023/06/why-did-the-united-states-invade-iraq-the-debate-at-20-years/>

Twenty years after the United States invaded Iraq, there is no shortage of explanations for why this war took place. Political scientists and journalists dominated the early waves of scholarship on the subject, but in the last few years historians have increasingly intervened. This includes major new works published this year from Melvyn Leffler and Samuel Helfont.¹ The invasion of Iraq remains the single most important foreign policy decision by a U.S. president in the 21st century, so the surfeit of analysis should surprise no one.

This article maps out the debate on the Iraq War's origins as they have developed over the last 20 years. It aims to play honest broker between competing schools of thought, clearly laying out their interpretations, assessing points of tension, and factoring in the influences of politics and ideology on scholarship. Below, I will show how divergent interpretations of the war have emerged from the different lenses, methodologies, and objectives that scholars have brought to the table.

No single article can tackle every aspect of Iraq War scholarship. Thus, this essay focuses on three questions that are essential for explaining the war's origins but that continue to divide scholars. First, was the Bush administration's decision to invade Iraq driven more by the desire for security or the pursuit of primacy? Second, was the Bush administration's decision to pursue "coercive diplomacy" in the fall and winter of 2002–2003 a genuine attempt to avoid war or a means to legitimize a decision for war made earlier in 2002? Third, how much did neoconservatives matter in the making of the Iraq War?



The first question — security vs. hegemony — constitutes the primary point of scholarly disagreement about the Iraq War. Security-focused explanations like those found in Leffler's new book argue that the Bush administration's primary motive was protecting the nation from future terrorist attacks in the transformed, post-9/11 environment in which threats like Iraq had to be re-evaluated.² Scholars in the hegemony school like Ahsan Butt argue, in contrast, that the Bush administration used 9/11 and the threat of Iraqi weapons of mass destruction as a pretext to justify a war that was motivated primarily by the desire for regional and/or global hegemony.³ Other important questions flow from this security-hegemony divide, including the nature of Bush's coercive diplomacy strategy and the role of neoconservatives in causing the war.

Useful historiographical analysis begins with explaining why the scholarly landscape looks the way it does and then proposes directions for growth. The unavoidable challenge of interpreting history is all the more difficult in this case, because scholars have access to only a fraction of the primary documentation. As a result, much of the debate has boiled down to how to approach, critique, and contextualize the same small body of sources. In addition, political and policy debates have often had an outsized, if not always ideal, impact on the scholarship.⁴

In methodological terms, the security school has largely trusted that what policymakers say their motives were, both at the time and in hindsight, is what they actually were, unless clear contradictory evidence can be found. For this group, the critical context for understanding the war is the pressurized post-9/11 environment in which protecting the nation was everything and in which most parties saw Iraq as a significant threat.

The hegemony school retorts that key questions about the war do not make sense when viewed through a security prism. This group points out that scholars should not trust the testimonies of policymakers who have a strong incentive to deny the more ideological or delusional aspects of their actions. Instead, these scholars cast the Iraq War decision in wider historical contexts, identifying factors like the longstanding primacist policy views of figures like Vice President Dick Cheney, Secretary of Defense Donald Rumsfeld, and Deputy Secretary of Defense Paul Wolfowitz that they believe have more explanatory relevance than security factors.

As might be expected with such a recent and contentious event, the Iraq War has not merely been a subject of scholarly analysis but an arena for rival political and policy views, especially when it comes to what lessons we can take away. Debates on the war's origins have real-world stakes in terms of what the United States should learn from the war as it moves into an era of great-power competition. Security school scholars often view the Iraq War as an understandable mistake given the harrowing post-9/11 context and the fact that almost everyone believed Iraq was producing weapons of mass destruction at some level.⁵ They therefore rarely call for major revisions to post-Iraq U.S. foreign policy. The hegemony school, in stark contrast, argues that this war emerged from the ruinous bipartisan pursuit of global primacy and that similar disasters will occur if that grand strategy is not abandoned.

A few caveats: This essay does not defend the existence of the security-hegemony divide nor take sides in this debate. Instead, it seeks to explain its parameters, evolution, and stakes. Some may object to this depiction of two broad interpretive camps as oversimplifying a vast body of nuanced scholarship. To address this problem, this article tries to identify possible means of synthesizing these interpretations. The security and hegemony camps do overlap in some ways, as discussed below, but this divide also reflects that scholars themselves have identified genuine differences about what set of factors drove the causal boat. Finally, this essay concludes with a plea for more global and cultural analysis of the Iraq War as a way to challenge this binary.

Nevertheless, there is value in "lumping" in historiographical analysis, which is particularly useful for newcomers to the field or non-specialists who want a bird's-eye view of the existing scholarship. This broad approach also helps to identify the essential questions that continue to divide and drive the field, questions that future work on the Iraq War should tackle. Consequently, this essay does not exhaust the totality of scholarship of the Iraq War, nor does it offer its own historical or theoretical explanation of the war's causes. Both tasks would occupy far too much space. Thus, certain topics on which there is outstanding work receive less attention, including the beliefs and decisions of the Baathist regime, the history of weapons inspectors prior to 2002–2003, problems with pre-war planning, and the international diplomacy that preceded the war's onset. These questions are important for fully understanding the war's origins, but they have not formed the primary lines of scholarly disagreement, which are the focal points of this essay.⁶



Security vs. Hegemony: The Core Divide

Did the United States invade Iraq in a misguided effort to remove a security threat in the unprecedentedly heated post-9/11 atmosphere? Or did U.S. leaders use 9/11 as a pretext to pursue an opportunistic war that was really about American hegemony?

The obvious answer might be “a little of both,” or that this is a false dichotomy. The United States, for example, could have pursued security through a hegemonic grand strategy that might have involved regime change in nations like Iraq. Iraq could have been seen as both a real security threat *and* an obstacle to U.S. primacy.⁷

Nonetheless, this core divide among scholars is real, reflecting meaningful differences in interpretation, contextualization, and even politics. The scholars themselves frequently identify security- or hegemony-based factors as the most salient. Security-focused explanations maintain that, in the post-9/11 atmosphere, hegemonic aspirations were secondary to security imperatives. Hegemony-focused explanations rarely dismiss security altogether, but they contend that concerns about Iraq’s weapons of mass destruction and terrorist ties served as pretexts for deep-seated hegemonic designs. Each school casts the war in different contexts, with the security school emphasizing the post-9/11 moment and the hegemony school stressing the preceding decades in which the architects of the war developed their policy worldviews.

The Security School

Leffler is the dean of the security school, which also includes Robert Jervis, Frederic Bozo, Alexander Debs, Ivo Daalder, James Lindsay, Peter Hahn, Hakan Tunc, and Steve Yetiv. While these scholars do not ignore larger U.S. goals and ideologies, they argue that the Bush administration’s pursuit of security in the aftermath of 9/11 was the primary cause of the decision to invade. Bush, Leffler writes, “went to war *not* out of a fanciful idea to make Iraq democratic, but to rid it of its deadly weapons, its links to terrorists, and its ruthless, unpredictable tyrant.”⁸ Jervis does not dismiss democracy as a secondary motive, but he claims that “[t]he fundamental cause of the invasion was the perception of unacceptable threat from Saddam [Hussein] triggered by the combination of pre-existing beliefs about his regime and the impact of terrorist attacks.”⁹ Bozo concludes that “the choice for war clearly arose first and foremost from a logic of national security.”¹⁰ Security school arguments emphasize the transformative impact of 9/11 on U.S. national security as essential for understanding the Iraq War. Leffler and Jervis argue that, while the Bush administration entered office with several prominent regime-change proponents in high-ranking positions, it did not obsess over Iraq in its first nine months nor make meaningful moves toward toppling Saddam Hussein. Bush also came into office opposing nation-building and promising strategic restraint.¹¹

But scholars in the security school agree that the weapons of mass destruction-terrorism-rogue state security threat was no mere pretext but rather the driving motive for the war.

The 9/11 attacks, however, revolutionized U.S. foreign policy and set the stage for the Iraq War. The Bush administration felt extraordinary anger, fear, and vulnerability after 9/11, which prompted it to rethink other security threats.¹² Leffler argues that, for the Bush team, “the risk calculus had changed dramatically after 9/11.”¹³ They could no longer tolerate states that pursued weapons of mass destruction, threatened their neighbors and/or the United States, and supported terrorism.

Why, then, invade Iraq in particular? The Bush administration viewed Iraq as the “nexus” of these threats.¹⁴ As Bush himself argued, Iraq checked the following boxes more than any other state: “state sponsors of terror ... sworn enemies of America ... hostile governments that threatened their neighbors ... regimes that pursued WMD [weapons of mass destruction].”¹⁵ Top officials may have made major mistakes and exaggerated regarding Iraq’s weapons of mass destruction and terrorist ties, but they did not hoodwink the people. Rather, they truly believed these threats were real and growing. Moreover, few analysts at the time, even from nations that opposed the war, accurately assessed the truth that Saddam was not engaged in meaningful production of weapons of mass destruction. Saddam also obstructed inspectors for nearly a decade, creating the reasonable impression that he aimed to resume production of such weapons.¹⁶

The United States could not wait for the Iraqi threat to fully emerge given the risk of “the smoking gun coming in the form of a mushroom cloud,” as National Security Adviser Condoleezza Rice famously stated.¹⁷ So, it declared a right to launch preventive wars to remove the threat. This



presumed right formed the core of the Bush Doctrine, which, for the security school, was less a blueprint for primacy than an adaptation of longstanding ideas about the use of force in the face of a new threat. [18](#)

For the security school, the Iraq War did not stem primarily from grand schemes of extending U.S. hegemony or liberal values. Overwhelming U.S. military power and the unipolarity of the international system made regime change possible, but the war was not motivated primarily by these factors. Leffler asserts that “missionary fervor or idealistic impulses” played little role in the Bush team’s decisions. [19](#) Tunc contends that hegemony makes little sense as a motive for the Iraq War, as eliminating this relatively minor rival would not have changed the global balance of power. [20](#)

Idealistic dreams and the global imbalance of power, after all, had existed for at least a decade when 9/11 happened. The attack was the decisive new variable that prompted a reevaluation of national security, which ultimately led to the invasion. Leffler summarizes the fundamental, security-centric causes: “They were seeking to safeguard the country from another attack, save American lives, avoid the opprobrium that would come from another assault, and preserve the country’s ability to exercise its power in the future on behalf of its interests.” [21](#)

Security school scholars often take a more sympathetic view of the Bush administration’s Iraq policy. Leffler stresses the emotional trauma of 9/11, including top officials’ visits to Ground Zero and meetings with first responders and the bereaved. Context is vital to this interpretation, as he argues: “Critics forget how ominous the al Qaeda threat seemed and how evil and manipulative Hussein really was.” [22](#) He maintains that the Bush team sought to “do the right thing” and protect the nation from what they believed was an imminent threat. [23](#) But scholars in the security school agree that the weapons of mass destruction-terrorism-rogue state security threat was no mere pretext but rather the driving motive for the war. As Jervis argues, given the consensus about Iraqi weapons of mass destruction and the post-9/11 need to rethink security threats, “There is little reason to doubt that Bush and his colleagues sincerely believed that Saddam had active WMD [weapons of mass destruction] programs.” [24](#)

The security school overlaps considerably with Bush officials’ memoirs, which also emphasize security motives for war. [25](#) These memoirs depict the emotional weight of the post-9/11 moment, in which the administration felt responsibility for not stopping 9/11 and dreaded the next attack. “I could not have forgiven myself had there been another attack,” recalls Rice. [26](#) Bush writes that “before 9/11, Saddam was a problem America might have been able to manage.” However, “through the lens of the post-9/11 world, my view changed.” [27](#) Protecting the nation from further terrorist attacks became the overriding priority, and threats like Iraq could no longer be tolerated. [28](#) Official memoirs emphasize that the administration did not want war with Iraq and sought ways to avoid it, but ultimately national security concerns required removing this menace. [29](#)

This overlap makes sense given the reliance of scholars like Leffler on interviews with administration insiders. However, it also raises concerns that the security school may be accepting policymakers’ portrayals of events at face value. Bush officials have an obvious interest in saying that they remained open to non-violent solutions to the Iraq problem or that they were not idealistic crusaders. [30](#) As we will see, the hegemony school takes a more adversarial approach to this question.

The Hegemony School

Scholars in the hegemony school include Butt, Stephen Walt, Andrew Bacevich, Patrick Porter, Paul Pillar, G. John Ikenberry, David Harvey, John Mearsheimer, and Jeffrey Record. They tend toward the realist school of international relations, but not exclusively. They acknowledge the role of security concerns in motivating the Iraq War, but they view security rationales as radically incomplete explanations. Their core claim is that the primary motivation of the invasion was maintaining and expanding U.S. hegemony. The hegemony school splits, however, on whether the United States sought realist or liberal forms of hegemony.

On the side of realist hegemony, Butt argues that the war stemmed from the “desire to maintain the United States’ global standing and hierarchic order,” with security acting more as a pretext for domestic consumption than a causal factor. [31](#) 9/11 threatened U.S. hegemony, leading the United States to opt for a “performative war” that would re-establish “generalized deterrence,” or the reputation for unassailable power and the willingness to use it that undergirded hegemony. [32](#) He quotes Rumsfeld saying on 9/11 that “[w]e need to bomb something else [other than Afghanistan] to prove that we’re, you know, big and



strong and not going to be pushed around by these kinds of attacks.”³³ Butt contends that nothing in the available intelligence about Iraq suggested that it was an imminent threat. It was, however, a convenient foe for demonstrating U.S. power, as it had not yet constructed any weapons of mass destruction, remained weak militarily and isolated diplomatically, and was detested by the U.S. public.³⁴

Scholars in the realist-hegemony camp see the Iraq War as a means to maintain realist priorities like unipolarity and U.S. freedom of action in the world.

Stephen Wertheim agrees, arguing that “the decision to invade Iraq stemmed from the pursuit of global primacy,” the goal of which is to “dissuade other countries from rising and challenging American dominance.”³⁵ Ikenberry and Daniel Deudney concur: “The primary objective of the war was the preservation and extension of American primacy in a region with high importance to American national interests.”³⁶ Record likewise contends that “the invasion was a conscious expression of America’s unchecked global military hegemony that was designed to perpetuate that hegemony by intimidating those who would challenge it.”³⁷

Scholars in the realist-hegemony camp see the Iraq War as a means to maintain realist priorities like unipolarity and U.S. freedom of action in the world. The Bush administration seized 9/11 and the ostensible Iraqi weapons-of-mass-destruction threat as a “pretext,” “opportunity,” or “rationale” to extend this agenda, which they believed would destroy the terrorist threat and other challenges to U.S. power.³⁸ Democratization was a secondary motive to justify a war that was grounded in the pursuit of power.³⁹

Walt, Porter, and Bacevich agree that the United States sought to demonstrate its power and preserve hegemony by invading Iraq, but they contend that the Bush administration aimed specifically to solidify liberal hegemony. Under this grand strategy, the United States sought to spread liberal democracy and capitalism, which were not only good in themselves but were ways to maintain global predominance.⁴⁰ The Cold War had restrained this strategy, but the Soviet collapse allowed the United States to pursue it with reckless idealism and hubris. The bipartisan foreign policy establishment came to assume the universality of liberal ideals and a presumed U.S. right to intervene anywhere in the world, either to protect human rights or suppress challenges to American power.⁴¹

When attacked on 9/11, according to this narrative, the United States did not examine whether liberal hegemony was generating resistance. Instead, the Bush administration, with bipartisan backing, escalated the pursuit of liberal hegemony and asserted a unilateral right to change the regimes of rival states through preventive war, also known as the Bush Doctrine. Security school scholars see this doctrine as a response to a new category of threat. The hegemony school, however, views it as a blueprint for preserving U.S. primacy that asserted the unilateral American right to destroy potential threats like Iraq and stated a desire to prevent the rise of peer competitors.⁴² Some scholars also emphasize the importance of protecting Israel and advancing U.S. oil interests as additional hegemonic motives for this war, although these remain controversial explanations.⁴³

For Walt, Porter, and others, the Iraq War emerged from the pursuit of liberal hegemony, a revisionist grand strategy that sought to spread democracy and other liberal values, topple tyrants, and thereby build a more peaceful and cooperative world order. Following this vision, the United States wanted not only to remove a threat but to revolutionize Middle Eastern politics by implanting democracy in Iraq.⁴⁴ They cite considerable evidence that democracy promotion was an important motive for the war, particularly for Bush, rather than a mere justification for a war based in power.⁴⁵ The 2002 *National Security Strategy*, for example, reflected this universalistic idealism in declaring, “The great struggles of the twentieth century between liberty and totalitarianism ended with a decisive victory for the forces of freedom — and a single sustainable model for national success: freedom, democracy, and free enterprise.”⁴⁶

This war fit the longstanding and essentially liberal belief of many U.S. policymakers that autocracies represent an inherent threat to long-term peace, prosperity, and security and that only a democratic international order can assure these goods.⁴⁷ As Bush argued in a February 2003 speech, “The world has a clear interest in the spread of democratic values because stable and free nations do not breed the ideologies of murder.”⁴⁸ Liberal idealism, as Michael MacDonald argues, also convinced the Bush administration that regime change in Iraq would be easy, because the Iraqis would quickly adopt the default of democracy after the removal of the Baathists.⁴⁹

Mearsheimer calls the Iraq War “probably the best example of this kind of liberal interventionism” that dominated post-Cold War U.S. thinking.⁵⁰ Bacevich argues that the weapons of mass



destruction threat was a “cover story” and that the war’s main objectives were to “force the Middle East into the U.S.-dominated liberal order of capitalist democracies and assert its prerogative of removing regimes that opposed U.S. interests.”⁵¹ As Porter contends, “The Iraq War ... was an effort to reorder the world. Its makers aimed to spread capitalist democracy on their terms.”⁵²

To some extent, this divide within the hegemony camp reflects the different worldviews of the top decision-makers in the Bush administration. Rumsfeld and Cheney fit a more realist paradigm, focusing on reasserting power more than spreading democracy. Others, like Wolfowitz, viewed the Iraq War as part of the liberal project. Bush embodied a mix of these perspectives.⁵³

Differences over whether the United States sought to achieve realist or liberal hegemony should not obscure fundamental commonalities of the hegemony school. These scholars concur that the United States had been pursuing some form of primacy well before 9/11, that 9/11 both threatened that primacy and provided a pretext or opportunity to reassert it, and that Iraq was less a threat than a convenient target for solidifying hegemony.

In terms of contextualization, the pre-9/11 era is more important for the hegemony school than the security school, as the former stress continuities in U.S. foreign policy stretching back into the Cold War.⁵⁴ These scholars emphasize that key architects of the war like Rumsfeld, Cheney, and Wolfowitz had openly supported U.S. hegemony in the decades preceding 9/11. Many cite the 1992 *Defense Planning Guidance*, which was written by Zalmay Khalilzad and Abram Shulsky under the oversight of Wolfowitz, then serving under Cheney.⁵⁵ This document endorsed a hegemonic grand strategy that would maintain indefinite global military dominance and seek to “prevent the re-emergence of a new rival.”⁵⁶ Wolfowitz, Rumsfeld, and a host of other future Bush administration officials also signed open letters in the late 1990s calling for regime change in Iraq and a primacist grand strategy.⁵⁷

Following 9/11, these hegemonists immediately linked the Baathist regime to the terrorism problem in spite of a dearth of evidence, pushed dubious intelligence, hyped the Iraqi threat, and downplayed the risks of invasion. For the hegemony school, this is evidence that the administration “wanted war,” to paraphrase Record’s book, and that its later claims that it went to war regretfully are self-serving myths.⁵⁸

Some Bush administration officials have bucked the official security-focused explanation and acknowledged the importance of larger ideological or hegemonic designs. CIA Director George Tenet wrote in his memoir that top administration members seemed uninterested in figuring out the details of Iraq’s weapons of mass destruction programs. He interpreted this to mean that they decided to invade Iraq using such weapons as a pretext. He held that “The United States did not go to war in Iraq solely because of WMD [weapons of mass destruction]. In my view, I doubt it was even the principal cause. Yet it was the public face put on it.” As real reasons, he pointed to “larger geostrategic calculations, ideology,” and “democratic transformation.”⁵⁹ White House Press Secretary Scott McLellan similarly concluded that “removing the ‘grave and gathering danger’ Iraq supposedly posed was primarily a means for achieving the far more grandiose objective of reshaping the Middle East as a region of peaceful democracies.”⁶⁰

Synthesizing the Security and Hegemony Schools

Why can’t the hegemony and security schools just get along? Some scholars have tried to synthesize these approaches. Michael Mazarr, Robert Draper, and Justin Vaisse’s works examine the national security urgency of the post-9/11 moment without ignoring the historical context of U.S. hegemony and idealism.⁶¹ In my own attempts at synthesis, I have contended that during the 1990s a bipartisan “regime change consensus” formed on Iraq that predisposed the U.S. foreign policy establishment to support Saddam’s ouster and to view containment as a failing alternative policy. Broad agreement about U.S. hegemony fed this consensus and made the Iraq War seem logical to many U.S. elites. Nevertheless, 9/11 was a critical variable that drastically decreased America’s willingness to tolerate threats like Iraq while providing more leeway to U.S. leaders to pursue risky strategies.⁶²

One way of synthesizing these schools is to create a division of causal labor, wherein the hegemony school helps explain “Why Iraq?” and the security school addresses “Why now?” Hegemony school analysts often ask: If the United States was really concerned about the proliferation of weapons of mass destruction, why not focus on countries with more advanced programs, like North Korea? If the United States was really concerned about terrorism, why not focus on more active state sponsors, like Iran?



After all, as Pillar and others argue, the Bush administration used the intelligence process not in a good-faith effort to accurately assess Iraq's weapons of mass destruction but to gather — if not inflate — evidence to support the case for regime change.

These inconsistencies having to do with “Why Iraq?” expose a key problem for security-based explanations: Iraq, which became the central front of the War on Terror, was neither the most powerful “rogue state,” nor was it involved in 9/11. Instead, in the hegemonic framework, Iraq was an opportunity more than a threat, and its putative weapons of mass destruction programs were a pretext more than a motive. As former CIA intelligence analyst Paul Pillar starkly puts it, concern about such weapons “was not the principal or even a major reason the Bush administration went to war.” It was “at most a subsidiary motivator of the policy.”⁶³ After all, as Pillar and others argue, the Bush administration used the intelligence process not in a good-faith effort to accurately assess Iraq's weapons of mass destruction but to gather — if not inflate — evidence to support the case for regime change.⁶⁴

However, the hegemony school struggles to answer the “Why now?” question. If the bipartisan pursuit of hegemony and liberal idealism are constants in U.S. foreign policy, then why did the Iraq War not happen sooner, possibly after inspectors left Iraq in 1998? By focusing on how 9/11 reshaped U.S. foreign policy and threat perception, the security school gets at a fundamental point that few analysts contest: A U.S. invasion and occupation of Iraq is virtually inconceivable without 9/11.

One interesting point of agreement between the security and hegemony schools is that the end of the Cold War constitutes an essential precondition for the Iraq War. The idea of the United States in the midst of the Cold War invading a mid-sized country — once a Soviet satellite — to change its regime seems far fetched. The hegemony school particularly emphasizes the importance of unipolarity, which it believes allowed dreams of hegemony, realist or liberal, to run wild in the U.S. imagination.⁶⁵ This leads one to speculate as to whether the return of multipolarity will deter the United States from further attempts at direct regime change.

The relationship between the 1990–1991 Gulf War and the 2003 Iraq War remains an under-studied aspect of this field. Scholars like Helfont, Christian Alfonsi, and myself have argued that the Gulf War's messy ending initiated a pattern of conflict between the United States and Iraq that festered throughout the 1990s, creating a strong desire in the U.S. political establishment to finish the job, even before 9/11.⁶⁶ There was, after all, no war with Iran or North Korea in the 1990s, nor was there an Iran or North Korean Liberation Act. There was, however, the 1998 Iraq Liberation Act, which declared regime change as the official U.S. policy toward Iraq.⁶⁷ Relatively few works, however, systematically trace U.S.-Iraqi relations through this period, although Helfont's recent book significantly rectifies this by tracing Iraq's challenge to the post-Cold War, U.S.-led international order through the 1990s.⁶⁸

Despite attempts at synthesis, there is a meaningful tension between the security and hegemony schools that makes any kind of reconciliation difficult. It is hard to interpret a war as both predetermined and contingent — harder still to view the Bush administration as obsessed with regime change and open to many ways of disarming Iraq. Moreover, as this section demonstrates, there is primary source evidence to support both major interpretations.

The security and hegemony schools' points of contrast also matter for how the war is interpreted as a whole. Was it an understandable tragedy or an unforced and unforgivable blunder?⁶⁹ In terms of periodization, was the war essentially rooted in a response to 9/11, or do its roots stretch back decades in U.S. foreign policy? Finally, does the Iraq War, especially the controversial Bush Doctrine, represent a sharp change in U.S. diplomatic history or continuity with previous trends, goals, and ideas?⁷⁰

What Was “Coercive Diplomacy” All About?

Whatever side scholars favor in the security-hegemony debate shades how they understand other key questions about the war's origins. This essay tackles two additional issues that have divided scholars, starting with the question of why Bush attempted a “coercive diplomacy” strategy in late 2002 and early 2003.

In the fall of 2002, under pressure from British Prime Minister Tony Blair and Secretary of State Colin Powell, Bush decided to take the “diplomatic track” on Iraq. On Sept. 12, at the United Nations, he called for Iraq to readmit weapons inspections or face being overthrown. He also



sought a congressional authorization to use force against Iraq.⁷¹ At the same time, the build-up of U.S. troops in the region put the credible threat of force behind this final attempt at diplomacy. Rice describes this strategy as “coercive diplomacy.”⁷²

But what was the purpose of coercive diplomacy? Was it a genuine attempt to peacefully disarm Iraq? Or was it a way of gaining legitimacy and allied and domestic political support for a predetermined policy of regime change? This debate matters for establishing when the Bush administration made the decision for war and the extent to which it was simply hell bent on regime change, no matter the circumstances. The security-hegemony debate is important but somewhat deterministic. The coercive diplomacy debate incorporates questions about the contingency of the war as well as possible off-ramps.

Leffler writes that, in early 2002, Bush was “not yet ready to choose between containment and regime change,” and he remained undecided into the fall of 2002.⁷³ Bush was torn as to whether disarmament could be achieved without regime change. Coercive diplomacy was a final attempt to find this out. When he adopted this strategy, he accepted that it might mean that war would not occur and that Saddam might remain in power for the time being. He also rejected, for the moment, the advice of more hawkish advisors like Cheney and Rumsfeld that working through the United Nations would be counter-productive.⁷⁴ As Leffler writes, Bush “decided to see if he could accomplish his key objectives ... without war.”⁷⁵ In this narrative, Bush did not decide to invade until January 2003, after Iraqi authorities had failed to fully comply with a new round of weapons inspections.⁷⁶

Other scholars, especially those in the security school, agree with Leffler’s view of coercive diplomacy. Frank Harvey claims that coercive diplomacy sought “to re-invigorate a failing containment policy by reinforcing multilateral, U.N. inspections that demanded full and complete compliance.”⁷⁷ Debs and Nuno Monteiro also agree that in supporting new inspections the Bush administration genuinely sought to test Iraqi cooperation and avoid war.⁷⁸

These analyses stress the contingency of Bush’s approach to Iraq. Some Bush officials may have been impassioned advocates of regime change, but Bush nonetheless proceeded deliberately and gave peaceful methods of disarmament a final chance. He did so because he prioritized disarmament by whatever means, not regime change for ulterior reasons. Again, this account matches U.S. leaders’ descriptions of their own actions. Bush states in his memoir, “My first choice was to use diplomacy” on Iraq.⁷⁹ Coercive diplomacy was an earnest attempt to avoid war, but Saddam’s failure to comply with inspections compelled Bush to choose war in early 2003.⁸⁰ Rice similarly claimed, “We invaded Iraq because we believed we had run out of other options.”⁸¹

For scholars like Leffler, the situation remained fluid and contingent until just months before the invasion. For scholars like Mazarr, the war was virtually inevitable once the Bush administration set its sights on Iraq in early 2002.

Michael Mazarr and others challenge Leffler’s account of coercive diplomacy and locate the decision to invade well before early 2003. Mazarr writes that “between September 11 and December 2001 ... the Bush administration — while nowhere near what would be defined as the formal ‘decision’ to go to war — had irrevocably committed itself to the downfall of Saddam Hussein.”⁸² War planning began in November 2002, and Bush made several private and public comments before spring 2002 that he intended to remove Saddam.⁸³

That fall, Bush sided with Powell in choosing the diplomatic track, but even Powell never challenged the wisdom of invading Iraq.⁸⁴ There was almost no debate in his administration about whether invading Iraq was a sound idea, suggesting that the decision had been made even before the coercive diplomacy effort began.⁸⁵ Mazarr adds that a “tidal wave of evidence can be found that many senior officials assumed war was inevitable long before September 2002.”⁸⁶ The Bush administration quickly judged that the inspections had failed in early 2003 and cemented the decision to invade in January.⁸⁷

My own research concurs with Mazarr and further adds that the idea that Bush sought to restore containment through coercive diplomacy makes little sense. Bush had already made the case earlier in 2002 that containment could not handle the “nexus” threat. Moreover, most of his advisers and the policy establishment already viewed containment as a dead letter. Finally, the Bush administration was exceedingly doubtful of the efficacy of inspections, and it set such a high bar for their success as to virtually predetermine failure.⁸⁸

Scholars in the hegemony school generally agree with Mazarr’s analysis of coercive diplomacy. They hold that the Bush administration was uninterested in peacefully resolving this crisis



because it was looking for an opportunity to assert U.S. power. They therefore view coercive diplomacy as a charade to legitimize a predetermined war. Butt, for example, argues that Iraq could not have done anything to avoid war, because the United States had decided to crush a rival to re-establish generalized deterrence.⁸⁹ John Prados contends that Bush made the decision for war in the early spring of 2002, and Richard Haass locates that decision in July 2002, all before coercive diplomacy began.⁹⁰

As with the core security-hegemony divide, the debate about coercive diplomacy resists resolution. For scholars like Leffler, the situation remained fluid and contingent until just months before the invasion. For scholars like Mazarr, the war was virtually inevitable once the Bush administration set its sights on Iraq in early 2002. A possible synthesis may be that the administration's intense pessimism about the possibility that Saddam would give in to U.S. threats and comply with inspections constituted a *de facto* decision for war, if not an absolutely final determination.⁹¹ If anything, coercive diplomacy might be another under-examined aspect of the Iraq War, skipped over by numerous analyses that assign the war's origins to security or hegemony.⁹² Doing so leads to overly deterministic explanations of the war that leave little room for contingency.

One way this impasse might be addressed is through more analysis of the State Department's role in the lead-up to war. Powell and his deputy Richard Armitage supported the war but were not true believers, and many skeptics of the war filled the State Department's higher ranks.⁹³ When more sources become available, it will be interesting to see whether Powell or anyone else asked any critical questions about the fundamental decision to go to war or pressed Bush to pursue coercive diplomacy thoroughly. This would show whether there really was uncertainty in the administration and openness to non-violent solutions, as Leffler claims, or whether the United States was on an unalterable path to war before the fall of 2002, as Mazarr argues.⁹⁴

Scholars should be careful, however, of thinking that new documentary evidence will fully resolve these disagreements. The British Iraq Inquiry, published in 2016, released a flood of primary sources and interviews on British policymaking on Iraq from 2001 to 2009.⁹⁵ Numerous scholars have drawn on this fascinating material, but interpretive tensions remain because they look at this evidence through different lenses. For example, Leffler argues that Blair's correspondence with Bush after 9/11 demonstrates that neither party was rushing to war with Iraq but merely establishing a general timeframe for pressuring the Iraqi regime to disarm.⁹⁶ This supports his larger argument that the Bush administration was not obsessed with war, attempted other means of disarming Iraq, and only decided on war after the exhaustion of other options.

Butt, in contrast, argues that these same sources demonstrate that "war was decided upon very soon after — probably even on-9/11." Blair, after all, told Bush on Oct. 11, 2001, that "I have no doubt we need to deal with Saddam" and that "we can devise a strategy for Saddam deliverable at a later date."⁹⁷ For Butt, this source shows that Bush and Blair agreed on the goal of regime change in Iraq and the reassertion of U.S. hegemony in the Middle East almost immediately after 9/11. Blair merely cautioned Bush not to rush into war without building a coalition.⁹⁸ Porter, author of a book on Britain's war in Iraq, also draws heavily on the Iraq Inquiry and arrives at a similar conclusion. He contends that the Blair government was as ideologically committed to strategic primacy and the spread of liberal democracy as Bush. It never seriously considered alternatives but "worried predominantly about how to create conditions that would legitimize a British military campaign, that would generate enough support."⁹⁹

The discrepancies between scholars using the same documents demonstrate the importance of the interpretive frameworks that analysts bring to their sources. As a result, new sources will not necessarily lead to convergence between interpretive camps.

How Important Were the Neocons?

The last major question this essay tackles about the Iraq War's origins is the role of neoconservatives. Were they the intellectual architects of this war or extraneous to the decision to invade? While the alignment here is imperfect, the security school tends to downplay neoconservatives while the hegemony school usually argues for their central importance. Neoconservatives are a loose intellectual movement that has evolved considerably since its origins in the 1960s. Vaisse defines third-wave neoconservatism as a



nationalistic movement that peaked in the 1990s and early 2000s. It sought to promote U.S. primacy, “national greatness,” and the spreading of democracy, all with a unilateralist bent.¹⁰⁰ A significant number of neoconservatives worked in high positions in the Bush administration, most notably Wolfowitz.¹⁰¹

While neoconservative intellectuals like Robert Kagan and William Kristol clearly advocated for regime change in public discourse, debate about the role of neoconservatives in bringing about the Iraq War has been contentious. Much early commentary crudely suggested that a “cabal” of neoconservatives hijacked U.S. foreign policy and drove the nation into a disastrous war. For instance, then-Sen. Joe Biden, who voted to authorize the Iraq War but later regretted this decision, said in July 2003, “They seem to have captured the heart and mind of the President, and they’re controlling the foreign policy agenda.” Frank Harvey convincingly argues that these narratives are not only simplistic but provide cover for the many political groups who supported what became an unpopular war.¹⁰²

Harvey, Leffler, and others argue that neoconservatives were either irrelevant or of secondary importance in causing the Iraq War. Harvey takes an extreme position here, arguing that they were totally extraneous and, in fact, lost most of the debates on Iraq before the invasion.¹⁰³ Leffler and Mazarr argue that, although there were neoconservatives in the Bush administration, neither Bush nor the top echelon of decision-makers were neoconservatives.¹⁰⁴ Leffler downplays the role of neoconservatism or any other ideology in the administration’s decision-making, focusing instead on security motives.¹⁰⁵

Without these ideas, Flibbert concludes, invading Iraq would not have made sense, making the actions of neoconservatives essential to explaining the war.

Daalder and Lindsay argue that Bush and most of his top advisers were “assertive nationalists,” or “traditional hard-line conservatives willing to use American military power to defeat threats to U.S. security but reluctant as a general rule to use American primacy to remake the world in its image.”¹⁰⁶ Jane Cramer and Edward Duggan contend that Bush, Rumsfeld, and Cheney, the three most important decision-makers in the administration, were not neoconservatives but “primacists” and consistent hard-liners who had never shown concern for democratization or human rights in their long careers.¹⁰⁷ In his history of Bush’s war cabinet, journalist James Mann contends that Bush relied mainly on the “Vulcans” — like Cheney, Rumsfeld, Rice, Armitage, and Dov Zakheim — for foreign policy guidance, few of whom were neoconservatives. Rather, these Vulcans “were focused above all on American military power” and maintaining U.S. primacy, especially after the Vietnam debacle.¹⁰⁸

These authors agree that neoconservatives like Wolfowitz may have pushed for regime change, but their presence in the administration was not vital for making this war happen.¹⁰⁹ Mazarr also minimizes the role of neoconservatives — but not ideology in general. He contends that “many aspects of the neocons’ foreign policy assumptions reflected the prevailing conventional wisdom in the U.S. national security community,” including primacy, exceptionalism, and the universality of democracy.¹¹⁰

Some scholars in the realist hegemony school agree with this analysis. Butt dismisses the role of neoconservatives, arguing that they provided an ideological gloss for a war that was really about power.¹¹¹ Oddly enough, some neoconservatives concur with the minimization of their own roles. Kagan, for instance, contends that security concerns drove decision-making and that the war “can be understood without reference to a neoconservative doctrine.”¹¹²

Many scholars, especially in the liberal hegemony school, argue instead that neoconservatives played an essential role in causing the Iraq War. For them, neoconservatism helps to address a key question: Why, after 9/11, did the United States invade a country that had not attacked it?

As Andrew Flibbert argues, neoconservative policy entrepreneurship closed the conceptual gap between Iraq and terrorism. Figures like Wolfowitz, Doug Feith, and Scooter Libby interpreted 9/11 through a “larger ideational framework” about America’s role in the world and acted as policy activists inside the administration and in the public discourse. They helped to set the post-9/11 agenda with a focus on Iraq, at a time when figures like Rice and Powell seemed skeptical of such a focus. They advanced a host of arguments for war: the nexus threat, Saddam’s brutality, protecting U.S. interests in the region, advancing democracy, transforming the Middle East, asserting U.S. power, and even improving Israeli-Palestinian relations. Without these ideas, Flibbert concludes, invading Iraq would not have made sense, making the actions of neoconservatives essential to explaining the war.¹¹³



The hegemony school naturally focuses on the role of neoconservatives in constructing a liberal hegemonic war. Pillar argues that “[t]he chief purpose of forcibly removing Saddam flowed from the central objectives of neoconservatism,” the core of which is “the proposition that the United States should use its power and influence to spread its freedom-oriented values.”¹¹⁴ Walt and Mearsheimer concur: “The driving force behind the Iraq War was a small band of neoconservatives who had long favored the energetic use of American power to reshape critical areas of the world.”¹¹⁵ Gary Dorrien notes that this band was in fact quite large: Over 20 neoconservatives held high-ranking positions in the Bush administration, forming an activist core for pushing war with Iraq.¹¹⁶

Vaisse adds that in 2003 Cheney ordered 30 copies of the neoconservative *Weekly Standard* to the White House every week.¹¹⁷ He notes that, while Bush may have campaigned as a restraint-minded realist, he and Rice essentially adopted a neoconservative worldview after 9/11, speaking often of a U.S. obligation to topple tyrants and spread liberal values.¹¹⁸ Other analysts show how neoconservatives led the way in promoting damning, if dubious, information about Saddam’s weapons of mass destruction programs and links to al-Qaeda that would help sell the war.¹¹⁹ Journalistic accounts of the Iraq War also tend to stress the role of neoconservative networks and personalities in clearing the path to war. They effectively demonstrate the close personal contacts of neoconservative intellectuals and Iraqi exiles like Ahmad Chalabi with top Bush administration officials. While they sometimes do not make systematic arguments about the war, they certainly show that neoconservative influence was swirling around the administration and the foreign policy establishment at the time.¹²⁰ The neoconservative issue is germane to larger questions about the Iraq War and recent U.S. foreign policy. Was ideology a fundamental motivator of the decision to invade or a justification that was developed to sell the war? Is the way to restore balance and restraint to U.S. foreign policy after Iraq simply to purge neoconservatives, or is more profound change needed? Are neoconservatives simply a new expression of America’s exceptionalist identity and missionary impulses dating back centuries, or are they a discrete and modern ideological movement?¹²¹ These are crucial issues for locating the Iraq War in the larger history of ideas and intellectuals in U.S. diplomatic history.

Iraq War Scholarship and U.S. Foreign Policy

The Iraq War’s long and costly nature has shaped discussions about what lessons it holds for U.S. foreign policy, but the competing interpretations of the war’s origins are also relevant for these debates. The majority of scholars in the security and hegemony schools agree that Iraq was a mistake, if not something worse. But they disagree on its consequences for U.S. foreign policy. Security-centric explanations of the war lend themselves to a less condemning portrayal of the Bush administration and the foreign policy establishment. Hal Brands and Peter Feaver refer to an “empathy defense,” arguing that “greater sensitivity to constraints, alternatives, and context can lead to a more favorable view of decisions taken in Afghanistan and Iraq following 9/11.” In this reading, Bush faced an unprecedented security threat after 9/11 and launched a mistaken war riddled with errors in intelligence, planning, and execution.¹²²

Those errors, however, do not mean that the United States needs to drastically rethink its position of global leadership.¹²³ Many conservatives, neoconservatives, and liberal internationalists have concluded that the lesson of Iraq is not to abandon an active and engaged global posture, but rather to eschew ambitious nation-building and democratization projects.¹²⁴ Brands argues that “the Iraq hangover” should not make U.S. leaders “strategically sluggish just as the dangers posed by great power rivals were growing.”¹²⁵ America’s defense of the liberal international order, they contend, has been overwhelmingly positive for U.S. interests as well as global democracy, prosperity, and peace.¹²⁶ The United States can continue to play this role while avoiding obvious mistakes like the Iraq invasion.¹²⁷ Nor does this war mean that the foreign policy establishment must be overthrown.¹²⁸

Still, this article suggests that even as the United States refocuses toward great-power competition, the meanings and lessons of the Iraq War remain hotly contested and highly consequential for America’s global role.

U.S. leaders seem to agree with this view of the lessons of Iraq, including those like President Barack Obama, who opposed the war originally. Obama, President Donald Trump, and Biden all criticized the Iraq War and have demonstrated skepticism toward nation-building interventions. Trump’s 2017 *National Security Strategy*, for example, states, “We are also realistic and understand that the American way of life cannot be imposed on others.”¹²⁹ Nonetheless, their national security strategies all affirm the



indispensability of engaged U.S. leadership and military primacy. For these scholars and leaders, the lesson of Iraq might be summed up as “Don’t do stupid shit,” as Obama once quipped. Instead, the country should carry on as the fulcrum of the liberal world order.¹³⁰ It should surprise no one that these figures prefer Leffler’s security-focused narrative of the Iraq War. Figures like Brands, Kagan, John Bolton, and Eric Edelman, Cheney’s deputy national security adviser, favorably blurbed or reviewed Leffler’s book, which does little to critique U.S. grand strategy.¹³¹ Bolton, a neoconservative architect of the war, praises Leffler for recognizing that “Bush was not eager for war ... his advisors did not lead him by the nose ... they were not obsessed with linking Saddam to 9/11,” and “their objectives did not include spreading democracy at the tip of a bayonet.”¹³² Brands, who has labelled the Iraq War a “debacle” and “tragedy,” nevertheless calls Leffler’s book “the most serious scholarly study of the war’s origins” for many of the same reasons as Bolton.¹³³ Scholars in the hegemony school could not disagree more about the Iraq War’s lessons. They contend that the war signals the bankruptcy of the overly ambitious and hyper-interventionist grand strategy of primacy. Primacy, as Wertheim argues, requires the United States to maintain U.S. forces around the globe and prevent the rise of great-power challengers, all while fueling a sense of messianic exceptionalism. He concludes that “the invasion of Iraq emerged from this logic,” and that, if the United States fails to fundamentally rethink its global role, it will rush headlong into more unnecessary conflicts.¹³⁴ For these critics, the Iraq War also demonstrated the myopia and conformism of the bipartisan policy establishment and its seeming addiction to an expansive global mission. This establishment, they argue, remains committed to a hegemonic role that has brought unnecessary wars, stunning human and monetary costs, balancing behavior by rivals, and the discrediting of U.S. leadership at home and abroad.¹³⁵ Deploying the Iraq War and other errors as a wedge, they aim to challenge the narrow, stultified conversation of the policy establishment and push U.S. grand strategy toward “realism and restraint,” in Walt’s words, while focusing more resources on preserving democracy and prosperity at home.¹³⁶

In sum, competing interpretations of the war’s origins are entwined with debates about its lessons. It is proper that scholars contest how this war should inform the future of U.S. foreign policy. Nonetheless, partisans in this debate risk filtering history through ideological prisms and using it to win arguments. Still, this article suggests that even as the United States refocuses toward great-power competition, the meanings and lessons of the Iraq War remain hotly contested and highly consequential for America’s global role. This is especially true as the generation that fought the Iraq and Afghanistan wars enters leadership positions in the military and politics. Their interpretations of that conflict will matter immensely for how they think and act, just as competing viewpoints about the Vietnam War mattered for that generation.

Cultural and Global Turns for the Iraq War

This paper’s core claim is that scholarship on the causes of the Iraq War can be usefully organized into security and hegemony schools. These categories simplify a wide range of analysis, but they also permit a bird’s eye look at the field 20 years after the war began. At this point, the hegemony school probably has more adherents among scholars of the war, although the war’s architects gravitate to the security school. The security-hegemony debate is not merely “academic.” It is a distinct interpretive divide that shapes how scholars approach their sources and leads to competing answers about other key questions. This divide also informs ongoing debates about U.S. foreign policy, with each school suggesting different lessons from the war. The polarization of the debate is real, but not ideal. Scholars should keep trying to synthesize these perspectives. Historians are particularly well suited for this task because they prioritize holistic, narrative, and multi-variable analysis rather than an insistence on parsimony and generalizability that is typically found among political scientists. One way to challenge the security-hegemony binary may be to adopt new methodological approaches to the Iraq War. The security-hegemony divide operates largely within traditional approaches to the study of war. Hahn describes these methods as focusing on “the exercise of power, the conduct of diplomacy, the practice of international politics, the interest in domestic politics and public opinion, and the application of military strength by U.S. government officials who calculated the national interests and formulated policies designed to achieve those interests.”¹³⁷

Many of these scholars have not consistently integrated cultural factors with the study of foreign policy or the causes of war.



New approaches could refresh this seemingly entrenched binary. The global turn in Cold War historiography, for example, broke up a debate focused on orthodox and revisionist accounts of the Cold War's roots. The conversation refocused itself on how the Cold War reshaped global history and intersected with trends like decolonization, as well as how the agency of smaller powers influenced the superpower struggle.¹³⁸ Some scholars have already advanced more global accounts of the Iraq War by digging into Iraqi sources, the role of the United Nations, and the regional politics of the Iraq conflict.¹³⁹ Until more sources are available on decision-making in the Bush administration, this may be a more productive route than further entrenchment in the security-hegemony divide. In addition, a cultural turn may be constructive for Iraq War scholarship. The cultural turn in diplomatic history led to more attention on how cultural factors like race, gender, religion, language, and memory shape policy and strategy.¹⁴⁰ Discussion of ideas and interests took a back seat to construction, imagination, narratives, symbols, and meaning in elite and popular culture.¹⁴¹ The transnational turn, moreover, highlighted the role of nonstate actors as important forces in the global arena. Scholars in this vein showed how a broader set of actors challenged the nation-state, formed networks, and exchanged ideas across borders, thus casting national politics in a global context.¹⁴² There has indeed been interesting work in history, anthropology, and post-colonial studies on the role of culture in the Iraq War and the "War on Terror." Andrew Preston and Lauren Turek examine how religion shaped Bush's worldview and foreign policy.¹⁴³ Melani McAlister and Deepa Kumar explore how media and popular culture portrayals of the Middle East helped justify the use of force there to domestic audiences.¹⁴⁴ Edward Said, Zachary Lockman, and others argue that the Iraq War should be understood in the context of Orientalist beliefs about supposedly backwards, dangerous Arabs and Muslims in need of the disciplining hand of Western rule.¹⁴⁵ Unfortunately, this work has often been stovepiped from the mainstream scholarship on the Iraq War's causes. Many of these scholars have not consistently integrated cultural factors with the study of foreign policy or the causes of war.¹⁴⁶ More traditional scholars, in turn, often overlook culture, race, gender, religion, and other factors. Students of the Iraq War and all of post-9/11 foreign policy should close these gaps by asking how culture interacts with and shapes policy, the perception of rivals, and decision-makers' understanding of themselves and America's role in the world.¹⁴⁷ There is considerable room for this kind of synthesis as scholarship of the Iraq War moves forward.

●► Endnotes are available at the source's URL.

Joseph Stieb is a historian and an assistant professor of national security affairs at the U.S. Naval War College. He is the author of *The Regime Change Consensus: Iraq in American Politics, 1990-2003* (Cambridge, 2021). He is working on a second book about Americans' interpretations of terrorism since the 1960s. He has published additional work in *Diplomatic History*, *Modern American History*, *The International History Review*, *War on the Rocks*, and other publications. **Acknowledgements:** I would like to thank Theo Milonopoulos and Brandon Wolfe-Hunnicut for suggestions about this article.

EDITOR'S COMMENT: Why did the US invade Iraq? Simply, because "*mine is bigger than yours*" ...

Crisis in Niger: West Africa at the cusp of a proxy war

By Ovigwe Eguegu

Source: <https://www.orfonline.org/expert-speak/crisis-in-niger-west-africa-at-the-cusp-of-a-proxy-war/>

Niger is quickly becoming a new flashpoint in great power competition as ECOWAS mulls military intervention in the wake of the coup in Niger

Last Wednesday, the world was greeted with the news of a military takeover in Niger. Expectedly, the Economic Community of West African States (ECOWAS) sanctioned and suspended Niger from the bloc. The grouping went further and threatened a [military intervention](#) if President Mohamed Bazoum is not reinstated within a week. Similarly, the United States (US), France, and the European Union (EU) wasted no time in condemning the coup. The reaction to the coup from within and outside the region is strongest compared to other recent coups, and the reasons are not far-fetched. Niger is a cornerstone of the Sahel Strategies of the US, France, and the European Union.



Exports of uranium from Niger are vital for French and European nuclear energy operations. So, it came as no surprise when France also [threatened](#) action against the Junta if they harm “French interests” in the country. While there is precedent for ECOWAS threat and use of military intervention, the equation changed when in solidarity with Niger, Burkina Faso and Mali released a joint statement condemning the possibility of military intervention, [stating](#) plainly that “all military intervention against Niger will be considered equivalent to a declaration of war against Burkina Faso and Mali”. This game-changing declaration means the use of force against the putschists in Niger would push West Africa into a conventional war, one that will quickly become a new flashpoint in great power competition with devastating consequences for the region.

Just as in Mali, Burkina Faso, and Guinea, the reasons Junta in Niger cited for their actions included chronic insecurity, poor economic conditions, and misrule.



Russia, France, and the wave of populist coups

The [overthrow](#) of President Mohamed Bazoum was the sixth successful coup in West Africa since 2020. General Abdourahamane Tiani who headed the presidential guard was later declared as head of state. On the surface, these coups are ambitious power grabs by disgruntled officers interrupting Africa’s democratisation process. Just as in Mali, Burkina Faso, and Guinea, the reasons Junta in Niger cited for their actions included chronic insecurity, poor economic conditions, and misrule. These reasons are not without merit. Maybe except for Guinea, there is a strong anti-neocolonial sentiment held by both citizens and the populations of these countries. Niger is one of the poorest countries in the world, and like Mali and Burkina Faso, is consistently at the bottom of the Human Development Index. Citizens of these countries blame neocolonial economic policies and structures for their economic woes, while experts blame the chronic underdevelopment in this region for the security challenges such as terrorism, human trafficking, and other security problems. [According](#) to the World Bank, Niger has been faced with an influx of displaced persons from Nigeria and Mali, and as of 2022, there were almost 295,000 refugees with roughly 350,000 displaced persons overall in the country. As of 2021, studies [suggest](#) that over 41.8 percent of Niger’s population is living in extreme poverty, and while there was a GDP growth of 1.4 percent in 2021, projections show that new economic programs are expected to boost GDP per-capita by 15 percent in the next year. Furthermore, irrigation programmes and a good rainy season [increased](#) agricultural production by 27 percent, a big boost considering agriculture alone accounts for 40 percent of the country’s GDP.

Niger has been faced with an influx of displaced persons from Nigeria and Mali, and as of 2022, there were almost 295,000 refugees with roughly 350,000 displaced persons overall in the country.

France has led regional security efforts for most of the last decade. Aside from setting up the G5-Sahel Force, Paris deployed over 5,000 troops under Operation Barkhane, the UN’s MINUSMA had a 15,000-troop presence while the EU had special forces deployed under Operation Takuba. Under these security



programmes, terrorism and violence in the region only increased. When Ibrahim Traore ceased power in Burkina Faso in September 2022, [40 percent](#) of the country's territory had come under the control of jihadists leading France and its European allies to lose credibility as security providers in the region.

UN and French-led security programs have often failed with mainstream media often downplaying this while simultaneously exaggerating Russia's growing influence in the region. While there is evidence of Russian actors [exploiting](#) anti-western sentiments, these exist because of poor governance, foreign meddling, and developmental challenges. Military cooperation between Mali and France has also deteriorated since the coup. In April last year, Mali [expelled](#) French troops ending Operation Barkhane after nine years of operations. In January 2023, Burkina Faso [ended](#) a 2018 military agreement with France and demanded the expulsion of French forces operating in the country. In both instances, the expulsion of French forces was [celebrated](#) by citizens who are often seen waving Russian flags alongside their own national flags.

UN and French-led security programs have often failed with mainstream media often downplaying this while simultaneously exaggerating Russia's growing influence in the region.

The coups in Mali and Burkina Faso saw Niger becoming one of the main partners of France, the US, and the EU in the region. French and EU personnel were redeployed from Mali and Burkina Faso to Niger, which is also home to a French base and [at least](#) two US airbases making it the main platform for France, AFRICOM, and the EU operations in the region. This is a security arrangement that the recent coup is going to disrupt. The Junta has [revoked](#) two military cooperation agreements with France, one dating back to 1977 and the second was signed in 2020. Niger holds more importance to France and Europe beyond security in West Africa. For perspective, over 50 percent of Nigerien uranium ore [goes](#) to France's nuclear energy system, and 24 percent of uranium imports to the EU come from Niger. With the threat of a military leadership pivoting from France, Paris and Western allies are sure to deliberate action and support any means to restore Bazoum, thereby securing their access to key energy resources for Europe.

ECOWAS mulls intervention

While plans of intervention are been discussed by ECOWAS officials in Abuja, Nigeria, a delegation of officials [arrived](#) in Niamey on 3 August as part of mediation efforts. However, the delegation did not spend the night as planned, nor did it meet with coup leader Abdourahamane Tiani or deposed President Mohamed Bazoum; a sign that talks did not go as planned. On that same Thursday, Senegal [confirmed](#) its troops will join any ECOWAS intervention in Niger. While the Niger's Junta [said](#): "any aggression or attempted aggression against the Niger will see an immediate and unannounced response from the Niger Defence and Security Forces on one of (the bloc's) members, with the exception of suspended friendly countries."

An ECOWAS military intervention is the worst thing that could take place in the region considering the existing security conditions. While Nigeria may contribute the highest number of troops to an ECOWAS military outfit, the country is [not](#) in a condition to conduct a war involving multiple countries. Furthermore, mass displacement and high mortality and migration will surely follow. With numerous internal challenges, economic, developmental, and humanitarian, facing the Sahel region, triggering a conflict between weak and fragile states amounts to self-destruction.

A better approach is for ECOWAS to enact deeper sanctions while doubling down on a diplomatic solution. In addition to the termination of existing financial aid packages, Niger could be on the receiving end of heavier sanctions that could be targeted towards financial ecosystems, transport, or other critical economic sectors. ECOWAS countries have enormous leverage vis-à-vis Niger. For Instance, Nigeria [supplies](#) 70 percent of Niger's electricity, and taken together Senegal and Cote Ivoire supply 40 percent of Niger's refined petroleum. Commitments will also be tested under a sanctions-heavy environment. However, it is important to factor in the will of the Nigerien people, some of whom have expressed vocal support for the junta.

With numerous internal challenges, economic, developmental, and humanitarian, facing the Sahel region, triggering a conflict between weak and fragile states amounts to self-destruction.

In all, the coup in Niger is one coup too many for the region, but with regional security and geopolitical dynamics, it important to access the rationale of an ECOWAS military intervention. On a wider geopolitical front, multipolarity and elements of alignment and non-alignment are emerging faster than ever, and traditional relations are being tested, terminated, or renegotiated. The so-called great power competition is in full swing and African countries are moving away from being passive, occupying a proactive role whether or not it follows an 'established decorum'.

One week after the coup, the Junta is making attempts to consolidate its grip on power. It has [announced](#) the reopening of borders with five neighbours, appointed new governors to the countries five regions, and says the country is on a transition towards democracy. However, no timelines were given. This should be seen from a pragmatists lens as well considering the plausibility of an outright economic collapse. With these developments, it must



be noted that military conflict will only affect vulnerable populations and further destabilise the region. An outcome that Africans do not wish for.

Ovigwe Eguegu is a Policy Analyst at Development Reimagined. He focuses on geopolitics with particular reference to Africa in a changing global order.

Niger, an impoverished country whose rich uranium and gold deposits are exploited by Westerners (only 5% goes back into the local economy), has experienced a population boom in the last 15 years, with its population soaring from 12 million to 25 million. Despite the extremely low average life expectancy due to hunger and lack of medical facilities that barely reach 60 years. Wagner will undertake the protection of the Presidential Palace and the main infrastructures of the country threatened by Nigeria. The US maintains a large base of reconnaissance drones operating across Africa, Europe, and the Middle East, as well as about 500 troops. The French maintain about 1200 soldiers. At the moment there are about 5,000 Russian-paid volunteers in Africa: They are active mainly in Mali, Libya, Sudan, Central African Republic, Mozambique, and the Democratic Republic of Congo.

Unity in Adversity

Immigration, Minorities and Religion in Europe

Edited by Vít Novotný



EDITOR'S COMMENT: Integration is not difficult to be achieved provided that newcomers are willing to work, learn the language, respect the ethics and culture of the hosting country, avoid extraordinary religious behaviors, and respect the law and order of their new second home country. If not, they are not welcome! Until now, in Greece, these prerequisites are not fulfilled; instead, they start with the attitude "We will illegally cross your land or sea borders whether you like it or not and we will settle in your country whether you like it or not!" They enjoy the generously given benefits; the majority is not working mainly because they do not have the skill even for the agriculture field; they give birth to countless children that they barely can support; they treat women of all ages as not human beings; they form gangs and conquer districts where they implement their laws. Do you think that this is the appropriate behavior to make them welcome by locals? To integrate with them? To bond with them? I do not think so – end of story.

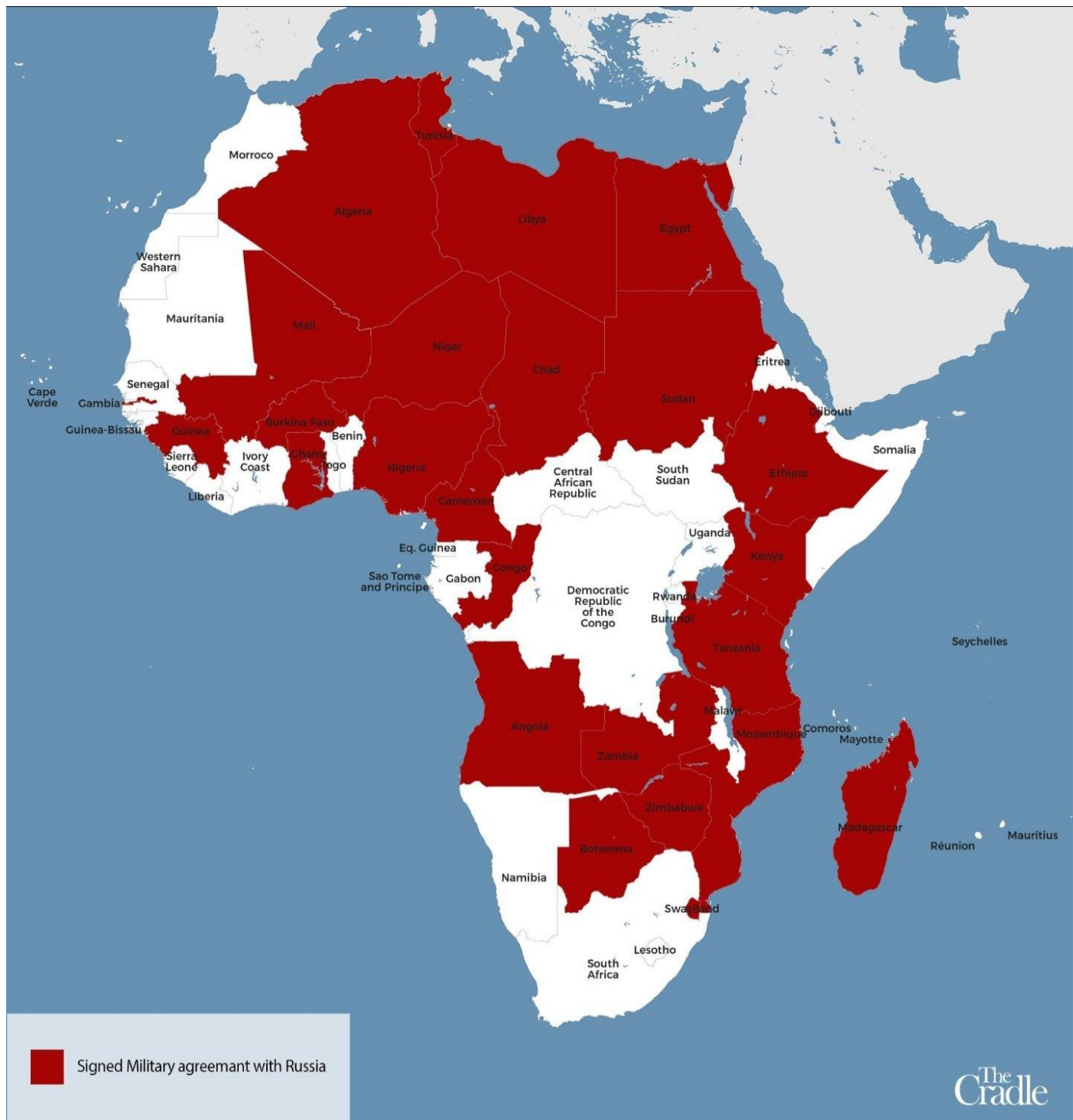
This problem with illegal immigration is nothing new. In fact, the Indians had a special name for it. They called it "white people."

— Jay Leno —



Geostrategic games in Africa

Source: <https://twitter.com/ricwe123/status/1688473848507686913>



Why is it that more and more African countries are willing to sign a military agreement with Russia? Could it be they are fed up with the dictates coming from the western world?

EDITOR'S COMMENT: Maybe it is because big Western powers do not read history and do not learn from the problems identified!



Greece – A country without borders



Aug08 – Myrtoan Sea (off-shore Peloponnese)



Jul02 – Tsambika Beach, Rhodes Island – debarkation in an organized beach



Le Monde

honte à vous d'ignorer
l'histoire!

La mer Egée était,
est et sera toujours
grecque !

Partez à la découverte de
nouvelles sensations à
~~Turkeyegean~~

PUBLICITÉ



**Ukrainian
proxy
war**

**The most
immoral
war**

EVER!

Scandinavia Prepares to Submit to Blasphemy Bullying

By Soren Kern

Source: <https://www.meforum.org/64664/scandinavia-prepares-to-submit-to-blasphemy>

Aug 07 – Denmark and Sweden, under growing pressure from Muslim countries, are contemplating free speech restrictions that would outlaw burning copies of the Quran. Recent Quran-burnings by anti-Islam activists in Copenhagen and Stockholm have sparked angry protests in several Muslim countries and increased the terrorist threat against the two Scandinavian countries.



The threats have fueled a debate about balancing free speech and security, but some observers are [warning](#) that changing free speech laws in the middle of a security crisis would be "giving in to blackmail." The editorial board of *Expressen*, one of Sweden's oldest newspapers, [noted](#) that doing so "would in practice mean that foreign actors are given power over which opinions are allowed in Sweden."

On July 31, the foreign ministers of the fifty-seven member states of the Organization of Islamic Cooperation (OIC) — a Saudi Arabia-based group that has long [called](#) for an international blasphemy law that would not only guarantee special protections for Islam, but also shield it from legitimate scrutiny and criticism — [convened](#) an "extraordinary session" to discuss responses to the Quran burnings. In a [statement](#), the OIC expressed anger at Denmark and Sweden

for failing to outlaw "the repetition of such acts of aggression" that "spread hatred and contempt for religions and threaten global peace, security and harmony." The OIC also called for an international law aimed at "criminalizing incitement to violence based on religion or belief," and demanded that the European Union "clarify the gravity and consequences of persisting in insulting Islamic symbols and sanctities." On July 12, the United Nations Human Rights Council (HRC) [approved](#) an OIC-sponsored resolution — "Countering Religious Hatred Constituting Incitement to Discrimination, Hostility or Violence" — that seeks to outlaw "public and premeditated acts of desecration of the Holy Qur'an." The resolution, which passed with a vote of twenty-eight in favor, twelve against, and seven abstentions, was opposed by the United States and the European Union on free speech grounds.

The OIC has long [pressed](#) the European Union and the United States to impose limits on free speech and expression about Islam. It recently has redoubled efforts to persuade Western democracies to implement HRC Resolution 16/18, which [calls](#) on all countries to combat "intolerance, negative stereotyping and stigmatization" of "religion and belief." Resolution 16/18, which was [adopted](#) at HRC headquarters in Geneva in March 2011, is widely [viewed](#) as the cornerstone of OIC efforts to advance the international legal concept of "defaming Islam." International human rights law as currently constituted protects individuals, not religions. The OIC effectively is seeking a paradigm shift to the existing international legal order that would make criticizing Islam a violation of human rights — at the expense of free speech. Denmark and Sweden, known for their storied [traditions](#) of constitutionally-protected free speech, have long been on the radar of Islamists. In September 2005, the Danish newspaper *Jyllands-Posten* published twelve editorial cartoons, some of which depicted Mohammad, the prophet of Islam. This sparked deadly riots across the Muslim world. As the *Middle East Quarterly* [noted](#) at the time, the cartoon controversy "had less to do with genuine outrage over the depiction of Islam's prophet and more to do with the ambitions, first, of a small group of radical imams, and, later, of jousting Middle Eastern powers." In Sweden, a Quran-burning rally in Stockholm in January 2023 [enraged](#) the Turkish government and jeopardized Sweden's bid to join the North Atlantic Treaty Organization (NATO). Turkish President Recep Tayyip Erdoğan [warned](#) that "as long as you allow my holy book, the Quran, to be burned and torn, we will not say 'yes' to your entry into NATO." That threat was widely interpreted as a demand that Sweden enact a new blasphemy law as a condition for NATO membership.

On February 8, in a reversal of long-standing policy, the Swedish government [refused](#) to allow anti-Islam activists to burn a Quran in front of the Turkish embassy in Stockholm. They subsequently prohibited a Quran burning rally that was planned for February 20 in front of the Iraqi embassy in the Swedish capital. On June 12, the Swedish Court of Appeals [ruled](#) that those bans were unconstitutional. Since then, [two Iraqi immigrants](#) — thirty-seven-year-old Salwan Momika, who arrived in Sweden from Iraq in 2018 and received a three-year residence permit in April 2021, and forty-eight-year-old Salwan Najem, who migrated to Sweden from Iraq in 1998 and became a Swedish citizen in June 2005 — have repeatedly desecrated the Islamic holy book.

On June 28, Momika [burned](#) a Quran outside Stockholm's Central Mosque. On July 20, Momika and Najem [stomped](#) on a Quran outside the Iraqi Embassy in Stockholm and on July 31, they [burned](#) a Quran



in front of the Swedish Parliament. The desecrations [provoked](#) widespread anger across the Muslim world, including from Erdoğan, who [vowed](#) to "teach the arrogant Western people that it is not freedom of expression to insult the sacred values of Muslims." Some analysts say Erdoğan, whose longstanding [goal](#) has been to criminalize criticism of Islam in Europe, is seizing on the Quran burnings and other "Islamophobia" [controversies](#) to extract concessions from Sweden and other European countries. Abdullah Bozkurt, an exiled Turkish journalist who lives in Sweden, told FWI that Erdoğan is seeking to "exert pressure on Western countries" and "strengthen his bargaining power" to crack down on his political opponents in Europe and to "undermine their well-founded criticisms of Türkiye on massive human rights violations." The Swedish Security Service (*Säkerhetspolisen*, *Säpo*) [warned](#) that Quran burnings and the subsequent protests in the Muslim world have resulted in a "worsening of the security situation." Säpo's deputy head of counter-terrorism, Susanna Trehörning, [told](#) SVT public television that there are "influential people who are now sending out very clear narratives about Sweden and also calls for revenge." She added that the "threat from people within the violent Islamist environment" was "very high." Swedish Prime Minister Ulf Kristersson [warned](#) that his country is facing its "most serious security challenge since World War II." Swedish Foreign Minister Tobias Billström, in a letter to the OIC, [noted](#) that although the government denounces the Quran burnings, freedom of expression is guaranteed by the constitution. Swedish Justice Minister Gunnar Strömmer [announced](#) that the government was considering possible changes to the Public Order Act but that there is no "quick fix" to stop the Quran burnings. Meanwhile, Sweden's Immigration Agency [said](#) that it was reviewing Momika's residency permit, which expires in 2024. On July 30, the Danish government issued a [statement](#) saying that it was exploring "the possibility of intervening in special situations where, for instance, other countries, cultures, and religions are being insulted, and where this could have significant negative consequences for Denmark, not least with regard to security." It added that "this must of course be done within the framework of the constitutionally protected freedom of expression and in a manner that does not change the fact that freedom of expression in Denmark has very broad scope." A July 6 opinion poll commissioned by SVT television [found](#) that 53 percent of Swedes favored a ban on Quran burnings, while 47 percent were opposed or unsure. This compares to a similar poll commissioned by TV4 Nyheterna in February which [showed](#) that 42 percent were in favor of such a ban while 67 percent were opposed or unsure. The editorial board of the Swedish newspaper *Dagens Nyheter* [warned](#) that Islamists "will not be content with a blasphemy law because they will always want to go one step further." The editorial board of the Swedish newspaper *Expressen* [agreed](#) that the Islamists pressuring Sweden are "unlikely to be content" with a ban on Quran burnings. "The risk is obvious that small Swedish concessions in this situation would only lead to new demands for submission." Sofie Löwenmark, a Swedish journalist who covers Islamism, [said](#) that calls for a ban on Quran burnings are a smokescreen to hide the larger objective: a ban on legitimate criticism of Islam.

Soeren Kern is a Middle East Forum Writing Fellow.

Supporting the right side of History



Aug 09 – A provocative photo with mortar shells has been making the rounds on the internet in the last few hours where, like communicating vessels, neo-Nazi fans of Dinamo Kyiv are supporting the neo-Nazi hooligans (BBB) of Dinamo Zagreb who brutalized the 29-year-old Michalis Katsouri fan of AEK FC in the bloody clash in New Philadelphia.



Proxy War #2 – coming soon ...



The recent developments on the African continent will lead to three major changes in the political, military and economic spheres in the region. In the political sphere, a new coalition of strongly anti-Western countries will emerge in Africa, paving the way for existing or new anti-Western movements in the future. In the military field, which complements the political one, the liberation of Niger will lead to the creation of a new military coalition against the West and possibly the fall of dominoes of Western bases in the Sahel region and of course the loss of hegemony for the Western bloc. This will cut off the West from the Sahel's valuable resources. The consequences of the war will be significant for the economy of the West with the European Union suffering the most.

Mordechai Kedar: What Will Israel's Next War Look Like?

By Marilyn Stern

Source: <https://www.meforum.org/64675/mordechai-keidar-what-will-israel-next-war-will>

Aug 07 – Mordechai Kedar, lecturer at [Bar-Ilan University](#) and vice president of the Israeli news site, [Newsrael](#), spoke to an August 7th Middle East Forum Webinar ([video](#)) about his threat assessment of the next Middle East war against Israel. The following is a summary of his comments:

Pronouncements by many in Israel's military that they will refuse to serve in protest of the government's judicial reforms have weakened the Jewish state's invincible image. In the Middle East, "if you are powerful, people will respect you. If you are weak, you're doomed." Iran, its Islamic Revolutionary Guard Corps (IRGC) in Syria, and its proxy Hezbollah in Lebanon, all smell blood while watching Israel's internal dissent, thinking the nation is "easy prey." This is why Israeli media is openly discussing "worst-case scenarios" if its enemies take this as an opportunity to orchestrate a multi-front offensive to eliminate it.

Israel has a history of multi-front assaults by its enemies, borne out during the 1948 Independence War, the Six-Day War in 1967, the War of Attrition in 1969-70, and the Yom Kippur War in 1973. Today, Iran's efforts to connect Lebanon and Hezbollah, Syria, Iraq, Yemen, and Hamas in Gaza in a multi-pronged attack on Israel constitute the first characteristic of a worst-case scenario: internal strife. Exacerbating the external threat is the possibility of a repeat of the riots that erupted within Israel in May 2021, when Arab Israelis, who comprise 20 percent





of the population, killed some Jews and destroyed synagogues before the violent outbreak was contained. The second likely characteristic of the next war will be Hezbollah's launching of up to 150,000 missiles against Israel's gas extraction and storage facilities, other infrastructure, air bases, ships at sea, and its cities. Such an attack would lead to the third characteristic of the next war, in which Hezbollah targets expand beyond military sites and public infrastructure. Thus, Hezbollah and IRGC militias in Syria, Iraq, Yemen, and Hamas will deliberately rain down missiles and drones on Israeli civilians and inflict as many casualties as possible to demoralize the population. Israel is psychologically preparing itself for the Arabic doctrine of "resistance," or the persistent state of jihad called *muqawama*. As non-state actors, these militias are not considered states and would therefore

not hesitate to commit total war in violation of the Geneva Conventions, which requires states to act in accordance with international law. One need only look at the ongoing war between Ukraine and Russia for the real-time battlefield effects of drone and missile strikes, the devastating effects of which illustrate such a worst-case scenario. Such destruction encourages Iran in its jihad against the Jewish state because, as war rages in Ukraine, the free world goes about its business. This signals to the Iranian regime that if it attacks Israel with the same "vicious" abandon that Russia attacks Ukraine, "the world will not take it so seriously."

The prospect of Israeli-Saudi normalization would not deter the Iranian threat because Saudi Arabia is militarily weak, as evidenced by its failure in its war against the Houthi militia in Yemen. While Israel welcomes "mutual recognition" with the Saudis, the price the Saudis will demand from Israel to appease the Palestinians may be too high. Although the U.S. administration has abandoned the idea of disabusing Iran of its nuclear ambitions, Israel will pursue its national interest in preventing Iran from acquiring nuclear weapons. Iran, a state actor committed to Israel's destruction, props up its non-state proxies, which would have no "backbone" without the Islamic regime's support. There is an idea that "Israel should concentrate on how to bring Iran to its knees . . . to devastate the military power of Iran." Such a strategy would represent an effort to cut off the "head of the octopus rather than fighting with its tentacles." "This has its logic." Still, the problem of reaching distant Iran remains logistically challenging because it requires crossing "states between Israel and Iran [that] are not so friendly."

If war breaks out and a decision is reached to eliminate the Iranian threat, the Israelis will put "all the[ir] differences . . . aside." Israel is a small country that fights "with our back to the sea." If Israelis see Iran's threats as a real danger, "Israel will return to its unity," because even those demonstrating against the government believe in the survival of the state. The Israeli soldiers protesting in the streets of Israel will "run to their units" since they know that "the first war which Israel loses . . . will also be its last war." There is no other option than to be "victorious again, and if needed, again and again and again."

Marilyn Stern is communications coordinator at the Middle East Forum.

Who is fighting on the Ukraine war front?



Dynamo Kiev – a country at war ...



Join the right side of History!

V. ZELENSKY

IS ONE OF 39 MILLION OF UKRAINIANS WHO NEVER SERVED OR HELP A SINGLE AMERICAN BIDEN ADMIN SENT HIS COUNTRY \$200 BILLION OF AMERICAN TAXPAYERS \$ & PLEDGED TO SEND MORE AS LONG AS IT TAKES

NICOLE GEE

WAS ONE OF 13 SERVICE MEMBERS WHO DIED IN A SUICIDE BLAST AT KABUL AIRPORT IN 2021. BIDEN ADMIN FORCED HER FAMILY TO PAY \$60,000 TO TRANSPORT HER BODY TO ARLINGTON NATIONAL CEMETERY



How Reliable and Robust Is Human Ability to Recognize Suspicious Activity?

Source: <https://www.homelandsecuritynewswire.com/dr20230815-how-reliable-and-robust-is-human-ability-to-recognize-suspicious-activity>

Aug 15 – Security procedures at large public venues and transportation hubs rely upon vigilant and engaged security officers who are tasked, in part, with timely and appropriate responses to suspicious behavior of potential hostile actors. The presumption is that hostile actors, armed with the “guilty knowledge” of their true intention, will behave in non-normative ways distinct enough from the behavior of normal site users, thus providing opportunities for security authorities to detect this suspicious behavior. But how capable are individuals at detecting suspicious behavior?

[CREST Research](#) released a [new report](#) which offers a systematic review of the current evidence base for the human ability to accurately recognize suspicious behavior.

Here are the report’s Executive Summary, Introduction, and Conclusions:

Executive Summary

- 7033 unique studies were sifted to identify studies that examined the human ability to recognize suspicious behavior.
- 11 studies met the inclusion criteria.
- Seven studies looked at the difference in ability between experienced CCTV operators and controls; two looked at the influence of context; one on the influence of stressors; and one on the influence of training.
- No significant differences were found between experts and novices. Accuracy appears to be around chance level.
- Familiarity with an area may have a positive effect on detecting suspicious behavior.
- Participants exposed to security cues while carrying out tasks were more often correctly identified by observers as either innocent or hostile based on their behavior.
- Behavior based training may increase an individual’s ability to recognize suspicious behavior.
- Individuals differ in cognitive and perceptual skills and therefore infer different meanings from viewed behavior. These differences in the interpretation of cues may affect the ability to accurately detect suspicious behavior.
- Cues of hostile intent may be difficult to interpret accurately due to the observer’s absence of the perpetrator’s baseline ‘normal’ behavior with which to compare.
- Establishing non-verbal indicators of hostile intent that are accurate across many contexts is difficult. Observers need knowledge of ‘normal’ behavior for each specific location.

Introduction

Security procedures at large public venues and transportation hubs rely upon vigilant and engaged security officers who are tasked, in part, with timely and appropriate responses to suspicious behaviors (behavior that seem unusual or out of place, that indicates that someone is in the process of planning or committing a malicious act) of potential hostiles (be they criminals, or terrorists) looking to victimize normal site users. This includes individuals conducting hostile reconnaissance, defined as “purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target” (CPNI, 2016).

The presumption is that hostiles, armed with the ‘guilty knowledge’ of their true intention will behave or present in non-normative ways versus normal site users and thus provide opportunities for security to detect these suspicious behaviors (Gill et al., 2020). But how capable are individuals at detecting suspicious behavior? This systematic review assesses the current evidence base for the human ability to accurately recognize suspicious behavior.

The evidence for a narrower form of deception – lie detection – paints an interesting picture. In terms of lie detection, Bond and DePaulo’s (2006) meta-analysis found that just 54% of untrained observer judgments were correct, only slightly higher than chance. Performance was worse when observers could only see the target person (52% accuracy), than when they could only hear them (63%). However, liars are more nervous and more conscious of their own behavior than truth tellers (Vrij, 2008; Vrij et al, 2019) and when being interviewed are aware that they are being actively observed and scrutinized. Those with hostile intent may not believe that they are being watched, but they may be vulnerable to the spotlight effect – a tendency to believe they are being noticed more than they are and as such overestimate the extent to which they are the focus of the attention of others (Gilovich et al, 2000).

Conclusions

Individuals differ in cognitive and perceptual skills and therefore infer different meanings from



viewed behavior. These differences in the interpretation of cues may affect the ability to accurately detect suspicious behavior. Observers of the environment need knowledge of behaviors linked to hostile intent, however establishing non-verbal indicators of hostile intent that are accurate across many contexts is difficult. Cues of intent may not be expressed in cases where the crime is expressive or spontaneous. Where they are apparent, they may be difficult to interpret accurately due to the observer's absence of the perpetrators baseline 'normal' behavior with which to compare. As these behaviors may deviate from situationally appropriate conduct observers also need knowledge of 'normal' behavior for that specific location.

Of course, offenders can deliberately modify their behavior to conceal intent. There may be overlap between normal and suspicious behavior in the same situation. As well as difficulties in establishing a universal baseline of behavior that is applicable in every context, problems also arise in keeping natural guardians vigilant. Tasking members of the public to perceive a scene as a whole, and then try to detect clusters of behavior that differ from the baseline is not feasible. Security system operators may not have an increased ability to identify suspicious behaviors except for when they have an understanding of the norms of the given environment. Little is known about the strategies observers of CCTV use when monitoring and interpreting behavior.

References

- Blechko, A., Darker, I., & Gale, A. (2008). Skills in detecting gun carrying from CCTV. In *2008 42nd Annual IEEE International Carnahan Conference on Security Technology* (265-271). IEEE.
- Blechko, A., Darker, I. T., & Gale, A. G. (2009). The role of emotion recognition from non-verbal behavior in detection of concealed firearm carrying. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 53, No. 18, pp. 1363-1367). Sage CA: Los Angeles, CA: SAGE Publications.
- Cooke N.J., & Winner J.L. (2008) Human factors of homeland security. In: Boehm-Davis DA (ed) *Reviews of human-factors and ergonomics* (3). Human Factors and Ergonomics Society, Santa Monica, CA, pp 79–110
- Crundall, D., & Eyre-Jackson, L. (2017). Predicting criminal incidents on the basis of non-verbal behavior: The role of experience. *Security Journal*, 30(3), 703-716.
- Graham, G., Sauer, J. D., Akehurst, L., Smith, J., & Hillstrom, A. P. (2018). CCTV observation: the effects of event type and instructions on fixation behavior in an applied change blindness task. *Applied cognitive psychology*, 32(1), 4-13.
- Grant, D., & Williams, D. (2011). The importance of perceiving social contexts when predicting crime and antisocial behavior in CCTV images. *Legal and Criminological Psychology*, 16(2), 307-322.
- Koller, C. I., Wetter, O. E., & Hofer, F. (2016). 'Who's the Thief?' The Influence of knowledge and experience on early detection of criminal intentions. *Applied Cognitive Psychology*, 30(2), 178-187.
- Mann, S., Deeb, H., Vrij, A., Hope, L., & Pontigia, L. (2020). Detecting smugglers: Identifying strategies and behaviors in individuals in possession of illicit objects. *Applied Cognitive Psychology*, 34(2), 372-386.
- Regens, J. L., Mould, N., Jensen III, C. J., Edger, D. N., Cid, D., & Graves, M. (2017). Effect of intelligence collection training on suspicious activity recognition by front line police officers. *Security Journal*, 30(3), 951-962.
- Troscianko, T., Holmes, A., Stillman, J., Mirmehdi, M., Wright, D., & Wilson, A. (2004). What happens next? The predictability of natural behavior viewed through CCTV cameras. *Perception*, 33(1), 87-101.
- Wijn, R., van den Berg, H., & Lousberg, M. (2013). On operator effectiveness: the role of expertise and familiarity of environment on the detection of deviant behaviour. *Personal and ubiquitous computing*, 17(1), 35-42.
- Wijn, R., van der Kleij, R., Kallen, V., Stekkinger, M., & de Vries, P. (2017). Telling friend from foe: Environmental cues improve detection accuracy of individuals with hostile intentions. *Legal and criminological psychology*, 22(2), 378-399.
- Zhang, K., Frumkin, L. A., Stedmon, A., & Lawson, G. (2013). Deception in context: coding nonverbal cues, situational variables and risk of detection. *Journal of Police and Criminal Psychology*, 28(2), 150-161.

Kosovo, Turkey And Ukraine: A Human Organ Trafficking Network?

By Piero Messina

Source: <https://www.argumentum.al/en/italian-media-reports-rama-meloni-discussed-the-construction-of-a-nuclear-power-plant-in-albania/>

Aug 14 – The investigation of a Turkish whistleblower may have revealed the worst face of the conflict between Russia and Ukraine (if there is an acceptable face to conflicts). Against the background of the armed conflict,



a network of traffickers in human organs would have arisen. That network would be the replay of operating methods already applied at the beginning of the century in Kosovo, during the conflict that led to the dismemberment of Yugoslavia. The reconstruction provided by the Turkish media speaks of a network of traffickers, managed by Ukrainian businessmen residing in Italy. The crime network was allegedly set up with the support of the Ukrainian administration. The channel would serve to supply human organs to the Turkish private health system, at lower prices than the European black market.

The author of *UkraineHumanRightsAbuses* believes that the agreement successfully coincided with the counteroffensive, which leads to the mass death of Ukrainian militants. This will allow organs to be sold abroad without the consent of their relatives.

Shortly before the special operation in December 2021, the Verkhovna Rada of Ukraine adopted a law allowing the removal of organs from the dead without notarized consent from them or their official representatives. The term “official” is vague – it can be a person who takes responsibility for the funeral. In military conditions, it may be the commander of the unit.

And given that such a product is in demand and brings a lot of money, this will become one of the sources of illegal enrichment. This practice has been known around the world, as well as the fact that Ukraine has been a source, transit and destination country for human trafficking since the early 1990s.

The Russian government also confirms this hypothesis. Russia has information that the leaders of the former UCK are involved in trafficking in human organs. The news was reported by “Rasijskav Gazeta”, in an article signed by Maria Zakharova, the spokeswoman for the Russian Foreign Ministry: “The UCK still works, but with a different name, and there is a possibility that it is present in Ukraine as a mercenary organization,” Zakharova said.

The central role of Kosovo in these criminal networks is a story well known by the international community. The first to speak of organ trade was Carla Del Ponte, magistrate of the ICTY from 1999 to 2007.

Until 2008, according to the prosecution’s thesis, Kosovo was at the center of an international network of trading in human organs. The trial was held in the Court of Pristina, before the EULEX court. Precisely Pristina was the epicenter of the crime. In the Medicus Clinic, in theory only a cardiological structure opened in 2000, there would have been a continuous coming and going of doctors, donors and patients from all over the world. The “victims” are at least thirty. Nine defendants. Donors and recipients were summoned by the organization’s intermediaries to Istanbul, a link between East and West and one of the world capitals of international organ trade since the end of the 1990s.

Albanian chain of organ trafficking in self - proclaimed Kosovo

Hashim Thaçi was the head of a Drenica group responsible for smuggling weapons drugs and human organs.

Ramush Haradinaj is the person most responsible of organ trafficking in Kosovo along side of Hashim Thaçi.

Dr. Yusuf Sonmez aka dr. Vulture was chief surgeon and one of the leaders of the criminal group which dealt with illegal kidney transplants. He was closely linked with Thaçi's group.

Shaip Muja is a surgeon and a health adviser of Hashim Thaçi. He is one of the leading co-conspirators in Thaçi's organized crime network and organ trafficking.

(Enlarge the page to read details)



Albanian Prime Minister Edi Rama is trying to defend Kosovo. The politician called for the withdrawal of a controversial report claiming the involvement of Albanians and Kosovars in organ trafficking at the end of the war between Kosovo and Serbia:

"I cannot stand still at this summit because the injustice towards the KLA and of its former leader Hashim Thaçi started right here, under the malevolent influence of its former member at the time, the Russian Federation".

The fault, therefore, as always lies with Russia. However, to deny Edi Rama's words, it is enough to read the extensive documentation collected, the evidence and testimonies, of the trial against the Kosovar doctors sentenced in the first and second instance by the European courts. Twenty years after the massacres of the former Yugoslav war, a definitive judgment is still awaited for those crimes against humanity. The usual wall of silence will be raised about what is happening in Ukraine today.

EDITOR'S COMMENT: Perhaps Albania is missing from the equation.

Rumors say that the starting tariff is 5,000 euros – via Darknet. According to the ad, the seller is asking for 5 thousand euros for an organ and specifically 25 thousand euros for the timely delivery of a heart and 12 thousand euros for a kidney.

Human organs are sold exclusively in the EU in a special medical refrigerator for 48 to 60 hours.

The package can be picked up at the agreed location after full prepayment or delivered in person after a 35% down payment of the purchase price.

Islamists Taking New Approach to Qur'an Burnings

By Dexter Van Zile

Source: <https://www.meforum.org/64696/islamists-taking-new-approach-to-quran-burnings>

Aug 15 – Europe is witnessing the all too predictable expressions of outrage and appeasement in the aftermath of Qur'an burnings in Sweden and Denmark, but astonishingly enough, new voices are emerging. Prominent Islamists in the West are telling their followers not to give Qur'an burners in Scandinavia what they want: proof that Muslims cannot live peaceably with non-Muslims and abide by the Western principle of free speech.

"We know the response they want," [said](#) Sheik Younus Kathrada during a July 9, 2023, sermon at Muslim Youth Victoria in British Columbia. "Don't give into them! They want us to look like fools parading in the streets, demonstrations, blah, blah, blah, and nothing happens."

by the United Nations Human Rights Council, all served to incite protests in Middle East, South Asia, Europe and North America. The recent round of blasphemy bullying began on June 29, 2023, the day after an Iraqi immigrant [burned](#) Qur'ans outside of a mosque in Stockholm, Sweden, and two protesters [did](#) the same thing in front of the Turkish embassy in Copenhagen, Denmark. A resolution condemning the Qur'an burning as "a violation of international human rights law" was [passed](#) by the United Nations Human Rights Council on July 7, 2023, all served to incite protests in Middle East, South Asia, Europe and North America.

The leaders of Stockholm Mosque, where one of the burnings took place, equated the act of protest by a few activists with government-led book burnings led by the Nazis in Germany prior to World War II and the burning of Jewish texts in Catholic-ruled countries in the Middle Ages. "Islamophobia in society is being normalised to a greater extent and every day the religious freedom for Swedish Muslims is shrinking," the mosque [declared](#) in a June 29 statement published by the UK Islamist publication 5Pillars.





Sheikh Kathrada in British Columbia took a different approach. Declaring that Qur'an burnings are a terrible insult to Muslims, their faith, and the God they worship, he said that responding with violent protests and angry rallies does nothing to stop them. Moreover, the real insult to God, he argued, is the failure of Muslims in his community to memorize the Qur'an and adhere to its teachings.

"In reality, what we should be doing is demonstrating against *you*," he said. "We should be holding rallies against *you*." Later, he stated, "We should be protesting against ourselves." Outside observers should not think that Kathrada, a well-known Islamist who has [declared](#) non-Muslims

as the enemies of the *umma*, has gone completely soft in his contempt for the kaffirs. In his July 9 sermon, he condemned his congregants who do not pay *zakat*, justifying their decision with the "flimsy excuse" that they already pay taxes to the government. "You're an enemy of Allah! You pay taxes to a kafir [infidel] government but you don't care about the law!" he said.

A similar response was offered by Jordanian-born Jafar Hawa, who preaches at the Prayer Center of Orland Park in Illinois. Hawa declared that protests against Qur'an burnings will not stop the outrages against Islam.

"They will not stop," Hawa said. "They do it all the time. They do it from the time of the prophet and they will continue doing it until the day of judgement. . . . If they are protected by the law, our Qur'an is protected by Allah." The best way to respond to these protests, he said, was for Muslims to intensify their religious practices. Before condemning Qur'an burners, Muslims should condemn themselves when they do not read the Qur'an and follow its teachings, he said.

"You are a Muslim — act like a Muslim!" he said. "Open this book and get your guidance from this book!" he said.

Mohammed Hijab, a UK-based Islamist with close [ties](#) to Andrew Tate, went so far as to [welcome](#) the attacks on Islam's holy book in a YouTube video posted on July 5, 2023. Qur'an burners, Hijab said, are "mascots" or "prostitutes" who can be used like tools to incite donations for the construction of a mosque in Norway. Qur'an burnings can be used to improve the "fundraising experience" for affected Muslims, he said. "You as the Muslim person and me as a Muslim person now have the have the ability to click the link below and donate to the biggest *dawa* Center in all of Scandinavia!" he said.

It's an improvement over the incitement directed at Salman Rushdie and his translators during the controversy over the *Satanic Verses* in the late 1980s and early 1990s. Maybe, just maybe, the imams of perpetual outrage are starting to worry that their followers are getting tired of rioting and protesting every time someone draws a picture of Mohammad or burns a Qur'an.

The upshot is that if Sweden and Denmark — and the rest of the West — can hold the line on free speech, the blasphemy bullies will change tactics. Instead of using Qur'an burnings to incite violence, they will use such events to raise money.

[Dexter Van Zile](#) is the managing editor of [Focus on Western Islamism](#).

What the h...?





Is this the future you want for your children?





T - NEWS

Team GB to use emergency security app at '24 Paris

Source: <https://www.sportsbusinessjournal.com/Daily/Global/2023/07/24/paris-2024-team-gb-app>



July 24 – British athletes competing in next year's Olympic Games in Paris will carry a "new emergency response app for their phones amid growing security concerns." A report by a leading geopolitical and security intelligence company states that the terrorism threat level for Paris remains "severe," with bomb-carrying drones cited among the potential dangers. There has also been an outbreak of civil disturbance across France this summer after the fatal shooting of French 17-year-old Nahel Merzouk in an encounter with police officers in a Paris suburb. The British Olympic Association (BOA) will send a delegation of **1,100 athletes and staff** to Paris, with the plan to provide an app that gives them "instant access to assistance while also allowing security staff to identify their whereabouts at any given time." BOA officials have been working in tandem with security specialists in preparation for Paris since the conclusion of the most recent Games in Japan.

United States tops 400 mass shootings in 2023

By Paul LeBlanc and Annette Choi

Source: <https://edition.cnn.com/2023/07/24/politics/us-400-mass-shootings/index.html>

July 14 – The United States has surpassed 400 mass shootings in 2023, setting the stage for a record-breaking year in gun violence without any significant federal firearm legislation on the horizon.

America reached the grim figure by Saturday — the earliest in a year 400 shootings have been recorded since at least 2013, [according to the Gun Violence Archive](#). Like CNN, the GVA — a non-profit group formed in 2013 to track gun-related violence — defines a mass shooting as one in which at least four people are shot, excluding the shooter. With five months remaining in 2023, the US has already [eclipsed the number of mass shootings recorded each year](#) from 2013 through 2018. Should the current



ICI C²BRNE DIARY – August 2023

pace continue, 2023 will see more mass shootings than in 2019 through 2022. The Gun Violence Archive started tracking these numbers in 2013.

In 2019, it took 356 days — nearly the entire year — to hit 400 mass shootings. This year and in 2021, however, the United States reached that marker in just seven months.

The rate of mass shootings in 2023 has [consistently outpaced that of past years](#), with an average of nearly two mass shootings a day.

Nearly 1 in 5 US adults has had a family member killed by a gun, including homicides and suicides, according to a 2023 [survey](#) from KFF (formerly known as the Kaiser Family Foundation). About the same proportion of adults have been personally threatened with a gun, and about 1 in 6 adults has witnessed an injury from a shooting, the survey found.

“This is the only country in the world where men who are having breaks with reality exorcise their demons through mass slaughter,” Democratic Sen. Chris Murphy of Connecticut, who has made gun safety legislation [central to his work](#) following the 2012 Sandy Hook Elementary School shooting, told CNN earlier this year.

US marks 400 mass shootings in just over 200 days

The United States reached 400 mass shootings in a record number of days in 2023, about midway through the year. 2019 was the first year to experience more than 400 mass shootings in one year since at least 2013.



“We’re not the only place in the world with mental illness. We’re not the only place in the world where people are paranoid. But only in America are we so casual about access to weapons of mass destruction and only in America do we fetishize violence so much that we end up with all the mass shootings,” he added.

The US also reached 100, 200, and 300 mass shootings more quickly this year than any other year since 2013. One hundred shootings were recorded by March; 200 by May.

Behind the scenes, Biden administration officials have been developing ways in which the federal government can respond in the short- and long-term after a mass shooting, recognizing the physical, mental, and economic ramifications.

But following passage of last year’s bipartisan gun safety law there’s been little political momentum for more gun safety legislation, even as the rate of mass shootings has picked up.

Shootings meet stubborn divide

Research published this year suggests that the effects of mass shootings on mental health may extend beyond the survivors and their communities to a much broader population.

In the days after a school shooting in Uvalde, Texas, in May 2022, a mental health crisis line received a spike in messages that referenced grief, guns and other firearm-related terms, according to a [study](#) funded by the US Centers for Disease Control and Prevention. The study did not track callers’ locations, but the [Crisis Text Line](#) — a non-profit organization offering free confidential crisis intervention — serves people nationwide.

In remarks at the National Safer Communities Summit in Connecticut last month, President Joe Biden delivered an impassioned speech arguing that he believes the movement has reached a “tipping point.”

“Whether we’re Democrats or Republicans, we all want families to be safe. We all want to drop them off at the house of worship, a mall, a movie, the school door without worrying that it’s the last time we’re ever going to see them. We all want our kids to have the freedom to learn, to read and to write instead of learning how to duck and cover in a classroom,” Biden said in remarks at the National Safer Communities Summit last month.

White House officials have been clear-eyed about the political realities Democrats face with the current makeup of Congress, where Republicans in control of the House of Representatives have rejected Biden’s calls for an assault weapons ban.

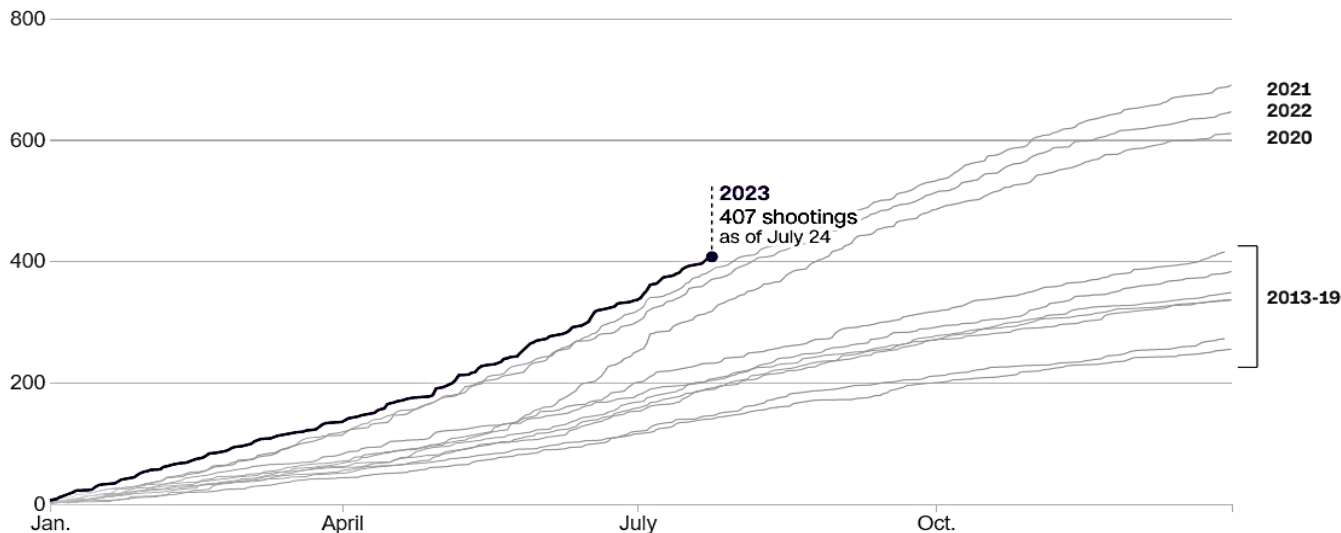


ICI C²BRNE DIARY – August 2023

Even during the first two years of Biden’s term, when both chambers of Congress were controlled by Democrats, an assault weapons ban gained little traction, in part because of the 60-vote threshold needed to break a filibuster and advance bills through the Senate.

More mass shootings in 2023 so far than at this point in any year since at least 2013

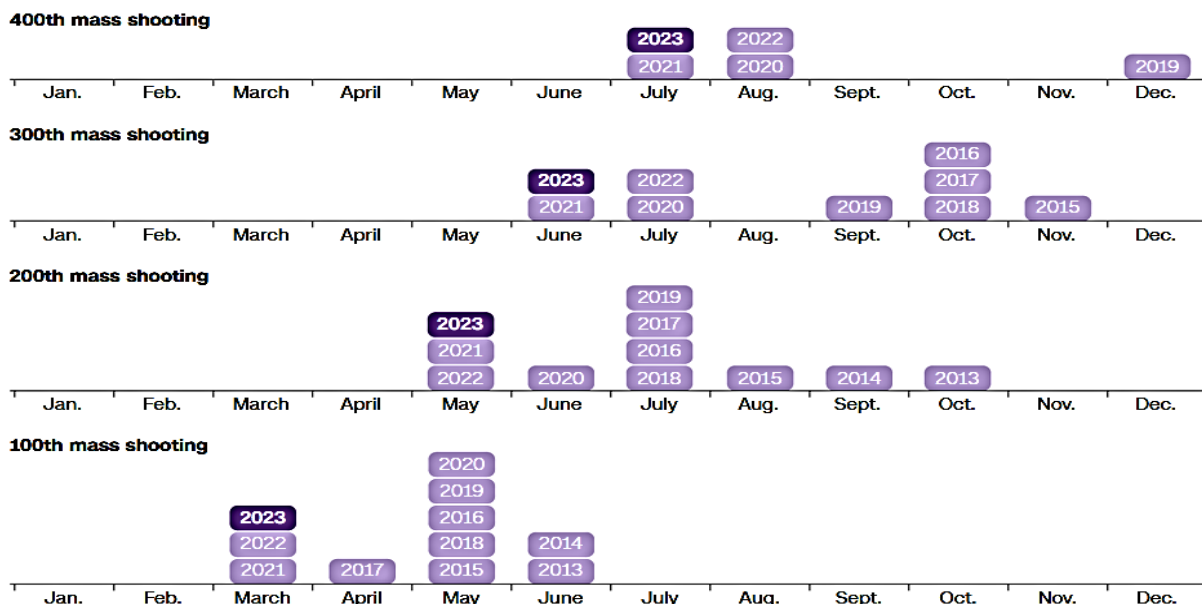
Over 400 mass shootings have taken place in the United States so far this year, including the one in Monterey Park, California — the deadliest attack since the Uvalde massacre in May 2022. There have been more shootings in 2023 than in any previous year since at least 2013.



Note: Data updated at 5:00 a.m. ET on July 25, 2023.

2021 and 2023 are the only years to reach 400 mass shootings as early as July

Over the past several years, mass shootings in the US have escalated at record pace.



A uniquely American tragedy

States with weaker gun laws have higher rates of gun deaths, including homicides, suicides and accidental killings, according to a study published in 2022 by Everytown for Gun Safety, a non-profit focused on gun violence prevention. The political debate on gun control in America, though, is untethered from that data.



And gun violence is still rising. Per [the US Centers for Disease Control and Prevention](#), the firearm homicide rate was 8.3% higher in 2021 than it was in 2020. Firearm suicide rates among people 10 years old and older also increased by 8.3% from 2020 to 2021. And the percentage of homicides attributed to firearm injuries rose from 79% in 2020 to 81% — the highest percentage in more than 50 years. Countries that have introduced laws to reduce gun-related deaths have seen significant progress, [a previous, in-depth CNN analysis found](#):

Australia. Less than two weeks after Australia's worst mass shooting, the federal government implemented a new program, banning rapid-fire rifles and shotguns, and unifying gun owner licensing and registrations across the country. In the next 10 years gun deaths in Australia fell by more than 50%. A 2010 study found the government's 1997 buyback program — part of the overall reform — led to a drop in firearm suicide rates that averaged 74% over the five years that followed.

South Africa. *Gun-related deaths dropped by almost half over a 10-year-period after new gun legislation, the Firearms Control Act, went into force in July 2004. The new laws made it much more difficult to obtain a firearm.*

New Zealand. *Gun laws were swiftly amended after the 2019 Christchurch mosque shootings. Just 24 hours after the attack, in which 51 people were killed, then-Prime Minister Jacinda Ardern announced that the country's gun laws would change. New Zealand's parliament voted almost unanimously to reform the country's gun laws less than a month later, banning all military-style semi-automatic weapons.*

Britain. *[The country] tightened its gun laws and banned most private handgun ownership after a mass shooting in 1996, a move that saw gun deaths drop by almost a quarter over a decade.*

But America's relationship to guns is unique, and its gun culture is a global outlier. For now, the deadly cycle of violence seems unlikely to abate.

[Paul LeBlanc](#) is a CNN Politics editor covering breaking news in Washington, DC.

[Annette Choi](#) is a data and graphics editor on CNN's Digital Visual News team. She covers a wide breadth of topics, including abortion and gun violence.

Six men guilty of murder over Brussels terrorist attacks in 2016

Source: <https://www.theguardian.com/world/2023/jul/25/eight-men-found-guilty-of-brussels-terrorist-attacks-in-2016>

July 25 – Six men have been found guilty of murder and attempted murder for their part in the [2016 Brussels terrorist attacks](#) that killed 32 people and injured more than 300.

They include [Salah Abdeslam](#), who is already serving a life sentence in France for his role in the 2015 Paris terrorist attacks which targeted the Bataclan theatre and France's national stadium, killing 130 people and injuring 350. He was arrested four days before the Brussels attack.

French authorities allowed Abdeslam, along with four others, to be transported to [Belgium](#) so they could face justice over the country's biggest peacetime attack.

Two other defendants were acquitted of murder but found guilty of participating in a terrorist group. Two others were acquitted of the charges they faced. In her closing remarks, Laurence Massart, the president of the Brussels court of assizes, recalled the devastation caused by the bombers, part of a Belgo-French cell of the [Islamic State](#) terrorist group, during the morning rush hour on 22 March 2016 at Brussels airport, in Zaventem, and in a metro station by the headquarters of the EU. The bombings put the country on edge and injured hundreds of people from almost a dozen countries.

The judge described how two blasts had torn through the check-in area at the airport, killing 15 people, injuring hundreds of others and causing "untold chaos". A third unexploded bomb was found on a trolley a



few hours later. Massart told how the explosions had ripped through the ceiling and torn apart suitcases, leaving an immediate aftermath of dust and an acrid smell.

"The silence was broken by the cries for help, a contrast with the total joy of a few moments before," she said.

At Maelbeek metro station a second cell of suicide bombers turned the underground stop into an "underground hell" that victims had said they "would never forget".

The verdicts were delivered to a packed court built especially for the trial in the former Nato headquarters on the outskirts of Brussels. Security was tight as the seven defendants who appeared in court were walked by the arm, one by one, into the defendants' box, by armed officers wearing balaclavas and bright pink armbands. One of the defendants was thought to have been killed in a drone attack in Syria but was tried, and found guilty, in absentia.

Also convicted was Mohamed Abrini, a childhood friend of Abdeslam and a Brussels native who walked away from the airport after his explosives failed to detonate. Identified as [the "man in the hat"](#), he was one of three suspects caught on camera in the airport.

The verdicts close a chapter in [the biggest trial in Belgium's judicial history](#), with more than 900 civil plaintiffs taking part in the hearings that began in December.

Eight of 10 defendants were charged with 32 counts of [terrorist murder](#), attempted terrorist murder of 695 people, and participation in the activities of a terrorist group.

An extraordinary session of the court was opened after 6.30pm to accommodate delivery of the jurors' answers, which were expected to take at least five hours to deliver.

About a dozen family members of victims, most of whom stayed away from the trial, were in attendance.

The defendants will be sentenced at a later date, probably in September.

Five of the defendants are already behind bars, having previously been sentenced in Paris in relation to the earlier terrorist attacks in the French capital.

Taliban Official Labels **Neckties** as Christian Symbol

Source: <https://bnn.network/world/afghanistan/the-necktie-controversy-taliban-official-labels-neckties-as-christian-symbol/>

July 26 – In a recent development, a high-ranking Taliban official, Mohammad Hashim Shaheed Wror, has publicly declared neckties as a symbol of the Christian cross, advocating for their removal from public use. Wror, who heads the Taliban's Invitation and Guidance Directorate, made these comments during a broadcast by TOLONews. His directorate is primarily tasked with instructing the Afghan population on appropriate Islamic practices.

Wror expressed concern over the continued use of neckties by professionals in Afghanistan, particularly doctors and engineers. This development comes amidst the Taliban's ongoing enforcement of strict religious rules on dress and behavior since their takeover of the country in August 2021. Although no explicit dress codes have been imposed on men, women are required to wear a hijab when in public spaces.

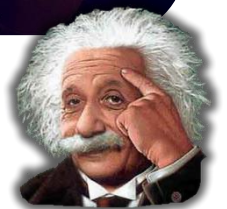
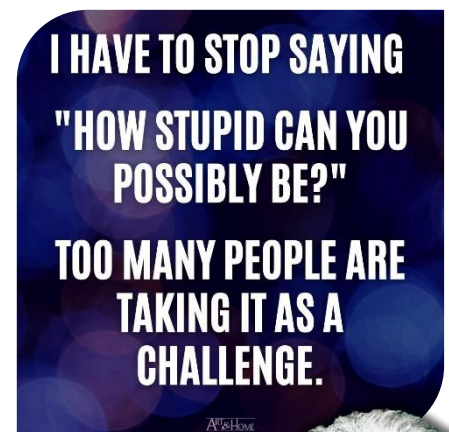
The Changing Attire Landscape in Afghanistan

Despite the Taliban's usual attire of shalwar kameez, waistcoat, and turban, some professionals and news presenters in the country have maintained their collar-and-tie dress. However, the tie's popularity in Western wear has declined since the Taliban's takeover.

The tie, believed to have originated in the 17th century, was popularized by the French. However, its perceived association with the Christian cross, according to Wror's recent statement, seems to have put its use at odds with the Taliban's religious directives.

Afghanistan and Public Dress Codes: Historical Perspective

Historically, Afghan administrations have attempted to regulate public dress, particularly for government officials. During the 1970s Soviet occupation, government employees were discouraged from wearing traditional clothes and were instead advised to wear suits. The former president Ashraf Ghani, who fled the country following the Taliban takeover, often wore Western suits when traveling abroad but chose to wear traditional clothing when in Afghanistan.



Interestingly, as part of their two-decade insurgency, Taliban fighters consistently wore shalwar kameez. However, since assuming power, they have introduced modern military uniforms for their armed forces.

Neckties: A Sign of Changing Attire Norms in Afghanistan?

The stance on the necktie taken by the Taliban official may indicate a further push towards traditional or religiously mandated attire within the country. Neckties worn by men being identified as a sign of the Christian cross only adds another layer to the complex cultural and religious dynamics of Afghanistan under Taliban rule.

While no official dress codes for men have been implemented yet, this development might signal a change in Afghanistan's professional dress standards. Whether this will extend to a wider range of Western-style clothing remains to be seen.

On the other hand, the continuity of necktie use among some professionals and news presenters suggests resistance to completely discarding Western influences in personal attire. The unfolding situation offers a fascinating insight into the evolving cultural norms in Afghanistan post the Taliban takeover.

Is Pakistan spreading Islamic extremism in Africa?

By Michael Rubin

Source: <https://www.firstpost.com/opinion/is-pakistan-spreading-islamic-extremism-in-africa-12921142.html>



A UN peacekeeper from Pakistan patrols on a street in Bitale, 40km north of the city of Bukavu, regional capital of South Kivu province of the Democratic Republic of Congo. Reuters

July 27 – On 12 August, 2020, Islamic militants calling themselves Ansar al-Sunnah seized the coastal town of Mocimboa da Praia in northern Mozambique. It was a bloodbath. The Mozambican Army, which had repelled a similar attack just five months previously, disintegrated. Within days, the militants controlled most of northern Mozambique's Cabo Delgado province and swore allegiance to the Islamic State. Unable to counter the group effectively, Russia's Wagner Group fled, their [first major defeat](#). In March 2021, the same terrorists emerged from the bush and attacked the port city of Palma, 40 kilometers south of the Tanzanian border, [besieging the Amarula Hotel](#) where more than 100 foreign contractors working for a nearby oil concession lived or sought shelter; eyewitnesses say dozens died.

In January 2022, I visited Cabo Delgado to witness firsthand counterinsurgency operations. In Palma, I attended a ceremony marking the opening of school after the Islamic State-mandated closures and



watched as the manager of the Amarula Hotel worked to plaster over bullet holes and remove shrapnel left over from rocket-propelled grenades. As I drove south into Mocimboa, the damage was far more devastating. Charred churches, burnt businesses, and ruined houses marked the town. Rusted hulks of vehicles dotted the roadway. The town had been without water or electricity since the Islamic State blew up generators, ripped up pipes, and tore down wires. The Islamic State's actions in Mozambique differed from what I saw of its occupation in Iraq and Syria. In its Middle Eastern incarnation, the Islamic State held its people hostage in the region's cities and sought to hijack the local economy to sell oil, wheat, and cement. With the exception of churches, the destruction in Mosul, Iraq and Raqqa, Syria were largely the result of fighting to liberate the cities, not perpetrated by the radicals themselves. In Mozambique, the terrorist destroyed everything and forced the entire population into the bush. The men and teenage boys they forced to become soldiers or face execution. The women and girls they forced into servitude or forced into marriage. Towns remained abandoned.

The Rwandan Army [deployed](#) to Cabo Delgado to lead the counterinsurgency fight and help restore Mozambique's shattered capabilities. The commander in Mocimboa showed me both captured weaponry such as AK-47s, grenades, mortars, and bazookas; electronics such as walkie-talkies, computers, and satellite phones and the literature captured Islamic State fighters carried. Literature is important because it shows the nature of radicalisation. Traditionally, Muslims and Christians lived together in Cabo Delgado down to the town and village. Local traditions, animist influences, and Sufism permeated Muslim practice. Moderation was paramount. This is why literature matters. Notebooks seized from captured fighters, some of whom I met, reflected arguments, radical interpretations, and Quranic citations to sway a largely illiterate population to extremist interpretations that justified terror and the ambitions of the Islamic State. Many of the tracts captured fighters carried originated in Karachi, Pakistan, according to publication data in the books and pamphlets. Stickers and stamps indicated they arrived through Mombasa, Kenya, the largest port in east Africa, 4,300 kilometres away.

Pakistan did not fund the Mozambique violence—that was the responsibility of Tanzanian businessmen who confused Islamist charities with piety and their Mozambican counterparts who paid Ansar al-Sunna protection money—but incitement matters and Pakistan often provided the platform upon which to brainwash recruits.

Because of the Rwandan intervention, Mozambique is no longer the epicentre of the Islamic State threat in Africa. While Nigeria and its neighbours continue to face Boko Haram violence, Al Shabaab destabilises Somalia and sponsors violence in Kenya and radicalism grows across the Sahel, and increasingly the Islamic State gravitates to the Democratic Republic of Congo (DRC, formerly known as Zaire). Unlike in the Sahel and Horn of Africa, there is little international counterterrorism presence to counter militant presence in Congo.

Years of instability, corruption, limited government control and neighbouring state interference have transformed the DRC. In the aftermath of Rwanda's [1994 anti-Tutsi Genocide](#), the génocidaires fled to eastern Congo. The United Nations set up camps for refugees pouring in from Rwanda but, compounding their inaction prior to the genocide itself, they neglected to disarm the Hutu militants. Just as in southern Lebanon and Gaza Strip, the UN refugee camps became incubators for terrorism that not only furthered internal unrest but also upset cross border stability. This in turn contributed to Congo becoming the focal point for two great African wars in the late 1990s and early 2000s that ultimately involved nine countries, numerous militias, and killed more than five million civilians.

It was against this backdrop that the Allied Democratic Forces (ADF) which, despite its name, is a radical Islamist group that evolved in part of more [extreme Tablighi Jamaat elements](#), moved into the DRC from Uganda, where today it represents itself as the Central African branch of the Islamic State. Initially in Congo's North Kivu province, it has now expanded into Ituri. Both provinces are resource rich, with gold, diamonds, other minerals, and oil. Even if the ADF does not mine gold and diamonds directly, extracting protection money under the guise of taxes fills its coffers and enables it to expand.

In 1999, the United Nations established a peacekeeping mission for the DRC that, in 2010, it renamed the United Nations Organisation Stabilization Mission in the Democratic Republic of the Congo (MONUSCO). Like many UN missions, [MONUSCO is big and bloated](#), with an annual budget in excess of \$1 billion. During conversations with me this month in Congo's capital Kinshasa, I asked about the source of support for the ADF, especially given the traditional moderation of Congolese Muslims. Locals reported that a major engine for radicalisation among the local population is MONUSCO and particularly the Pakistani component that [numbers](#) approximately 1,700 persons.

In short, Congolese say that while the Pakistani component to MONUSCO might wear blue hats, many take it upon themselves as a personal mission to propagate and catalyze a more extreme interpretation of Islam common in Pakistan but foreign to Congo. Just as Pakistani literature emanating from Karachi's publishing houses passively supported the Islamic State in Mozambique, Pakistan's UN component appears much more actively even if unofficially to encourage and enable the Islamic State in Central Africa. This is not to allege a vast Inter-Services Intelligence (ISI) conspiracy in the DRC. Rather, it is the natural outgrowth of Islamic extremism among Pakistan's officer



corps. To deploy on a UN mission is for Pakistani soldiers a reward. UN assignments are more lucrative than normal army service, and an assignment Pakistan's military leadership offers only to the most ideologically loyal. This in turn [requires embracing the Islamist radicalism](#) that has marked Pakistan's officer corps since the Bangladesh defeat and the rule of president-turned-prime minister Zulfikar Ali Bhutto.

I asked Congolese officials why they simply did not complain to the UN leadership. The answer: UN procedures give little recourse to recall national components. Just as the UN cited its own bureaucratic procedures to do nothing during the Rwanda genocide and then refuse to disarm its perpetrators in the UN's eastern Congo refugee camps, so too does its inaction today set the stage for far greater bloodshed. The Pakistanis enabling the ADF's rise do not care; they will simply return to Pakistan with full bank accounts and no need to suffer direct consequences for their actions.

Both Mozambique and Congo must do much more to restore order and reduce their permeability to the Islamic State. Pakistan is not responsible for their decades of poor governance, but individuals in Islamabad are increasingly seeking to take advantage of it. Islamic extremism have left Pakistan teetering on the brink of state failure. It is tragic that rather than recognise their ideological cancer, many Pakistanis now seek to export it.

Michael Rubin is a senior fellow at the American Enterprise Institute in Washington, DC.

+ Denmark

Sweden Is Now a 'Priority' Target for Islamist Terrorists

By Chris Tomlinson

Source: <https://europeanconservative.com/articles/news/sweden-is-now-a-priority-target-for-islamist-terrorists/>

July 29 – Sweden has seen several protests involving the burning of the Quran over the last few years but recent burnings and desecrations of the Muslim holy book have fuelled increasing tension between Sweden and countries in the Muslim world.

The Swedish Security Police Säpo, which is responsible for counter-terrorism operations and other espionage operations, is now warning that Sweden has become a priority target for Islamic radicals looking to carry out acts of terror.

Security Service Chief Charlotte von Essen [held a press conference](#) Thursday, July 27th, along with Sweden's Minister of Justice Gunnar Strömmer to discuss the country's deteriorating security situation. Von Essen said,

In the past, we have seen that Sweden has been a legitimate target, just like many other countries in the West. Now Sweden is being singled out in particular, which makes us a more prioritized target.

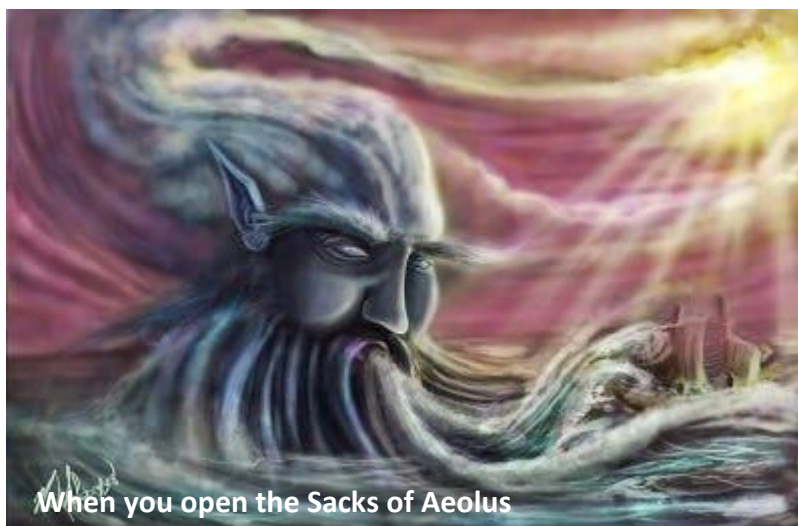
Minister of Justice Strömmer linked the situation to the recent Quran burnings saying,

The reactions against Sweden have been very strong. The government has been working to maintain dialogue with countries in the Muslim world.

Earlier this year in January, Danish anti-Islam activist Rasmus Paludan burned a copy of the Quran in front of the Turkish embassy in Stockholm, leading to [condemnation from the Turkish government](#) at the time, further complicating Sweden's bid to join the NATO military alliance.

This month, Turkish authorities issued [an arrest warrant](#) for Plaudan, although the Danish activist simply laughed off the warrant and explained he had no plans to ever visit Turkey.

Another activist, Iraqi migrant Salwan Momika, has also held similar demonstrations, either burning or desecrating the Quran. Earlier this month Momika desecrated the Quran in front of the Iraqi embassy, which had been preceded just hours before by the storming of the Swedish embassy in Baghdad by protestors who lit the embassy on fire.



Following Momika's protest, Iraqi authorities laid the blame on Sweden for allowing the demonstration to go ahead in the first place and [announced](#) that they would be cutting formal diplomatic ties with Sweden, leading to the removal of the Swedish ambassador and the recalling of Iraq's top diplomat in Sweden.

"The Iraqi government has informed the Swedish government through diplomatic channels that any recurring incident involving the burning of the Holy Quran on Swedish soil would lead to the breaking of diplomatic relations," Iraqi Prime Minister Mohammed Shia al-Sudan said.

One of the top Muslim universities in the world, the al-Azhar University in Cairo has also condemned Sweden for allowing the burnings and desecrations to happen, arguing for [a boycott of Swedish goods](#) in the Islamic world.

Despite all of the outrage and the likelihood of Sweden becoming a target for terror, Von Essen stated Thursday that the country's terror level will not yet be raised and will remain at level three of five, where it has been since 2016, but noted the situation could change quickly.

The security chief added that Swedes should not be afraid but should remain vigilant and report anything they think may be suspicious.

Sweden has only seen one major Islamic terror attack in recent years in 2017 when Uzbek asylum seeker [Rakhmat Akilov](#) drove a truck through a shopping area in Stockholm, killing five people, including an [eleven-year-old girl](#) named Ebba Åkerlund.

Von Essen's warnings are not without merit, however, as Swedish authorities claimed to have [foiled a terror plot](#) in April of this year that they said was linked to the January Quran burning by Rasmus Paludan.

A total of five people, believed to have links to international Islamist extremism, were arrested by police and were allegedly in the planning phase of carrying out an attack.

[Chris Tomlinson](#) is a British-Canadian journalist for *The European Conservative*. He is focused on migration, European politics, far-left extremism, and Islamic terrorism. Formerly of *Breitbart News*, he has covered stories from the migration crisis to Brexit and the rise of populism and traditional conservatism across Europe.

Terrorism and cyber attack warning as 25 biggest threats facing Ireland revealed

Source: <https://www.irishmirror.ie/news/irish-news/terrorism-cyber-attack-warning-25-30618234>

Aug 03 – Ireland faces an increased threat from terrorism and cyber-attacks – because we spend so little money on defence, the government has admitted.

This year's national risk assessment also finds that Ireland faces 25 different potential threats – from terrorism to financial instability, as well as climate change, AI and even housing problems.

And the assessment, published on Wednesday morning by Taoiseach Leo Varadkar, also warns that extremist groups here are trying to stoke up tensions about the rising levels of immigration.

"The increase in the immigrant population in Ireland has occurred in a short time frame and with relatively limited upheaval compared to other countries.

"However, social tensions can be exploited by extremist groups, such as through the spread of mis/disinformation, including by malevolent actors," the report says.

But the report also reserves special mention for dangers posed to Ireland that are potentially made worse because of the low level of spending on [the Defence Forces](#) - who are meant to be able to protect us from external and internal threats.

The assessment comes a year after the Commission on the Defence Forces warned [the military would not be able to offer a meaningful defence](#) of the country and made sweeping recommendations to solve the crisis.

But 12 months on, the government-written risk assessment admits our low military spending could make threats even more dangerous.

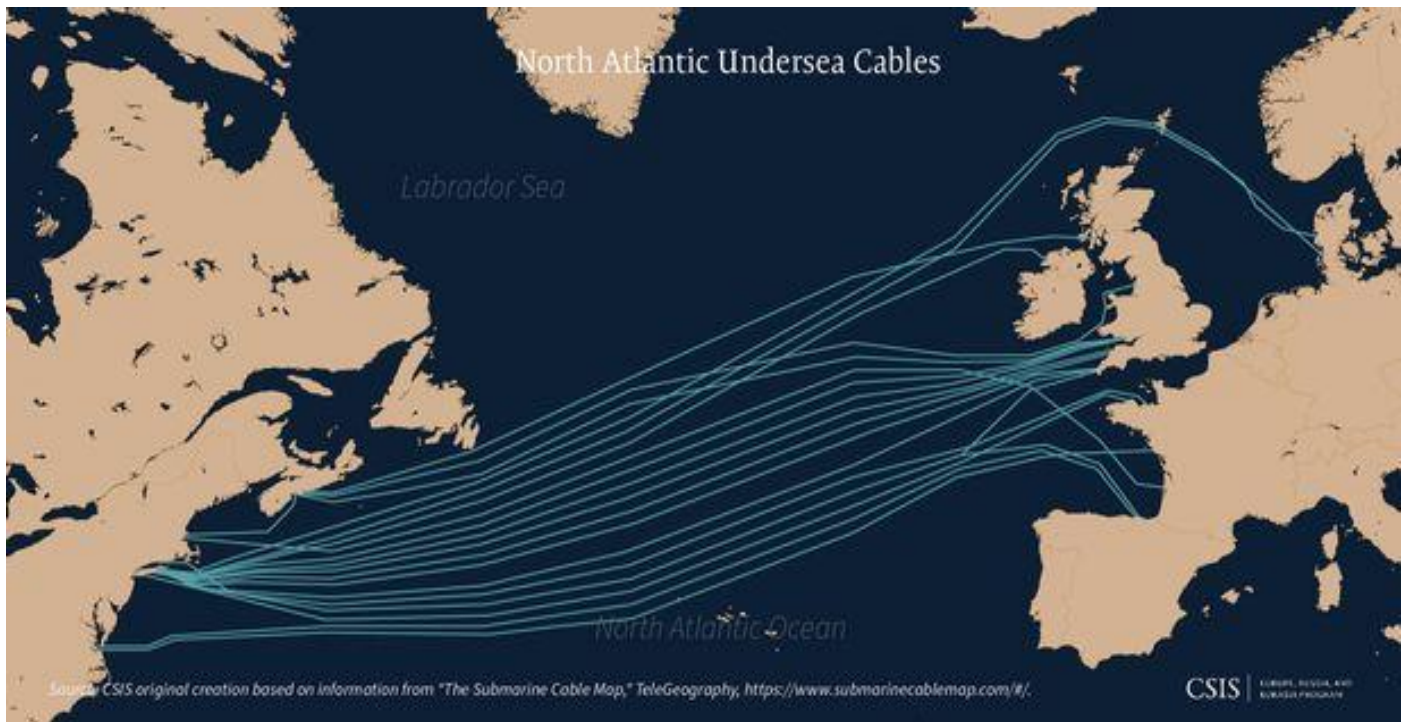
It says: "The risks to [Ireland](#) posed by armed conflict, terrorism and hybrid security threats are potentially compounded by our having one of the lowest levels of investment in military and defence capabilities within Europe."

The report also highlights [the vulnerability of vital undersea cables that run in Irish waters](#).

The cables carry internet traffic between the US and Europe – but security experts have repeatedly warned that they could be attacked by saboteurs, including [Russia](#).

An attack that damaged one of the cables would have a devastating effect on world business and communication - but Ireland has no real way of protecting them.





Many cables connect the US and Ireland

The report says the concerns are getting stronger – and also highlights the 2021 cyber-attack on [the HSE](#) which caused havoc here for months.

It says: “Concerns about related threats to strategic infrastructure, cybersecurity and maritime security, including the risk to telecommunications and energy transmission infrastructure from acts of sabotage, have become more pressing.

“The presence of [significant communication and cloud infrastructure in Ireland](#) exposes our country to an additional degree of risk from both State and non-State actors.

“The potential disruptive effect of cyber-attacks was starkly demonstrated by the HSE [cyber security incident in May 2021](#).

“Furthermore, the emergence of hybrid threats, utilising a mix of cyber and other methods, has expanded the potential vectors of attack. Foreign information manipulation and interference also poses a risk to the security of the State.”

The assessment also warns that failure to restore the power sharing government in [Northern Ireland](#) could cause problems for the whole island.

It warns: “Restoring the devolved institutions following the May 2022 elections is vital in supporting political stability in Northern Ireland, including to address the legacy of the past and ongoing work to tackle residual paramilitarism.

“Failure of post-Brexit arrangements or [the continued absence of the Northern Ireland institutions](#) would present a risk to political stability and its economic outlook, with potential significant implications for Ireland.

“Strengthening relationships both on the island of Ireland, including through the Shared Island Initiative and between Britain and Ireland in a post-[Brexit](#) context remain key to this.”

The report also warns that Ireland is vulnerable to a global economic downturn – and says the recent international [rise in inflation](#) poses a substantial and immediate risk to the Irish economy.

It also says that Ireland is particularly vulnerable to disruptions to supply or [price rises in oil and gas](#) - because of our location. We are at the edge of western Europe and have to pay more to get supplies here.

And it highlights the risk posed to the Irish economy by Brexit – with challenges to the relationship between Ireland and Britain.

It says: “Ireland’s post-Brexit relationship with Great Britain will continue to present challenges, in particular as it diverges from [the European Union](#).

“These risks could impact upon trade and investment in both directions, even though mitigated by proximity, and interdependency such as in [the area of renewable energy policy](#).

“Brexit will also continue to have an impact on Ireland’s trade with Great Britain, as the UK moves to introduce checks and controls on imports.”



And it warns all of society could be affected by a failure to solve [the housing crisis](#).

It says: “An [inability to effectively and efficiently bring about an increase in the supply](#) of housing risks creating a chronic situation, with associated implications for our society and economy.

“Housing shortages and [pricing issues are unlikely to rectify themselves](#) over the short term with the COVID-19 pandemic having impacted housing completions and now increased construction material inflation, shortages in skilled labour, and rising viability challenges, all having an impact on supply.

“Russia’s full-scale [invasion of Ukraine](#) has exacerbated supply chain and inflationary issues, further undermining deliverability of an adequate housing stock.”

Welcoming the risk assessment, which has been published every year since 2014, Taoiseach [Leo Varadkar](#) said it was vital that the state knew the potential threats it faced.

He said: “The list of 25 risks outlined in this year’s National Risk Assessment vary in nature, ranging from unavoidable global risks, such as climate change, to acute hazards, such as chemical, biological, [radiological and nuclear threats](#).

“Many of the risks identified for 2023 have been identified in previous iterations of the National Risk Assessment, however many of these have evolved, given a changed social and economic context. Some risks have increased in significance, including those related to the security of our energy supply, fiscal sustainability, and protectionism and deglobalisation, and there are newer risks relating to the proliferation of disruptive technology, such as Artificial Intelligence.

“Despite the varying nature of the identified risks, all require our awareness and our consideration, so that we can better prepare for their possible occurrence.”

Lure of Jihad: How role of women in Islamic State is changing and gaining significance

By Vaasu Sharma

Source: <https://www.firstpost.com/opinion/lure-of-jihad-how-role-of-women-in-islamic-state-is-changing-and-gaining-significance-12961412.html>



Aug 05 – The downdrift in the activities of Islamic State, owing to targeted efforts to eliminate the group leadership, it would be interesting to take a peep into the recruitment of women by the Islamic State (IS) as an alternative option to sustain itself and understand the underlying motivation and effectiveness of such action by the group. It will also give an insight into the IS’ ideology, recruitment strategies, indoctrination processes, and the factors inducing them for their engagements in regions, including India’s Kerala. The understanding of



these dynamics may facilitate policymakers/researchers to make pragmatic and effective contributions in countering group activities. This brief article explores the IS' ideology, recruitment strategies, methods of indoctrination, women's specific roles, and the factors driving Indian women, particularly in Kerala, to join the IS. By addressing these aspects, one can assess women's involvement in IS and their potential implications for global security. One cannot gainsay that female Jihadists have been in existence in the past too as testified by the fact that [one-third](#) of all violent terrorist attacks, documented globally, from 1985 to 2005, were attributed to women. During the very period, an investigation by Yoram Schweitzer exposed that nearly 15 per cent of the global suicide bombings owe their roots to approximately 220 documented instances of female suicide bombers. Despite male jihadists remaining key players in the majority of jihadist activities, it is an open secret that women are progressively occupying the key role in such activities.

Women in Jihadist organizations

There have been historical records to prove that women have remained active in war activities, though mainly in supporting roles of nursing/caregiving than direct combat, in various regions across the globe. This pattern persisted in contemporary Middle Eastern contexts, where women joined Jihadist organizations in the role of mothers. The 237 stories of Palestinians, linked to the initial Intifada between 1988-90, which were documented by Sharif Kanaana reveal key roles of women in [28 per cent](#) of the narratives. Kanaana states that Palestinian mothers inadvertently facilitate the continuation of resistance by giving birth to male offspring, who eventually become fighters. Hence, women's roles are deemed indispensable for the perseverance of resistance.

Jihadist organizations, however, do have instances of women engaged in violent activities. Even the Quran mentions female fighters, including the revered Nusayba bint Ka'ab, also known as [Umm Umarah](#). She actively fought in six battles, including the Battle of Uhud, where she defended Prophet Muhammad alongside her husband and sons. These Islamic historical examples justify women's involvement in contemporary Jihadist movements.

Women's evolving roles in IS

In its initial days, IS was not focused on the recruitment of female followers. However, the women's role gradually assumed significance with the evolution of the organisation's objectives. Under the core IS ideology, propagating the establishment of an Islamic caliphate, governed by Sharia, women are supposed to don the traditional roles as wives, mothers, and homemakers to preserve moral purity. Apart from Jihadist duties women play a crucial role in nourishing and tending to the injured fighters, raising children and maintaining households. IS members use various social media platforms, such as Twitter and Telegram to engage online with foreign women. They allure women to travel to places like Syria, with the promises such as – a devout Jihadist husband, the experience of life in an authentic Islamic state, and an opportunity to dedicate themselves to their religion. The presence of a larger number of female members in IS in turn draws a greater influx of male recruits. The potential male recruits get allured by the prospect of Western blonde converts, who are regarded as more sexually desirable within the ideological framework of the organisation. In July 2018, the estimated number of Western individuals who joined IS as foreign fighters and civilians reached 41,490, out of which [4,761](#) were women and 4,640 were minors. According to Mia Bloom, a professor at the Center for Terrorism and Security Studies at UMass Lowell, [many girls](#) are enticed to join IS due to a combination of fantasies and the belief that their involvement will empower them, offer an exciting life, and give their lives meaning.

One side of the spectrum considers that Jihadist women are the victims of brainwashing and its proponents advocate their potential repatriation, on the other hand, there are women and men, who adopted the IS ideology fueled by its narratives and propaganda. They diligently fulfil the roles assigned to them and women apart from marrying and giving birth to the offspring of Daesh militants, undergoing training, and assuming the mantle of terrorism.

Some women holding divergent views from Western-associated values, such as feminism, opt their innate inclination towards submission. They derive fulfilment from being dominated and directed. Aligned with the conviction that adherence to Sharia law signifies the most righteous path, these women perceive Western societies as incapable of fulfilling this ideological framework. The proponents of this position advocate for strict measures, opposing the repatriation of these individuals.

Significantly, IS considers women as a better option for carrying out suicide bombings, as women in society are largely perceived as associated with caregiving roles and draw lower security scrutiny in public arenas. Further, they possess the potential to exploit prevalent social norms and gender biases, prevalent in counterterrorism endeavours.

The IS subjects women to rigorous indoctrination procedures to brainwash their beliefs and behaviours by employing diverse methods, including isolation, psychological manipulation, exploitation of vulnerabilities, coercion, and the reinforcement of extremist ideology. By severing women from their previous social networks and sources of information, IS fosters a sense of dependence and loyalty. IS shapes their perception of the world and instills a profound sense of duty/devotion towards the group by utilising propaganda and fear-based tactics. Through coercion tactics involving pressure, deceit, or even physical force, IS exercises control over women's actions and choices



and through the relentless underpinning of their extremist ideology, indoctrinates women with a distorted interpretation of Islam that justifies their acts of violence and brutality. It transforms women into devoted adherents of IS' cause.

Decoding IS recruitment of women in India

From an Indian perspective, Islamic State made inroads in Kerala from 2013 onwards. In early 2014, IS began establishing and deploying modules in Kerala that facilitated religious conversions and recruited professionals to join their forces in Afghanistan and Syria. Numerous individuals from Kerala, both men and women, have joined the ranks of the Islamic State of Khorasan Province (ISKP) in recent years. The United Nations, in its [2020 terrorism report](#), has cautioned about the significant presence of IS terrorists in Kerala. The four girls trapped and lured to become Muslims, left India in 2016 to join the ISKP (Islamic State of Khorasan Province) – the Khorasan edition of IS – in Afghanistan along with a group of 21 men and women from Kerala. They were first taken to Iran and then they crossed over to Afghanistan on foot from Iran. One, Nimisha was the only Hindu girl among these four girls. The other three were Christian.

Women's recruitment in India, specifically in Kerala, can be attributed to socio-economic hardships, radical ideologies circulated through social media platforms, a perceived sense of marginalisation/injustice, the allure of an idealised Islamic state, and the presence of networks to facilitate the recruitment/travel to conflict zones. The reasons behind Kerala's women joining IS are multifaceted. One significant factor is their conversion to Islam prior to their departure for Afghanistan. These conversions, motivated by either love or faith, make them more susceptible to radicalisation, especially if they face opposition or discrimination from their society or family. The online radicalisation exposure provides them with access to ideological narratives, peer groups, and emotional support that shaped their worldview and motivated their decision to join IS. Additionally, family ties played a crucial role in the recruitment process. The women were accompanied by their husbands and children when they migrated to Afghanistan, and family members often acted as recruiters or facilitators. The choice of Afghanistan over Syria or Iraq, as their destination by Kerala women may be attributed to factors such as geographical proximity, logistical convenience, ideological affinity, or personal preferences.

India as a whole has experienced fewer IS recruitments than West as India has a strong national identity that transcends religious or ethnic differences, fostering a sense of pride in democratic values and institutions. The country pursues moderate Islam and promotes pluralism, tolerance, inclusivity, and harmonious coexistence with other faiths/cultures. Additionally, effective counter-terrorism measures, including proactive security and intelligence agencies, international cooperation, and comprehensive legal frameworks, contribute to the prevention and detection of potential IS threats within the country. Furthermore, India's vibrant civil society actively engages in countering radicalisation through initiatives such as interfaith dialogue, social harmony, education, etc.

Conclusion

A thorough examination of the role of women within IS sheds light on the organisation's ideology, recruitment strategies, and indoctrination methods. It also reveals the factors and dynamics driving Indian women, particularly from Kerala, towards IS, which are multifaceted, including socio-economic challenges and online radicalisation among others. By understanding the ideology, recruitment strategies, indoctrination processes, and underlying motivations, comprehensive counterterrorism measures can be developed. Effective prevention efforts should involve countering online radicalisation, promoting alternative narratives, and strengthening community resilience. The strategies should prioritise empowerment and inclusion, by ensuring access to education, economic opportunities, and social support networks. The targeted strategies must aim to lessen the appeal of extremist ideologies, dismantle recruitment networks, and promote social resilience against radicalisation.

[Vaasu Sharma](#) is currently pursuing a Ph.D. in International Relations at the University of Haifa in Israel.

Terrorism: What's behind surge in arrests of under-18s?

By Rachel Stonehouse (BBC Newsbeat)

Source: <https://www.bbc.com/news/newsbeat-66365312>

Aug 03 – Record numbers of young people are being arrested for terrorism-related offences. And their journey into extremism tends to start online.

Jon started going down the rabbit hole when he saw a social media post.

He was at school when a friend showed him something about British soldiers living on the streets.

It struck a chord with Jon. His uncle was in the Army, and here was a group that cared about how former soldiers were treated.



So Jon followed it, and that's when things turned darker.

"Once I got involved they'd be saying things to me like how veterans were struggling because of people from other countries taking money out of the system," he says.

Jon, whose name we've changed, says he absorbed more and more posts making questionable claims like these, and his views gradually became "more extreme".

But it also gave Jon a sense of purpose.

"I was a very angry guy, struggling academically and didn't know where my life was going," he says.

Jon got pulled towards the far-right and groups usually associated with racism and ultra-nationalism - the belief that one country and its people are superior to others.

His story's not unusual.

A worrying trend

Figures from UK Counter Terrorism Policing (CTP) show that one in five of those arrested for terrorism-related offences are under 18.

In 2019, just 4% of those arrested were aged under 18 - but by 2022 the figure had increased to 20%.

Matt Jukes, the head of CTP, says it's a "really worrying trend".

"These extreme ideologies are much more available online and on social media than they ever were before," he says.

"And we know young people are exploring dark corners of the web."

Experiences in these shadowy sites, groups and forums can spill over into the real world, and in Jon's case that was trying to convert others.

He even started delivering hate speeches at college, which got the attention of the school's safeguarding lead.

By the time she approached Jon he was so far-gone that he offered her a campaign sticker and invited her to a demonstration.

Thinking back, Jon, who's now 23, says that was "the best thing I ever did".

'It was all fake'

It led to him being referred to the government's counter-terrorism programme, Prevent.

The scheme is designed to stop people being drawn into terrorism before it's too late, and schools and colleges were given a legal duty to identify those at risk in 2015.

It's been heavily criticised since, particularly by Muslim groups who say it unfairly targets their faith.

In the year up to March 2022, CTP say there were 6,406 referrals to Prevent - 20% related to extreme right-wing ideology and 16% to Islamist ideology.

[A recent review](#) - which was itself accused of bias - said Prevent had failed to stop people referred to the programme who went on to be involved in attacks.

But the people behind it say it's been successful at diverting people away from a dark path.

Jon says he got on really well with his intervention worker, who went through the statistics and claims in the posts he'd been sharing. And it showed that they weren't factually accurate.

"He got me to download an app of the Quran and showed me that all quotes I'd been sharing from it weren't even in there.

"It was all fake," he says.

CTP chief Matt says the pandemic has fuelled the increase in young people involved in terrorist offending, and that social isolation and time spent online is a contributing factor.

The way young people interact with hateful content is also changing.

More and more are taking elements of existing extreme viewpoints and merging them together to create new ideologies, according to CTP.

"We're seeing a big increase in people drawing down hateful content and using that to construct their own view of the world," says Matt.

Police want more under-25s to report their concerns, so they've recruited people who've been caught up in terror attacks to show the results of extremist ideologies.

People like Max Balegde, who was with his little sister when an Islamist terrorist [detonated a bomb at Manchester Arena](#) following an Ariana Grande gig in 2017.

They weren't physically hurt, but Max still experiences the psychological impact and flashbacks to what they witnessed.

"It's so easy to get swept up in it and believe things that aren't true," he says.



"I hope I can interact with people who've been seeing stuff on social media, and share my story about the impact that terrorism can have on people's lives."

Travis Frain also works with young people to share his story.

Travis was 19 when he suffered a fractured leg, shrapnel wound and broke his left hand in [the 2017 Westminster Bridge attack](#) in London.

He was one of dozens hurt when a terrorist drove a car along the pavement of the bridge, which crosses the River Thames next to the Houses of Parliament.

"I looked up and saw a car coming towards me, I went over the bonnet into the air, and then hit the concrete," he says.

He ended up quitting university and moving back home to recover, but counts himself as "one of the lucky ones".

Max, Travis and Jon hope speaking out will mean luck no longer comes into it, and people can be kept away from extremism.

And Jon has a piece of advice for anyone worried that they or a friend might be slipping down the rabbit hole.

"Reach out and get some help," he says.

"Don't be scared of leaving or getting in trouble, you'll just get good help to turn your life around."

Quran-burnings can fuel Islamic extremism, terrorism - opinion

By Salem Alketbi

Source: <https://www.jpost.com/opinion/article-753989>



Sweden raises its terror threat level to high for fear of attacks following recent Quran burnings

BURNING A Swedish flag to denounce the desecration of a Koran outside a Stockholm mosque (?), in Karachi, Pakistan, July 7. (photo credit: Akhtar Soomro/Reuters)

Aug 08 – Those who are keeping up with the developments resulting from the insult to Islamic sensitivities – the [burning of copies of the Quran](#) in European countries – can grasp the gravity of the situation. These events impact the anticipated international collaboration in countering extremism and terrorist ideologies, as well as efforts to foster a culture of tolerance and coexistence among different nations and peoples.

Without a doubt, some European governments use the "freedom of expression" catchphrase to justify these transgressions and violations, unjustifiable and baffling when we consider the potential repercussions when dealing with such a highly sensitive issue that deeply affects the emotions of over one and a half billion Muslims worldwide, including the Muslim citizens of those same European countries.



However, what grabs my attention in this matter is that the Islamic response to these violations goes beyond the formal protocol framework. It's no longer limited to official protests or conveying the countries' angry positions to European authorities. Instead, well-known extremist organizations like the Iranian [Islamic Revolutionary Guard Corps](#) have gotten involved, which comes as no surprise. Its commander, Brig.-Gen. Hossein Salami issued a revenge threat, saying, "We will not allow those who insult the Quran to have security. If someone wants to play with our Quran and religion, we will play with all his world. Sooner or later the vengeful hand of mujaheds will reach politicians and stage managers behind this sort of crimes."

The continuous repetition of [insults against the Quran in Denmark](#) and Sweden needs to end, and the authorities in both countries must confront these violations firmly and decisively. This is vital for maintaining global security and stability because the way the matter is currently being dealt with fosters hostility between Islam and the West – providing fertile ground and ample opportunity for spreading terrorist ideologies, thereby endangering these countries themselves.

Relations between Islam and the West are in danger due to Quran-burning tensions

The involvement of organizations such as the Iranian Islamic Revolutionary Guard Corps in this crisis doesn't benefit the interests of Islam, Muslims, or the West. The leader of the Iranian militia is exploiting these violations to stir up the emotions of millions of ordinary Muslims, dragging the crisis onto a slippery slope. Of course, no sensible person wants these matters to be handled outside the legal framework. The authorities in the relevant European countries, which have been and continue to be the stage of these unacceptable trespasses, should confront the radicals instead of giving them approvals or endorsing these crimes under the guise of "freedom of expression." And yet, these countries' silence and their efforts to rationalize rather than condemn the violations, fuel extremism, and embolden hard-liners in the Islamic world to amplify their voices and attract many to their positions and ideas – promoting revenge and defense of Islam among other slogans. This loud hush from the relevant authorities in European countries, combined with the repeated offensive violations against the sentiments of all Muslims, is creating a serious political headache for governments of Islamic countries. It is undermining their efforts to root out extremism and radical ideologies from their societies.

It may even impede their ability to address unacceptable practices, such as attempts to storm or launch attacks on European embassies, fueled by apparent anger or protectiveness towards Islam, but in reality, exploiting slogans and inflaming emotions. These offensive violations are exploited by extremist organizations to further their own goals and spread their ideas within communities. The recurrence of vile actions that offend the feelings of all Muslims cannot be justified within any political or legal framework. The principles concerning the preservation of freedoms are clear and unambiguous. What is happening again and again is clearly a breach of these constitutional and legal principles – prior even their being a violation of Islamic or other sanctities.

Laws and constitutions are all established to ensure the security and stability of countries and of people, preventing anything that threatens or undermines this security. Therefore, permitting such infringements on the heightened sensitivities of millions around the world creates a disassociation from the duty to safeguard constitutional rights, and involves a deliberate misinterpretation – or a lack of understanding of the situation from all angles.

Moreover, such decisions and stances have catastrophic consequences for the culture of tolerance and coexistence, which serves as the sole lifeline for humanity to steer clear of the epidemic of violence and terrorism and hopefully eradicate them completely.

[Salem Alketbi](#) is a UAE political analyst and former Federal National Council candidate.

Existential Terrorism: Can Terrorists Destroy Humanity?

By Zachary Kallenborn and Gary Ackerman

Published online by Cambridge University Press: 04 August 2023

Source: <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/existential-terrorism-can-terrorists-destroy-humanity/5A3724049B1985D8762AACC4DDBB8C0C>

Abstract

Mass-casualty terrorism and terrorism involving unconventional weapons have received extensive academic and policy attention, yet few academics have considered the broader question of whether such behaviours could pose a plausible risk to humanity's survival or continued flourishing. Despite several terrorist and other violent non-state actors having evinced an interest in causing existential harm to humanity, their ambition has historically vastly outweighed their capability. Nonetheless, three pathways to existential harm exist: existential attack, existential spoilers and systemic harm. Each pathway varies in its risk dynamics considerably. Although an existential attack is plausible, it would require extraordinary levels of terrorist capability. Conversely, modest terrorist capabilities might be sufficient to



spoil risk mitigation measures or cause systemic harm, but such actions would only result in existential harm under highly contingent circumstances. Overall, we conclude that the likelihood of terrorism causing existential harm is extremely low, at least in the near to medium term, but it is theoretically possible for terrorists to intentionally destroy humanity.

The Islamist roots of French disorder

By Liam Duffy (counter-terrorism researcher)

Source: <https://www.newstatesman.com/world/europe/2023/08/islamist-roots-french-disorder>



Aug 07 – The most [destructive, spectacular and costly riots](#) in [France](#)'s recent history, surpassing even the infamous unrest of 2005, are over. To the Anglophone media and its audiences they were an expression of the anger felt among the children of France's former overseas possessions – a generational resentment fuelled by experiences of poverty, discrimination and painful colonial legacies.

Others have noted the opportunistic, even recreational quality of rioting, but the anger – the rage – against France among parts of its youth is real and goes deeper than one specific event.

Socio-economic woes are crucial in explaining this tide of feeling. Yet any analysis which takes this into account but omits the specific and sustained delegitimation of France contained within that feeling is incomplete. There are political currents busily undermining the republic's foundations, all combining with very real structural failings to create a fragile and combustible atmosphere.

Much of that atmosphere is generated within France's banlieues and the *cités*. These social housing complexes are heavily caricatured, supposedly designed to banish the poor and the undesirable to isolated slums out of sight for the creative and professional classes inside each city's *périphérique*.

Yet there was a degree of utopian naivety in their creation. Class and ethnic discrimination was not necessarily the aim of these environments. As the scholar Hugo Micheron explains, the enormous Mirail housing complex erected in Toulouse in the 1970s was dreamt of by architects as a self-contained haven for the working classes, a mirror to the pink city's historic centre ville. Over the decades though, projects like Mirail only exacerbated



feelings of alienation. Today Mirail is a symbol of the most visceral expression of the rage against France: jihadism. France has been hit harder by jihadism than any European state. The Mirail alone provided dozens to France's Isis exodus – the largest contingent of any Western country. As with last month's rioting, the allure of jihadism among some French Muslims was put down to socio-economic marginalisation and the rigid demands of *laïcité* (state secularism). France holds a special place in the jihadist imagination, which demands that it be targeted for both atrocities and recruitment. The movement's origins in [Europe](#) stem in large part from the overspill of Algeria's bloody civil war, while Andrew Hussey notes how the former al-Qaeda leader Ayman al-Zawahiri loathed France both for the Napoleonic invasion of Egypt and for providing Israel's nuclear reactor. Later, in 2016, the official Isis spokesman, Abu Muhammad al-Adnani, instructed followers to kill the "spiteful and filthy French" however they could. For European jihadists, France is the country that most closely resembles all they reject: the birthplace of enlightenment ideas, the home of secularism. For some, the objections are a matter of moral taste: it is a land of seduction, of bon vivants, a place where pornstars become celebrities and where breasts are visible from beaches to newsstands. Even the very personification of the Republic, Marianne, bears her flesh. It is no coincidence that the deadly attacks of November 2015 explicitly targeted places of life, enjoyment and mingling between sexes and creeds.

Then there is [the puzzle of Marseille](#), the Mediterranean metropolis which is synonymous with socio-economic woes and risks becoming Europe's first "narco-city". Despite these challenges, the eccentric port city was largely unaffected by Isis radicalisation. This is because to the extent that jihadists were able to recruit in France, it was not necessarily poverty or discrimination that was decisive, but whether a neighbourhood had been targeted and ideologically prepared over the course of decades by other Islamist movements. Marseille's *quartiers* were not.

Islamism is absent from much of the international coverage about the serious problems faced by the French state. Yet it plays a pivotal role in the French domestic debate on the left and right, particularly when it comes to the European offshoots of the Muslim Brotherhood. Unlike al-Qaeda or Isis, this Islamist group's strategy does not involve recruiting large numbers of people – it can take years to actually be inducted into the elite circles of "Brothers". Instead, a small but influential cadre of educated and professional activists uses terrestrial and social media, and political platforms, to disseminate a message which is not necessarily openly Islamist, but which conforms to the Brothers' view of the world. One of the results has been to foster a kind of siege mentality in the hopes of shielding Muslims from the supposed corruption of Western societies. More radical Brotherhood activists have compared the plight of French Muslims to that of Jews in 1930s Europe or, more recently, to the Srebrenica massacre.

Unlike Islamists in other European contexts, French Islamists demonise the entire foundations of the state and society as irretrievably hostile and Islamophobic. This rhetoric filters out to audiences well beyond Islamist sympathisers, but its impact can also be seen among jihadists: one French Isis recruit was surprised to learn that his British counterparts didn't seem to hate their country of origin as much, putting it down to the perceived humiliation inflicted by universalism and *laïcité*, while the ringleader of the 2015 Paris attacks (a Belgian) had content on his phone from a legal NGO presenting France as persecuting Islam.

This campaign has been reinforced by a more fundamentalist brand of Islamism, in France's growing Salafist population. Salafism is a rigid brand of Islam whose followers live their lives according to the example of the first generations of Muslims. Salafi activists employ the principle of loyalty and disavowal, encouraging complete rupture with surrounding unbelief. These are by no means austere religious quietists – in certain neighbourhoods, like Trappes, west of Paris, or again, in Toulouse, Salafi activists muscled out drug gangs, in others they absorbed them. These activists vilify "man-made" French law and institutions, but they also intensely delegitimise other interpretations of Islam.

In 2018 the Salafist following was thought to be up to 50,000 strong, a figure which had grown exponentially in the preceding decade but which does not account for the social control this milieu is able to exercise over countless others in certain neighbourhoods, potentially preventing them from accessing the rights every citizen is afforded by the republic.

Online, Salafi activists are approaching something like hegemony. Young people looking for guidance on their religion are less likely to find the Islam of their parents or grandparents, but they will probably run into Salafism. A leaked government briefing detailed how Salafist and Islamist "influencers" are operating on mainstream social media platforms actively encouraging young people to violate school rules and confront teachers, particularly on matters of secularism and school uniform. Other research shows how Whatsapp chain messages are broadcast to followers to dictate every detail of their day, in particular for women and girls. For the Islamist-Salafist scene, the classroom is a key battleground in their offensive against France, evident in the increasing threats against schoolteachers, and the daylight decapitation of one in October 2020.

There is another movement joining the chorus of delegitimation of France. This is the decolonial thought which intensely divides the French left, most of whom remain attached to republican principles inherited from revolution. Sometimes derided as "woke" and attributed to cultural pollution emanating from American campuses, activists associated with the Indigénistes of the Republic political party in fact make claims about France for which it is hard to find an analogue in Anglo-American discourse: that the French state's treatment of



its non-white contingent is a continuation of colonial policy in Algeria and elsewhere. Hence the term “indigéniste” (native). Colonialism never ended, they claim, it continues today inside metropolitan France. Shortly after the delinquent jihadist Mohamed Merah’s murderous rampage against soldiers and Jewish schoolchildren in 2012, one leading indigéniste activist, Houria Bouteldja, implied the attack was a false flag by the state, or at least comprehensible as a response to the daily humiliation of being a Muslim in France. An example of such humiliation Merah endured was alleged to have endured was the imposition of a moment’s silence for the victims of 9/11 in school. There are obviously significant distinctions between these disparate currents, but the internal borders between them can be porous in ideas and personnel. In different places and different contexts, they have sidelined ideological differences and collaborated. They also converge on common enemies, and their list of grievances against France strongly overlaps: the country’s colonial past, universalism and laïcité as thin veneers for oppression, and the even thinner veneer for hate speech represented by freedom of expression – under which *Charlie Hebdo*’s blasphemous cartoons are permitted.

Alienated young people do not need to have accepted the core tenets of Islamism, Salafism or decolonial thought to have been exposed to and absorbed these grievances. There are unquestionably failures of state and society when it comes to integration, but there are also organised and influential movements actively working against integration and against the existing social contract, a fact which features prominently in French media but is mostly absent in international commentary. We owe it to our neighbour to better understand the complexities of its current malaise – something which cannot be done without accounting for a kind of generational revolt, not just against liberal values and French republican institutions, but against mainstream Muslim institutions too.

Africa records 34 terrorist attacks in July; East and Horn of Africa account for half: Al-Azhar

Source: <https://english.ahram.org.eg/News/506239.aspx>

Aug 08 – Terrorist attacks in July claimed 254 lives, left 126 people injured and two others kidnapped, the observatory said. East Africa and the Horn of Africa came first among African regions in the number of terrorist attacks in July, accounting for 47.1 percent, while the troubled Sahel region came first in the number of victims. [West Africa](#), which faces expanding activity of the Islamic State (IS) and Boko Haram terrorist groups, saw a decline in attacks thanks to the formation of a joint military force by local states to fight terrorism in the region, the observatory noted. All terrorist attacks in West Africa last month took place in Nigeria, killing 48, injuring 11 and kidnapping two. Three attacks took place in Central Africa last month, all in DR Congo, which abounds with valuable resources such as diamonds, copper, gold and fuel.

Such wealth plays a pivotal role in attracting terrorist organizations to the Central African country, the observatory added.

Meanwhile, counterterrorism operations, particularly in Somalia, Burkina Faso and Mali killed 648 terrorists and arrested 307 others, while 28 surrendered. The observatory called for African government forces to manage counterterrorism operations based on a comprehensive security strategy. Such a strategy should be based on improving economic security to stop the spread of terrorist groups which thrive on state vulnerability and destitution.

The Instability of the Sahel: a Military Coup in Niger - An Impetus for the Spread of Radical Islam in the Continent

Dr. David Doukhan
August 2023

 Reichman
University

International Institute for
Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation



Europe's second front: The risks and challenges of the Balkan Peninsula's fundamentalist Islamist organizations

By Peter Almos Kiss

[Source](#)

The first front of the terrorist threat to Europe is sufficiently well known: second or third-generation young Muslims who grew up in the European states, but are alienated from and hate their host societies, and adopted the radical ideology of political Islam. The second front – radical Islam in the western Balkans – has received less attention.

There is a good reason for this: for the time being it is only a distant storm cloud on the horizon. However, it can strike without warning at any moment, like a tropical storm. This essay analyzes the origins of this threat, estimates its extent and seriousness, and recommends policies to prepare for it.

Syria: New Islamic State Attack Indicates Uptick in Group's Activities

Source: <https://worldview.stratfor.com/situation-report/syria-new-islamic-state-attack-indicates-uptick-groups-activities>

US Forces Witness 'dramatic' Drop In Islamic State Activity In Iraq, Syria, Says Pentagon

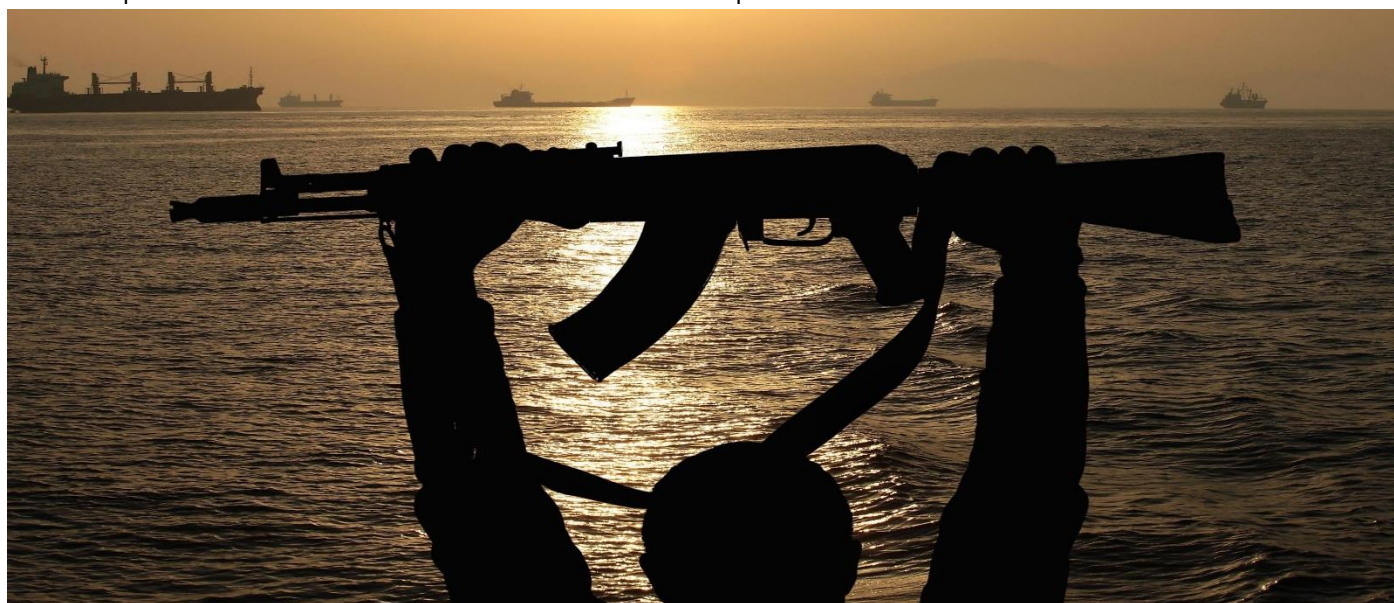
Source: <https://www.republicworld.com/world-news/us-news/us-forces-witness-dramatic-drop-in-islamic-state-activity-in-iraq-syria-says-pentagon-articleshow.html>



EDITOR'S COMMENT: Is it so difficult to decide if the IS is dead or alive?

The World's Most Pirate-Infested Waters

Source: <https://www.worldatlas.com/modern-world/the-world-s-most-pirate-infested-waters.html>



Modern media often depicts piracy as a relic of the past, a nuisance of a bygone era. While it might be true that the scale of piracy that occurred in the Americas in the 17th and 16th centuries is long gone, the practice of high seas robbery is far from over. The world we live in today is home to thousands of instances



of piracy each year. Many regions around the globe are faced with this problem in different ways, but the threat still persists. While we might not see another [Blackbeard](#) anytime soon, in many parts of the world, pirates are no laughing matter.



Malacca Strait

Suspected pirates assemble on the deck of a dhow in waters off western Malaysia, January 2006. Image credit: Chief Information Systems Technician Kenneth Anderson, Public domain, via Wikimedia Commons

The Malacca Strait is a body of water located in the [South China Sea](#) that connects the [Indian Ocean](#) to the [Pacific Ocean](#) and, most importantly, serves Asia as a highway for trade and vital foreign imports like oil and natural gas. More than 120,000 ships pass through the strait each year. Its high level of traffic has attracted the eyes of those looking to get rich quickly through the theft of whatever might be on board or by taking hostages. From 1995 - 2013

nearly 41% of the world's pirate attacks occurred here. All of which had varying levels of success.

Somalia

A combined force of NATO-led counter-piracy troops intercept a suspected Somali pirated vessel. Image credit: Defence Imagery via Flickr.com

If there is one part of the world that is known for its rampant piracy, it is [Somalia](#). Made famous from instances like the capture of the American cargo ship, the Maersk Alabama in 2009, Somali piracy really started to take off during the mid to late 1990s.

Most of the pirates raid international shipping in hopes of capturing crewmembers and ransoming them off to their respective nations. It is not uncommon for the ransom numbers to be incredibly high. These outrageous ransoms have often led to the lengthy imprisonment of many. In one such case, an American journalist was held captive for nearly 1,000 days while negotiating his release. Today the issue of piracy has certainly died down thanks to much tighter security measures employed by large shipping companies as well as a much more noticeable military presence of the American Navy.





South China Sea

Ship crew fitting razor wire around the ship to protect ship from piracy attack while transiting a high risk area.

While the [Malacca Strait](#) might be the most dangerous part of the South China Sea, the rest of the region is no stranger to piracy. Usually consisting of Malaysians and Indonesians, these groups are known to be some of the more violent and dangerous in the world. These groups tend to prey on smaller civilian vessels that do not have the same level of security or protection as the large multinational shipping containers. The small ships are much easier to board as well. The South China Sea saw a 19% increase in pirate activity in 2020, which has worried many surrounding nations. Each nation with a large hand in that region works

tirelessly to try and counter this growing and concerning menace.

Nigeria



A fishing coastal village in Nigeria. Villages like these often become the target of the region's pirates. Editorial credit: Alucardion / Shutterstock.com

Piracy in West African waters has always existed in one way or another for centuries. However, in recent years, there has been a disturbing trend pointing toward pirate groups moving away from targeting



valuable shipping lanes and raiding small coastal villages instead. The number of pirate attacks that took place on the water in 2021 was as low as six, thanks to an increased security effort made by the Nigerian government. However, this lack of activity might have been misleading as raids on villages have increased.

Most of these fishing villages are poor and have little in the way of valuables to be taken. The majority of these raids are done so in the hope of capturing hostages and ransoming them back to their families. While this does not generate the money once available from passing cargoships, the family are easy targets and usually left defenseless.

Benin



A ship sailing in the Gulf of Guinea was rendered pirate-proof with barbed exterior wiring to prevent pirates from climbing up.

Another West African nation, piracy off the coast of [Benin](#), saw an all-time high in 2018 and was capped off with the dramatic boarding of the Norwegian ship the MV Bonita. This ship carried various valuable minerals, such as gypsum and cobalt. However, it was not the minerals that they were after but the crew instead. Nine of the crew members were captured.

As East Africa has cooled down since the middle of the 2010s, it appears that West Africa will likely remain one of the most dangerous shipping routes in the world when it comes to pirates. The Benin government has made considerable efforts to try and deter further acts of piracy, but the threat still remains relatively high. Only time will tell how the various coastal nation of West Africa deals with this blight. It will most likely take the cooperation of all countries within the region to tackle this problem once and for all.



Piracy is far from dead. The theft of valuable goods and especially the kidnapping of sailors remains a huge issue in many of the world's most heavily traveled waterways. It is not likely that these regions will be stuck with pirates forever, but if history has taught us anything, it's that ridding yourself of such a problem is no easy feat. As security gets tighter and military and police presence is increased in these regions, there is hope that the situation can still get under control. But this is often easier said than done.

Islamists burns down Church in Pakistan; Houses of Christians nearby hunted down and attacked

Source: <https://english.janamtv.com/news/world/68905/islamists-burns-down-church-in-pakistan-houses-of-christians-nearby-hunted-down-and-attacked/>



Aug 16 – Ongoing repression against minority communities in Pakistan continues to cause concern, as a group of Islamists targeted a church in Faisalabad. The incident unfolded on Jaranwala Road within Punjab province's Faisalabad district. Tragically, the church was set ablaze and subjected to looting.

The assailants alleged that the church had insulted the Quran and committed blasphemy, fueling their destructive actions. Disturbing footage of the incident has circulated on social media platforms, showcasing the severity of the attack. The Islamists extended their aggression to the neighbouring homes of Christian residents, igniting fires there as well.

Authorities have taken steps to address the situation, initiating a First Information Report (FIR) in connection with the incident, and are said to be working diligently to bring the situation under control, as the actions of the extremists have led to a troubling escalation. Bishop Azad Marshall, a prominent figure within the Christian community, responded to the distressing event. Regrettably, Pakistan has witnessed a concerning pattern of violence directed at minority groups, including Hindus, Sikhs, Christians, and Ahmadis. Instances of atrocities against these communities are regrettably prevalent.

Bishop Azad Marshall highlighted the unjust persecution faced by Christians in Pakistan, where false allegations of Quran desecration are often used as a pretext for targeting them. A few months earlier, temples in Pakistan were also subjected to these same atrocities.

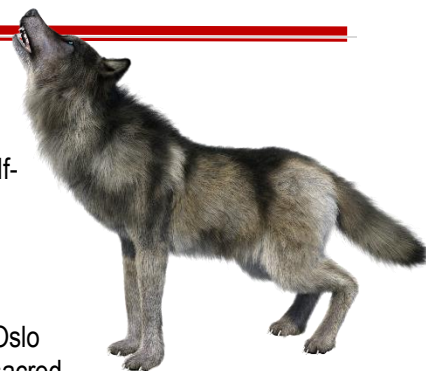
EDITOR'S COMMENT: Yes, the same Pakistanis that we save from drowning in the Greek Aegean Sea and offer them work in our fields via trans-government agreements for land workers ...



Unique Dangers Posed by Lone-Wolf Terrorists

By Jeffrey D. Simon

Source: <https://www.domesticpreparedness.com/articles/unique-dangers-posed-by-lone-wolf-terrorists>



So-called “lone-wolf” terrorists have proved time and again that they can initiate attacks that match and even surpass the death toll and destruction wrought by large, better known, and much better financed terrorist organizations. In Norway, for example, Anders Breivik set off a bomb in Oslo on 22 July 2011 that killed eight innocent people, then traveled to Norway’s Utoya Island and massacred 69 more, many of them teenagers attending a political summer camp.

Meanwhile, in the United States, Major Nidal Malik Hasan, an Army psychiatrist, is accused of opening fire at Fort Hood, Texas, on 5 November 2009 – killing 13 people and wounding 32 others in the worst terrorist attack ever to take place on a U.S. domestic military installation. More than three years later, he is still awaiting trial (which is scheduled to begin this May).

Not quite eight years earlier, shortly after the 9/11 attacks, an anonymous attacker (believed by some to be a government microbiologist at Fort Detrick, Maryland, who later committed suicide) sent letters filled with anthrax spores to several Congressional offices and media news rooms, creating a new crisis atmosphere about the potential threat of a bioterrorism attack.

Creative, Empowered & Elusive Predators

Despite their usual anonymity and lack of “partners,” lone-wolf terrorists share a number of typical characteristics – the first and perhaps most dangerous of which is that, because there is no group decision-making process involved that might stifle individual creativity, lone wolves are free to carry out any type of attack they might think of, with little or no fear of the likely consequences. This independence has led to some of the most innovative attacks in terrorism history. For example, lone wolves were responsible for the first U.S.:

- [Vehicle bombing](#) – a horse-drawn wagon filled with dynamite was detonated in New York City in 1920, killing more than 30 and injuring several hundred others;
- [Major midair plane bombing](#) – a bomb that was packed in a passenger’s luggage exploded over Colorado in 1955, killing 44;
- [Airplane hijacking](#) – a National Airlines plane was hijacked and diverted from Florida to Cuba in 1961 (the crew and passengers were not harmed); and
- [Anthrax letter attacks](#) – mentioned earlier, killing five people and sickening 17 others.

A second “typical” characteristic about lone wolves is that they have little or no constraints limiting their level of violence. They are seldom if ever concerned about alienating supporters (as at least some terrorist groups might be), and they do not seem to fear a potential government crackdown following an attack. This latter trait makes them prime candidates to use weapons of mass destruction, specifically including biological or chemical agents, which usually are available on the open market.

A third generalization is that it is extremely difficult to identify and/or capture lone wolves. There are usually no communications to intercept and/or members of a group to arrest and interrogate about potential plots. This can be seen most obviously in the case of Theodore Kaczynski, the infamous “Unabomber” who was responsible for 16 bombings that killed three people and injured 23 more – but was able to elude law enforcement for almost 18 years (1978-1996). He was finally captured in early April of 1996 and is now serving a life sentence without parole.

A Carefully Planned Attack

Lone wolves can also be quite devious in planning a terrorist operation. A prime example is Eric Rudolph, an antiabortion lone wolf who set off a bomb at the 1996 Summer Olympic Games in Atlanta, Georgia, that killed one person and injured more than 100 others (a cameraman also died from a heart attack as he ran to cover the incident). He later bombed two abortion clinics, killing one person and, in an alleged attempt to kill homosexuals – a lesbian nightclub. At the scene of some of his attacks, he also planted second bombs that were set to explode after police and other emergency responders had arrived to deal with the initial explosions. In one case, police discovered the second bomb and defused it, but in another case the second bomb went off as planned, injuring several people, including police officers. Rudolph was finally arrested in 2003 and is now serving a life sentence without parole.

Breivik, the Norwegian anti-Islamic lone-wolf terrorist, apparently set off the bomb in Oslo primarily to divert the attention of law enforcement personnel so he could then travel to Utoya and kill as many as possible of the young people attending the summer camp there. He wore a policeman’s uniform and told camp



officials – who had already heard the news about the Oslo bombing – that he was there to protect the campers. Breivik then walked to the area where the campers' tents were located and began shooting as many people as he could find.

Following the Norway shootings, one police official stated that Breivik “just came out of nowhere.” Another claimed that there had been “no warning lights” that Breivik was a terrorist. Their statements seem to imply that there is little if anything that can be done to prevent lone-wolf terrorist attacks. That is not quite the case, though. On the contrary, Breivik had actually made his presence known by using the Internet to purchase large quantities of ammonium nitrate fertilizer – which he later used to build the car bomb that he set off in Oslo. Norwegian authorities were initially suspicious of Breivik's online purchase, but erroneously concluded that the fertilizer was in fact intended for agricultural use on a farm that Breivik had rented.

Breivik also advocated violence a number of times in a 1,500-page “manifesto” that he posted online shortly before his murderous attacks. “Once you decide to strike,” he wrote, “it is better to kill too many than not enough, or you risk reducing the desired ideological impact of the strike.” Like many other lone wolves, Breivik therefore did not, as suggested, simply “come out of nowhere.”

Preventive Strategies

Through a mix of creative and innovative strategies, it is in fact possible to reduce the likelihood of a lone wolf succeeding in an attack. Such strategies include: (a) improving detection devices in post offices and other facilities to help identify, in advance, package bombs or letters containing anthrax spores; (b) expanding the number and use of closed circuit television (CCTV) cameras in public buildings and other settings; (c) accelerating the further development of computer technology that can recognize “suspicious” behavior in public places – and instantly forward the information to a control center where the decision whether or not to notify the police would be made; (d) further advances in biometrics, including the use of gait analysis to determine the speed, stride, and other characteristics of a person's walk to determine if that person may be carrying a bomb or other weapon; and (e) the analysis of facial expressions to predict hostile intent (an obviously difficult task).

Another potentially important strategy for identifying lone wolves before they strike is to monitor the Internet – but without violating the civil liberties of law-abiding citizens – to identify those who are visiting extremist chat rooms, purchasing bomb-making materials and/or other suspicious items online, or posting ominous threats and manifestos.

In short, the lone-wolf threat seems likely to grow in the coming years. The current age of terrorism is one in which any number of people can become knowledgeable, empowered, and radicalized via the Internet and other means. Today there is also the possibility that at least some of the insurgents from the wars in Iraq and Afghanistan might later take their expertise to other regions and launch individual attacks. It is therefore important that governments and societies be as committed to dealing with the lone-wolf terrorist threat as they have been to the threat posed by al-Qaida and other terrorist groups.

Jeffrey D. Simon is an internationally recognized author, lecturer, and consultant on terrorism and political violence. He is president of Political Risk Assessment Company Inc., and a visiting lecturer in the Department of Political Science at UCLA. His most recent book, *Lone Wolf Terrorism: Understanding the Growing Threat*, was published in 2013. A former RAND analyst, he has conducted research and analysis on terrorism for more than 25 years. His writings on terrorism, political violence, and political risk have appeared in many publications, including the *Journal of the American Medical Association*, *Foreign Policy*, and the *New York Times*. His website can be found at <http://www.futureterrorism.com>. He earned a B.A. in History from the University of California at Berkeley, an M.A. in Political Science from Indiana University, and a Ph.D. in Political Science from the University of Southern California.

Our Very Own No-Go Zone - San Francisco

By Sam Faddis

Source: <https://andmagazine.substack.com/p/our-very-own-no-go-zone-san-francisco>

Aug 17 – “In light of the conditions at the [federal building] we recommend employees ... maximize the use of telework for the foreseeable future,” [Cheryl Campbell](#), HHS Assistant Secretary for Administration.

That is a portion of a [memo](#) sent out to all federal employees in San Francisco days ago. Crime is so bad in downtown San Francisco where the federal building in question is located that your government no longer considers it safe to have them come to work. One of America's greatest cities is now a no-go zone on par with the worst hellholes on the planet.

In an open letter to city leaders recently, the owner of one of San Francisco's most historic businesses, Gump's luxury department store, laid out clearly what has happened to the city under Democratic leadership.

In a full-page ad published in the *San Francisco Chronicle*, Gump's CEO John Chachas [said](#) in part.





"Gump's has been a San Francisco icon for more than 165 years. Today, as we prepare for our 166th holiday season at 250 Post Street, we fear this may be our last because of the profound erosion of this city's current conditions."

"San Francisco now suffers from a 'tyranny of the minority' —behavior and actions of the few that jeopardize the livelihood of the many. The ramifications of COVID policies advising people to abandon their offices are only beginning to be understood. **Equally devastating has been a litany of destructive San Francisco strategies, including allowing the homeless to occupy our sidewalks, to openly distribute and use illegal drugs, to harass the public, and to defile the city's streets.**"

"Such abject disregard for civilized conduct makes San Francisco unlivable for its residents, unsafe for our employees, and unwelcoming to visitors from around the world."

The streets and sidewalks of downtown San Francisco are open sewers. Homeless people and drug addicts defecate openly anywhere they want. The city's response has been to launch an app called [Snapcrap](#) (I did not make that up). This lets city residents take pictures of human feces and send the pictures to the city which will then dispatch a team to clean up the mess.

San Francisco has one of the highest [crime rates](#) in America. It is more dangerous than 98% of the communities in California. Homicides are up 20.7% since the beginning of the year, while robberies and motor vehicle thefts are up 14% and 13%, respectively, according to San Francisco police data.

[Nordstrom's](#) just pulled out of San Francisco. Target has its entire product range locked up to prevent shoplifting. Whole Foods also appears to be pulling out. These are not isolated cases. Everyone is getting out.

There were 203 retailers open on the streets surrounding San Francisco's historic Union Square in 2019. By May 2023, only 107, or 53%, [were still in business](#).

The entire Westfield Mall in downtown San Francisco has shut its doors. The owners of the mall left no doubt as to the reason they were closing up shop.

"A growing number of retailers and businesses are leaving the area due to the unsafe conditions for customers, retailers, and employees, coupled with the fact that these significant issues are preventing an economic recovery of the area," a mall spokesperson said.

Employees at Target which now keeps its entire inventory under lock and key had [this](#) to say about shoplifting in talking to local news recently.

"Every 10 minutes you see it," another worker said who also did not wish to be named. "Look in some corner of the store, and you'll see people shoveling stuff into a bag—food, cosmetics."





Another worker who also spoke on the condition they not be named said lipstick and nail polish were regularly stolen in handfuls. Yet another staff member reported regularly seeing homeless people taking food and sometimes eating it in the store. Tin foil is also taken in large quantities because it is used to smoke fentanyl. Congressman Kevin Kiley of California perhaps summed all of this up best in a recent [Tweet](#). "Crime in San Francisco is so out-of-control that employees at the Federal Building are being told to stay home. The building is home to Nancy Pelosi's office, as well as the U.S. Departments of Labor and Health & Human Services. HHS, which is headed by former CA Attorney General Xavier Becerra, told workers to "maximize the use of telework for the foreseeable future" because of "conditions" around the building. The SF Chronicle described those conditions: "Dozens of dealers routinely plant themselves on, next to or across the street from the property, operating in shifts as users smoke, snort or shoot up their recent purchases." In recent months, San Francisco's decline has reached a point of total collapse. Whole Foods, Nordstrom, T-Mobile, Saks, and Anthropologie all announced their departure because of crime. Newsom even claimed he was sending in the National Guard. If California offers a preview of where our country is headed, San Francisco offers an even starker warning. This is where failed policies, radical politics, and public corruption are in their most advanced stage – and where residents are most rapidly fleeing." The world is filled with hellholes and no-go zones. We have one right here in America now. It's called San Francisco.

EDITOR'S COMMENT: Perhaps a portion of the tons of money given to the Ukrainian proxy war could help ease the situation back home.

Norway's far-right mass killer Breivik sues state over prison isolation

Source: <https://www.aljazeera.com/news/2023/8/19/norways-far-right-mass-killer-breivik-sues-state-over-prison-isolation>

Aug 19 – [Norwegian mass killer Anders Behring Breivik](#) is suing the state for allegedly violating his human rights due to being held in "extreme" isolation, and has filed another application for parole, his lawyer said.

A neo-Nazi, Breivik killed 77 people, most of them teenagers, in shootings and a bombing attack in Norway's worst peacetime atrocity in July 2011.

Breivik, now 44, [is serving Norway's longest sentence, 21 years](#), which can be extended if he is still considered a threat.



“He’s suing the state because he has been in an extreme isolation for 11 years, and has no contacts with other people except his guards,” Breivik’s lawyer Oeystein Storrvik told the Reuters news agency on Friday.

Audacity of a thousand monkeys!



**3.3 months
per citizen
murdered**

“He [Breivik] was moved to a new prison last year, and we hoped that there would be better conditions and that he could meet other people,” Storrvik added.

Norwegian daily Aftenposten was the first to report about the case earlier on Friday.

In 2017, Breivik lost a human rights case when an appeals court overturned a lower court verdict that his near-isolation in a three-room cell was inhumane.

Last year, a Norwegian court also rejected his parole application, saying he still posed a risk of violence.

Storrvik said he expected the Oslo district court to hear the lawsuit next year.

Afghanistan Reemerging as a Terrorism Incubator

By Jeff Seldin

Source: <https://www.voanews.com/a/afghanistan-reemerging-as-a-terrorism-incubator-/7230546.html>

Aug 18 – Two years after the Taliban takeover of Afghanistan, there is growing consensus that the country is again devolving into a hotbed of terrorism activity that is already beginning to affect the region, if not yet capable of reaching the West.

Some of the more damning assessments have come from a United Nations sanctions monitoring team, which warned in a report in June that the Taliban “have not delivered on the counter-terrorism provisions” in the Doha Accords, the agreement that paved the way for the withdrawal of U.S. forces.

Instead, the report, based on U.N. member state intelligence, warned that “a range of terrorist groups have greater freedom of maneuver under the Taliban de facto authorities.”

The various groups “are making good use of this,” the report added. “The threat of terrorism is rising in both Afghanistan and the region.”





A man walks past the site of a suicide attack along the roadside in Faizabad district of Badakhshan province on June 6, 2023.

Some estimates put the number of terrorist groups in Afghanistan at about 20, and even some of Afghanistan's neighbors have raised concerns.

Pakistan, for instance, has repeatedly pointed to a [surge of terrorism-related deaths](#), many concentrated along its border with Afghanistan.

The Taliban have rejected such allegations.

Earlier this month, a Taliban official touted a ruling by supreme leader Hibatullah Akhundzada forbidding cross-border attacks on Pakistan.

Chief spokesman Zabihullah Mujahid went even further, telling VOA that Taliban fighters had essentially put an end to the terrorist threat in Afghanistan.

"Those found guilty of indulging in such activities will be brought to justice and punished in line with our legal system," he said, saying the Islamic State terror group's Afghan affiliate, known as IS-Khorasan or ISIS-K, had been "decimated" by Taliban counterterrorism operations. [taliban-to-mark-august-15-victory-day-against](#)

The Taliban have also gotten a public show of support from U.S. President Joe Biden, who caused a stir last month July when he indicated the Taliban had been true to their word.

"Remember what I said about Afghanistan? I said al-Qaida would not be there. I said it wouldn't be there. I said we'd get help from the Taliban," Biden said in response to a question about the frenzied U.S. withdrawal from Afghanistan.

"What's happening now? What's going on?" Biden said. "Read your press. I was right."

A U.S. official who spoke to VOA on the condition of anonymity said Biden was referring in part to the Taliban's role in [killing the leader of the Islamic State terror cell](#) that was behind an August 2021 bombing at Kabul airport. The attack killed 13 U.S. troops and about 170 Afghan civilians.

Other U.S. officials remain wary, though, pointing to long-term plans by both al-Qaida and IS-Khorasan, each of which has the intent, if not the capability, to attack U.S. and Western targets.

"Our intelligence is degraded," the commander of U.S. Central Command, General Michael "Erik" Kurilla, told the Senate Armed Services Committee in March when asked about the military's ability to track the two terror groups.

"I believe we can see the broad contours of an attack [plot]," he said. "Sometimes we lack the granularity to see the full picture."

Some former officials wonder how long it will be before al-Qaida or IS-Khorasan is able to break through.



“Neither al-Qaida nor [IS] in Afghanistan currently has the capability to strike U.S. interests but I don’t agree we can assume that beyond the short term,” Edmund Fitton-Brown, a former senior U.N. counterterrorism official and sanctions monitoring team coordinator, said during a recent webinar hosted by the Washington-based Foundation for Defense of Democracies.

Other analysts have expressed similar concerns.

“Afghanistan seems eerily reminiscent to pre-9/11 Afghanistan, with the number of groups that are allegedly active,” said Colin Clarke, director of research at the global intelligence firm The Soufan Group.

“Terrorist groups thrive and indeed flourish amid instability. And that’s exactly what we have here,” he told VOA in June.

Below is a look at the Taliban and the major terrorist organizations now operating in Afghanistan, and how they have fared in the two years since U.S. and coalition forces left the country.

Taliban

Since its emergence in 1994, the Taliban movement, which calls itself the Islamic Emirate of Afghanistan, has been led by an emir, a central figure appointed for life by a religious council of Taliban leaders.

Like his two predecessors, current Emir Hibatullah Akhundzada leads a reclusive life in southern Afghanistan’s Kandahar province, surrounded by his inner circle.

June’s U.N. sanctions monitoring team report said Akhundzada “has become more assertive, projecting control and authority by appointing loyalists to positions of power” while growing ever more conservative.

But Akhundzada’s assertiveness may belie growing frictions within the movement as rumors swirl about his failing health after multiple bouts with COVID-19.

The U.N. report said the movement appears split with one faction, based in Kandahar, loyal to Akhundzada, and a second Kabul-based faction led by Interior Minister Sirajuddin Haqqani, acting Defense Minister Mullah Mohammad Yaqub Omari and intelligence chief Abdul-Haq Wassiq.

Haqqani, who leads the semi-autonomous Haqqani network, also is said to be feuding with other Taliban officials, including First Deputy Prime Minister, Mullah Baradar, as the two jockey for power and influence.

There are also questions about the Taliban’s armed forces.

The most recent estimates from U.S. intelligence agencies and U.N. member states are a year old and put the number of Taliban fighters between 58,000 and 100,000, with numbers fluctuating according to the time of year and battlefield conditions.

A U.N. report from May of last year suggested the Taliban were seeking to increase the size of their standing military to as many as 350,000 fighters and even establish a nascent air force, with some 40 operational aircraft captured from the former U.S.-backed Afghan military.

And despite claims of success against IS-Khorasan, there is evidence that the Taliban are struggling to eradicate the group.

“The Taliban have quietly reached out requesting intelligence and logistical support to fight ISIL-K, offering itself as a counterterrorism partner,” the most recent U.N. report on Afghanistan said, using another acronym for the Islamic State group’s Afghan affiliate.

The same report, though, questioned the Taliban’s promises to distance itself from traditional terrorist allies, saying the Taliban link with al-Qaida and Tehrik-e-Taliban Pakistan “remains strong and symbiotic.”

Moreover, there have been indications that some al-Qaida members are well integrated into Taliban-run Afghan military units.

Some analysts, however, caution that the Taliban’s grip on power should not be underestimated.

“The Taliban holds all the cards,” said Bill Roggio, a senior fellow with the Foundation for the Defense of Democracies.

“The Taliban has near total domination of the security situation,” he said during a recent webinar. “Groups like the Islamic State Khorasan Province, which a lot of people think is the real threat that emanates from Afghanistan — it’s a minor player.”

Islamic State Khorasan Province

IS-Khorasan is a sworn enemy of both the Taliban and al-Qaida, which has deep and long-standing ties to the Taliban leadership. But IS-Khorasan also benefits from the Taliban takeover of Afghanistan.

According to a June report by the U.N. sanctions monitoring team, IS-Khorasan has exploited both the Taliban’s inability to establish control over remote areas and growing dissatisfaction with Taliban rule.

“Attacks against high-profile Taliban figures raised [IS-Khorasan] morale, prevented defections and boosted recruitment, including from within the Taliban’s ranks,” the U.N. report said.

The increase in recruitment, at least according to intelligence shared by U.N. member states, is significant.

Whereas IS-Khorasan was thought to have between 1,500 and 4,000 fighters at this time last year, the new estimates put the IS affiliate’s force strength at up to 6,000 members.



The intelligence also suggests IS-Khorasan has vastly expanded its footprint.

Once mostly limited to remote parts of Kunar, Nangarhar and Nuristan provinces, in the country's northeast, along the Pakistan border, IS-Khorasan is now thought to have strongholds or camps in at least 13 of the country's 34 provinces as well as a network of sleeper cells that can reach Kabul and beyond.

A subsequent U.N. report, also based on member state intelligence, further warned IS-Khorasan may be building up its ability to threaten the region and even Europe, and that the group "is becoming more sophisticated in its attacks against both the Taliban and international targets."

Not everyone agrees. U.S. officials in particular have pushed back hard against the U.N. assessment.

The estimate that IS-Khorasan boasts 4,000 to 6,000 members "is thousands more than the [U.S.] intelligence community has assessed or assessed there to be," a senior U.S. official told VOA.

The official, speaking on the condition of anonymity in order to discuss sensitive intelligence, further refuted some of the more dire warnings of IS-Khorasan's ability to pose a threat far beyond Afghanistan.

"Our view is that ISIS-K has not closed that ambition-capacity gap that it very much hoped to close after the U.S. departure, and indeed has faced some very real setbacks and some very concerted pressure from the Taliban," the official said.

Officials familiar with the June U.N. report told VOA they are convinced there are some significant disagreements on the state of IS-Khorasan within the U.S. government. Some U.S. officials have publicly stated their concerns.

In March, U.S. Central Command's General Michael Kurilla told lawmakers that IS-Khorasan "can do an external operation against U.S. or Western interests abroad in under six months with little to no warning.

A week earlier, Lieutenant General Scott Berrier, chief of the Defense Intelligence Agency, told lawmakers, "It's a matter of time before they may have the ability and intent to attack the West."

Earlier this year, Christine Abizaid, director of the National Counterterrorism Center, called IS-Khorasan the "threat actor I am most concerned about."

One area in which officials from the U.S. and other countries seem to be in agreement is that there are questions about IS-Khorasan's path moving forward.

In June, intelligence officials in Pakistan and Afghanistan told VOA that the IS-Khorasan leader, Sanaulah Ghafari, was killed by Taliban forces in a mountainous region of Afghanistan's Kunar province.

However, neither U.S. officials nor officials from other U.N. member states who have provided intelligence on IS-Khorasan have been able to confirm that Ghafari, also known as Shahab al-Muhajir, is in fact dead.

Al-Qaida core

Intelligence assessments from a number of countries shared with the U.N. in the months after the Taliban takeover of Afghanistan suggested al-Qaida was enjoying "a significant boost" from the withdrawal of U.S. forces.

Recent intelligence assessments from the U.N. suggest nothing has changed.

The link between the Taliban and al-Qaida "remains close and symbiotic, with Al-Qaida viewing Taliban-administered Afghanistan a safe haven," the U.N. sanctions monitoring team said in its June report.

While al-Qaida appears to be maintaining a low profile, "there are indications that Al-Qaida is rebuilding operational capability," the report warned, pointing to new training bases in Badghis, Helmand, Nangarhar, Nuristan and Zabul provinces.

The number of al-Qaida core personnel is also thought to have grown significantly, from just several dozen members shortly after the Taliban takeover to between 30 and 60 senior officials and another 400 fighters and some 1,600 family members.

Intelligence shared by U.N. member states further warns that al-Qaida members are being given roles within the Taliban's security forces and that al-Qaida fighters are even benefiting from so-called Taliban welfare payments.

As with IS-Khorasan, the assessments of many U.N. member states clash with intelligence being shared by the U.S.

"These numbers are wildly out of whack with the best estimates of the U.S. intelligence community, and indeed the best estimates of our partners and allies," a senior administration official told VOA in June, speaking on the condition of anonymity.

In contrast to the U.N. estimate of 30 to 60 al-Qaida core officials residing in Afghanistan, the senior U.S. official told VOA: "There was one ... and we dealt with it," referring to the July 30, 2022, drone strike that killed al-Qaida leader Ayman al-Zawahiri.

Al-Qaida "simply has not reconstituted a presence in Afghanistan since the U.S. departure in August 2021," the official added, asserting that it is unlikely attempts by al-Qaida to establish training camps in Afghanistan, as the U.N.'s June report claimed, would go unnoticed by the U.S. and its allies and partners.

The disagreement between the U.S. and other countries keeping watch over al-Qaida in Afghanistan goes even further.



Some U.N. member states assert that Afghanistan has been hospitable enough to host visits by al-Qaida core's de facto leader, Saif al-Adel, and presumed al-Qaida No.2, Abd al-Rahman al-Maghrebi, [both of whom are based in Iran](#).

One U.N. member state has suggested that al-Adel has decided to make Afghanistan his new base of operations.

Senior U.S. officials have rejected such claims.

"We do not have indications that the likes of Saif al-Adel have traveled to Afghanistan," according to the senior U.S. official who spoke to VOA in June. "Al-Qaida, as far as we can tell, and we look pretty closely, they do not see Afghanistan right now as a permissive or hospitable environment in which to attempt to operate."

Other U.S. officials have played down the threat al-Qaida in Afghanistan currently poses to the U.S. homeland.

"We have achieved what I would call [a] suppressive effect," Department of Homeland Security Counterterrorism Coordinator Nicholas Rasmussen said in March.

Additionally, some countries' intelligence services and some analysts suggest the long-standing ties between al-Qaida and the Taliban may be preventing al-Qaida from growing into a dire threat.

"In the case of a stable Afghanistan, the al-Qaida core might consider relocating to other operational theatres, to avoid offending their Taliban hosts," the U.N. said in its June report. "Member States suggested that, in the mid- to long term, Al-Qaida would be strengthened by increased instability within Afghanistan."

Al-Qaida in the Indian Subcontinent

Just as with al-Qaida core, there are divergent views on the status of al-Qaida in the Indian Subcontinent, or AQIS, one of al-Qaida's key offshoots.

In January, the U.S. National Counterterrorism Center's Abizaid, called AQIS "defunct."

Months earlier, an assessment from the U.S. Defense Intelligence Agency [said AQIS had maybe 200 members still in Afghanistan](#).

The most recent assessment by U.N. member states suggests AQIS is not dead, but that its footprint in Afghanistan has somewhat lessened, from up to 400 fighters in 2022 to up to 200 fighters at present.

The U.N. assessment places AQIS fighters in Kandahar, Nimruz, Farah, Helmand and Herat provinces.

Other than the number of estimated fighters, there are lingering questions about AQIS' viability as a terrorist entity.

A U.S. intelligence assessment that was declassified last year called AQIS "largely inactive," with many of its members focused more on media production than on plotting terror attacks against the West. Some U.S. counterterrorism officials wondered whether AQIS might eventually be absorbed by the Taliban.

One U.N. member state said its intelligence suggested AQIS may be preparing to try to spread into Bangladesh, Indian-administered Jammu and Kashmir, and Myanmar.

But the same intelligence agency warned some AQIS members appear ready to switch allegiance and join with IS-Khorasan.

Other U.N. member states believe AQIS is working more actively with Tehreek-e-Taliban Pakistan, which like al-Qaida has a strong relationship with the Taliban.

AQIS fighters, including native Afghans and fighters from Bangladesh, Pakistan, India and Myanmar, were said to have fought alongside the Taliban against the U.S.-backed government prior to its collapse.

AQIS leader Osama Mehmood, and AQIS deputy leader Atif Yahya Ghouri, are both thought to reside in Afghanistan.

Haqqani network

The Haqqani network is widely considered to be the most influential and strategically successful extremist group in the region.

Prior to the Taliban takeover of Afghanistan, the Haqqani network was seen as nominally loyal to the Taliban, with some countries describing it as "semi-autonomous," noting it maintained ties with both al-Qaida and IS-Khorasan.

Since the Taliban takeover, the relationship has grown somewhat more complicated, as the network's leader, Sirajuddin Haqqani, is also the Taliban's interior minister.

The network's ties to al-Qaida appear to remain entrenched, as former al-Qaida leader Ayman al-Zawahiri was staying at a guest house linked to Sirajuddin Haqqani when al-Zawahiri was killed in a U.S. drone strike in July 2022.

But tensions with the Taliban have emerged.

In February, Sirajuddin Haqqani publicly criticized Taliban supreme leader Hibatullah Akhundzada for "monopolizing" power.

Some U.N. member states have advised in recent reports that Sirajuddin Haqqani may be trying to build support, possibly to undermine Akhundzada and replace him with Mullah Yaqub, the son of Taliban founder Mullah Omar.

Previous U.N. intelligence assessments warned the Haqqani network a "highly skilled core of members who specialize in complex attacks and provide technical skills, such as improvised explosive device and rocket construction."



The Haqqani network is also thought to oversee a force of between 3,000 and 10,000 traditional armed fighters in Khost, Paktika and Paktiya provinces, as well as at least one elite unit. The network also controls security in Kabul and across much of Afghanistan. Newer intelligence assessments shared by U.N. member states suggest the Haqqani network is increasingly getting involved in the production and distribution of methamphetamine and synthetic drugs.

For much of its existence, the group was based in Pakistan's tribal areas as it operated across the border in Afghanistan.

The Haqqani network has been accused of perpetrating some of the deadliest and most sophisticated attacks against U.S., Indian and former Afghan government targets in Afghanistan since 2001. They are also believed to have strong ties to Pakistani intelligence. The U.S. designated the Haqqani network a foreign terrorist organization in 2012, and Sirajuddin Haqqani has a \$10 million bounty on his head from the U.S. government.

Intelligence gathered in recent years from some U.N. member states said the Haqqani network has at times acted as a go-between for the Taliban and IS-Khorasan, and that with the tacit approval of the Taliban, they directed the Islamic State affiliate to attack the now defunct U.S.-backed Afghan government.

With U.S. forces no longer in Afghanistan, it appears the Haqqani network has ceased to nurture ties with IS-Khorasan.

Tehreek-e-Taliban Pakistan

Most active on the 2,640-kilometer border between Afghanistan and Pakistan, Tehreek-e-Taliban Pakistan, or TTP, is an insurgent group involved in terrorist attacks in both countries.

U.N. intelligence estimates put the number of TTP fighters between 4,000 and 6,000, up from an estimate of 3,000 to 4,000 fighters last year.

The group's stated objectives are to end the Pakistani government's control over the Pashtun territories of Pakistan and to form a strict government based on Shariah, Islamic law.

Intelligence shared by member states with the U.N. finds TTP, like al-Qaida, maintains a "strong and symbiotic" relationship with the Taliban that is "unlikely to dissipate."

Recent intelligence assessments suggest TTP has been emboldened by the Taliban takeover of Afghanistan and is looking to reestablish control of territory in Pakistan.

Although TTP's ambitions appear to have been boosted by a reunification with several splinter groups, a recent U.N. report cautioned that "TTP capability is assessed as not matching its ambition, given that it does not control territory and lacks popular appeal in the tribal areas."

Following talks between Pakistani and Taliban officials earlier this month ((August)), Taliban leader Hibatullah Akhundzada ruled cross-border attacks by the TTP on Pakistan to be "haram" or forbidden under Islam.

In the meantime, there is some evidence to suggest TTP fighters have been getting training and ideological guidance from al-Qaida, and some countries have voiced concern that TTP might evolve into an umbrella organization for foreign fighters.

U.S. forces in Afghanistan and the Pakistani military have killed or captured several TTP leaders over the past two decades.

The group's current leader, Noor Wali Mehsud, has publicly declared allegiance to the Afghan Taliban leader.

The Islamic Movement of Uzbekistan

The Islamic Movement of Uzbekistan, was founded in the late 1990s with help and financial support from al-Qaida founder Osama bin Laden. Several IMU leaders have served as part of the al-Qaida hierarchy. The group has sought to replace the Uzbek government with a strictly Islamic regime.

IMU launched its first attack in February 1999 by simultaneously detonating five car bombs in Tashkent, the Uzbek capital. The group is also believed to have carried out attacks in Afghanistan and Pakistan.

In 2015, then-IMU leader Usman Ghazi and other senior members of the group shifted allegiance from al-Qaida to the rival Islamic State group. The move did not sit well with Taliban leaders, who launched a major military campaign against Ghazi, killing him and nearly wiping out the group.

According to U.N. member states, IMU has somewhat rebounded under the leadership of a new emir, Mamasoli Samatov, and now has anywhere from 150 to 550 fighters.

Khatiba Imam al-Bukhari

Khatiba Imam al-Bukhari was founded in 2011 by fighters who left the IMU and fought against the U.S.-backed Afghan government alongside the Taliban.

The group is led by Dilshod Dekhanov, a Tajik national.



Khatiba Imam al-Bukhari is also thought to have about 80 to 100 or so fighters across Badghis, Badakhshan, Faryab and Jowzjan provinces.

Previously, it was also thought to have dozens of fighters in Syria, possibly in Latakia or Idlib governorates.

According to the U.N., Khatiba Imam al-Bukhari 's numbers in Afghanistan had been growing due to the successful recruitment of locals and due to money from the Taliban and funds acquired via its leadership in Syria.

Islamic Jihad Group

According to intelligence assessments shared with the U.N., the Islamic Jihad Group has been considered "the most combat-ready Central Asian group in Afghanistan," and is known for expertise in "military tactics and the manufacture of improvised explosive devices."

The group is led by Ilimbek Mamatov, a Kyrgyz national. The group's second-in-command, Amsattor Atabaev, hails from Tajikistan. U.N. member states assess that it now has between 200 and 250 fighters.

Islamic Jihad Group fighters have operated across Badakhshan, Baghlan and Kunduz provinces, some having fought alongside Taliban forces.

Eastern Turkistan Islamic Movement/Turkistan Islamic Party

The Eastern Turkistan Islamic Movement, or ETIM, also known as the Turkistan Islamic Party, was first established in the Xinjiang region of China, with its first reported attack in 1998.

After 2001, it began getting help from both al-Qaida and the Taliban, and it has been consistently active in Afghanistan since 2007. According to intelligence estimates provided by U.N. member states, ETIM has between 300 and 1,200 fighters in Afghanistan training for and plotting attacks on Chinese targets.

A U.N. report from June warned ETIM "continues to recruit fighters of various nationalities in an effort to internationalize" and that it "actively expanded the scope of its operations and built operational bases and armories in Baghlan province."

One U.N. member state warned that ETIM "formulated a long-term plan to train young fighters, with hundreds already trained."

Intelligence shared with the U.N. suggested the Taliban last year relocated many ETIM fighters from Badakhshan province, which borders China, "to both protect and restrain the group." But more recent intelligence estimates from one U.N. member state cautioned ETIM was working to revive terrorist activities in Xinjiang.

It is thought that ETIM members have been given Afghan passports and identity papers.

In addition to the group's close ties to the Taliban and al-Qaida, it has been reported to collaborate with other groups in Afghanistan, including TTP and Jamaat Ansarullah, an ethnically Tajik faction of the IMU.

There is also evidence to suggest that ETIM has developed closer ties with IS-Khorasan, with some ETIM fighters joining IS-Khorasan operations.

Jamaat Ansarullah

According to recent U.N. member state intelligence, Jamaat Ansarullah remains closely affiliated with al-Qaida and also the Taliban. The group's 100 to 250 fighters are led by Asliddin Khairiddinovich Davlatov, with some U.N. members warning up to 30 have been issued Afghan passports.

U.N. member states also warned that JA fighters joined Taliban forces in several offensives against the anti-Taliban National Resistance Front.

Lashkar-e-Islam

Lashkar-e-Islam was founded in the Khyber district of Pakistan in 2004 but relocated to Afghanistan's Nangarhar province in 2014, following clashes with the Pakistani military.

Since coming to Afghanistan, Lashkar-e-Islam has clashed with IS-Khorasan, with major skirmishes taking place in 2018 as the two groups fought for control of territory and resources.

Hezb-e-Islami

Hezb-e-Islami, or "Party of Islam," was founded in 1976 by former Afghan Prime Minister Gulbuddin Hekmatyar.

The group shares much of the same ideology as the Taliban, and its fighters have assisted the Taliban in the past.

In 2015, Hekmatyar ordered his followers to help IS fighters in Afghanistan but never pledged allegiance to IS.



Hezb-e-Islami was known to target U.S. forces in Afghanistan, carrying out a series of attacks on U.S. and coalition forces in from 2013 to 2015.

Lashkar-e-Taiba

Lashkar-e-Taiba, or "Army of the Pure," was founded in Pakistan in the 1990s and is sometimes known as Jamaat-ud-Dawa. Led by Hafiz Muhammad Saeed and aligned with al-Qaida, the group is perhaps best known for carrying out the November 2008 attacks in Mumbai, India, that killed more than 160 people.

Intelligence assessments shared with the U.N. said the group's leadership met with Taliban officials in January 2002 and was operating training camps in Afghanistan, having previously sent fighters to Afghanistan to assist the Taliban.

Saeed, who has been in and out of Pakistani custody, was found guilty in Pakistan in April 2022 on charges related to terrorism financing and was sentenced to 31 years in prison.

The U.S. is offering a \$10 million reward for information leading to Saeed's conviction in the Mumbai attacks. Saeed has denied any involvement.

Jeff Seldin serves as VOA's National Security Correspondent tracking developments in intelligence, counterterrorism, and cyber since March 2015, following a stint covering the Pentagon. His current focus has been on terror groups such as ISIS and al-Qaida, while also covering U.S. election security, as well as covering developments with Russia, China, North Korea and other global hotspots. Before coming to VOA, Jeff covered government, politics, business and consumer issues at all-news station WTOP in Washington and at its sister station, Federal News Radio. He has also worked in radio and TV in Philadelphia, Wilmington, Delaware, and Syracuse, New York.

Can an Entire Nation have Attention Deficit Disorder?

By Bob Hennelly

Source: <https://www.insidernj.com/can-an-entire-nation-have-attention-deficit-disorder/>

Aug 18 – In this summer of Trump indictments, there's so much that's being eclipsed by this essential multi-faceted effort to hold him accountable for trying to derail the peaceful democratic transfer of power. This internal myopic fixation on all things Trump is happening as the larger world around us continues to turn whether or not we are engaged in it. This introspective national dynamic creates dangerous blind spots that can be exploited like they were on Sept. 11 when those hijacked passenger airliners were turned into weapons of mass destruction we did not see coming.

And then for twenty years all we saw was red.

For the 20 years that followed the World Trade Center attack, the United States prosecuted its global war on terrorism that cost trillions and according to [Brown University's Watson Institute of International & Public Affairs](#) helped contribute directly to the deaths of as many as 900,000 with another 3.6 to 3.8 million perishing from the ecological and economic fallout from the open-ended warfare. Shaky nations were further destabilized and [tens of millions of refugees](#) left their homes to find sanctuary from a never ending cycle of violence that seemed to actually proliferate terrorism and terrorist groups like ISIS that didn't exist when we started.

It's a track record that's so horrific you can understand why we opt to look away and why a corporate media that's supported by the military industrial complex avoids it.

Are we up to the heavy lift of holding the Trump junta liable for their treason and calumny while also simultaneously learning the lessons from that global war on terrorism that commandeered the national agenda while Trump was still selling steaks?

Yes, there was beltway corruption before Trump and our national security apparatus had serious problems before Putin's front man got into the White House.

Now, we have to do deal with both problems in real time. The world turns whether we are paying attention to it or not. That's something that Rep. Andy Kim (D-3rd Dist.), who was first elected to his seat in 2018, knows all too well as a former civilian official with the U.S. State Department and Pentagon on the ground in Afghanistan.

"Long story short, I was a sophomore in college when Sept. 11 happened," Kim told InsiderNJ during a wide-ranging interview. "Being from New Jersey it had a particular resonance and concern, so I decided to give my whole life to service, in particular foreign policy. So, I went and got a doctorate in international relations and joined up with the State Department, worked as a career public servant in foreign policy, and worked at the Pentagon."

Kim continued. "I was based out of Afghanistan in 2011 as a civilian advisor to the military and then worked at the White House National Security Council dealing with counterterrorism and in particular countering



the terrorist group ISIS. So, this was something I lived and breathed. I was a career public servant. I worked both under Republicans and Democrats.”

The U.S. ‘stayed the course’ in Afghanistan under four U.S. presidents, two Republican and two Democrats.

Ironically, part of Kim’s job description at the U.S. State Department and the Pentagon when he was stationed in Afghanistan was to brief visiting members of Congress about what was going on inside the beleaguered country. He recalls the failure of U.S. intelligence and the military to [downplay the emergence of ISIS](#) and its lethality which created a real disconnect between what was really going on in Afghanistan and what our leaders were being told.

“Well, I think the underestimation of ISIS happened across the board,” Kim told InsiderNJ. “It was a comprehensive failure for our country, not just the military but also in terms of intelligence—in terms of diplomacy. I have seen that with my own eyes and the challenges that come with these huge problems that we were facing especially in Iraq and Afghanistan.”

Kim said it was “a huge challenge” for forward deployed Americans like himself to feel empowered to report back to Congress what they were actually seeing on the ground and not just parrot back what the power structure wanted to project back home.

“That was something we thought about when we were out in Afghanistan,” Kim said. “We are coming across and getting our own sense of what’s happening [on the ground], and we asked ourselves, are people back in DC understanding this? Do the people in the Situation Room and in power, on Capitol Hill and elsewhere, understand?”

Kim continued. “And look, members of Congress would come out for a visit. I have done that myself traveling out to Afghanistan in 2019 to try and see with my own eyes. It was really interesting having been somebody who worked in Afghanistan and helped support these Congressional delegations before. Now, returning as a member of Congress I was briefed in the same room at the headquarters in Kabul that I worked in and briefed members of Congress when I was a staffer. So, having seen it from both sides, gives me a greater sense of my own personal belief about what information is needed and how do I try to get as full of a picture as possible because oftentimes, people are quite silent with what they hear.”

The lack of a ‘speak-up’ culture, where flattering superiors by stroking their vanity and validating their false assumptions is the only way to advance up the ranks can have disastrous results.

This month marks the second anniversary of America’s chaotic exit from Afghanistan after 20 years of armed conflict making it this [nation’s longest war](#). The departure was marred by a catastrophic suicide bombing that killed 13 American military personnel and more than 100 Afghans made all the more horrific because we were trying to leave.

In February 2020, the Trump administration signed the [Doha Agreement](#) with the Taliban committing to exiting Afghanistan in nine and half months in exchange for the Taliban not permitting anyone to use their country as a base to “threaten the security of the United States and its allies.”

Meanwhile, in the real work conditions on the ground continued to [deteriorate](#) as fighting between the Taliban and Afghanistan National Defense forces intensified with the Taliban gaining and holding much of the country.

By 2021, when the U.S. finalized its exit, despite hundreds of billions of dollars invested in Afghanistan’s national military, the [national defense forces collapsed immediately](#). Testifying before Congress a month later U.S. Defense Secretary Lloyd Austin testified “the fact that the Afghan army we and our partners trained simply melted away – in many cases without firing a shot – took us all by surprise.”

Surprised?!

Several years before the Afghan army collapsed so spectacularly, the U.S. Special Inspector General for Afghanistan Reconstruction (SIGAR) [revealed](#) that, while the US Forces-Afghanistan reported there were 319,000 Afghan soldiers, the actual number was closer to 120,000. “Persistent reports” of discrepancies in Afghan troop strength “raise questions” over whether or not US taxpayers are actually paying for “ghost soldiers,” SIGAR John Sopko said in a letter to the Pentagon in August of 2016.

Over the arc of its operation SIGAR, a watchdog agency set up by Congress in 2008, the agency helped to secure well over a hundred convictions of government contractors, active-duty and retired US military personnel, while recovering hundreds of millions in criminal fines, restitutions, forfeitures, civil-settlement recoveries, as well as flagging billions more in waste.

In 2016 SIGAR released a ‘lessons learned’ [report](#) entitled “Corruption in Conflict: Lessons from the US Experience in Afghanistan.” It evaluated how the US government viewed the risks of corruption going in, how the US responded to the corruption it encountered, and just how ineffective those responses were.

The SIGAR analysis describes how the pursuit of strategic and military goals all too often trumped concerns about fighting the corruption that US personnel found rampant throughout Afghan society.

According to the report, the United States facilitated “the growth of corruption by injecting tens of billions of dollars into the Afghan economy, using flawed oversight and contracting practices,” while collaborating “with malign power brokers” all in hopes of realizing short-term military goals.



As a consequence, the United States “helped to lay a foundation for continued impunity” for bad actors that ultimately undermined the “rule of law” and actually promoted the kind of corruption that had historically driven the local population away from the central government and “to the Taliban as a way of expressing opposition” to a government they believed to be illegitimate.

The SIGAR report quotes former US Ambassador to Afghanistan Ryan Crocker making the disconcerting observation that “the ultimate failure for our efforts wasn’t an insurgency. It was more the weight of endemic corruption.”

Kim attended a recent Congressional oversight hearings that was convened to examine the circumstances surrounding the U.S. exit from Afghanistan this inconvenient history was not discussed.

One of the subject matter witnesses, retired Col. Seth Krummrich, the former Chief of Staff for the Special Operations Command that oversaw U.S. operations in Afghanistan, testified described the corrosive impact of “selectively” using intelligence to re-enforce preconceived notions.

“The trap decision makers fall into is selectively choosing the intelligence that supports their favored course of action rather than letting the intelligence shape and inform their decision,” Krummrich told the panel.

After the testimony of subject matter experts, the hearing devolved into Republicans blaming President Biden for the way the way his administration ended America’s 20-year misadventure.

“I agree there were many mistakes made in the 20 years, but the ultimate mistake ended 20 years of blood and treasure with now the Taliban in charge raising their flag over our embassy taking \$7 billion of our weapons, leaving the women behind under Sharia law now where they can’t even go outside,” said Rep. Michael McCaul, chair of the Committee on Foreign Affairs.

The hearing had a surreal quality because so many of the Republican House members that were piling on the Biden White House, like [Rep. Elise Stefanick \(R-NY\)](#) voted AFTER the Jan. 6 violent insurrection in the U.S. Capitol not to certify Biden’s legitimate election.

Perhaps had Donald Trump not been so obsessed with staying in power beyond his term in office he could have been paying attention to the disaster brewing in Afghanistan.

Kim told InsiderNJ he was frustrated the U.S. exit had become a “political cudgel with people trying to weaponize the issue for the sake of the 2024 election.... I still truly believe that politics has no place in national security and in the Situation Room. We have to find ways, especially when we are talking about life and death, to have that kind of broader perspective and that humility that comes with it.”

Kim continued. “Yes, we spend a lot of time at that hearing talking about the 13 service members who were tragically killed, and yes, I want to make sure that we are honoring their service—that we are learning lessons from that, but we also have to just keep in mind the bigger context. Over 2,400 Americans died in Afghanistan and each one of their lives was tragically lost and was a sacrifice for this country. So, we need to learn about that.”

To that end, Kim worked with Sen. Tammy Duckworth (D-IL), an Iraqi war veteran who lost her legs in combat while piloting a Blackhawk helicopter, to draft the [Afghanistan War Commission Act](#) which was enacted as part of the 2022 National Defense Authorization Act.

The panel will look at U.S. actions just prior to the 9/11 attacks, through the twenty years of the U.S. engagement, right up through the military withdrawal. The Commission has four years from its first meeting to produce a final report with its findings, “conclusions, and recommendations to address any mistakes in the conduct of the war.”

“When we look at the circumstances that lead to the evacuation and all the chaos that was there, we also need to look out how after 20 years of war and trillions of dollars and over 2,400 lives lost, how did we get to the point where the Taliban was still so strong and capable across the entire country,” Kim said. “How was it that we got to a point we had to negotiate with them one on one, without the Afghan government in the room which was one of the questions I was pointing to during the hearing—just to point out that there were so many points along the way that lead to this lapse in August when the evacuation was happening that we need to look at because it created that snowball.”

InsiderNJ asked Kim how the U.S. foreign policy and military command structure could turn a blind eye to the dashboard with blinking hazard lights provided by SIGAR for well over a decade on the war in Afghanistan.

“Exactly, that really gets to the issues that underpins so much of what we have seen and what I saw in Iraq as well,” Kim said. “Did the Iraqi security forces have the will to fight? Did the Afghanistan National Security forces have the will to fight? Was that a credible operation? We spent so much time trying to build up these forces and we’ve learned the lessons of how much that has blown up in our faces. We have to reevaluate.”

Kim continued. “We have to really look at that carefully and draw upon those lessons for future potential challenges. And we see that right now with the fighting in Ukraine and how do we try to approach that learning lessons from the past.” Even now, the two term Congressman is concerned that as the U.S. shifts



its geo-political focus to China and “arming up” Taiwan it hasn’t fully grasped the lessons we need to learn from the last 20 years post 9/11.

“How are we going to learn our lessons from this all?” Kim asks with a sense of urgency. “It feels like in Congress we are not doing that. Instead, we are making things worse in my opinion by politicizing these issues and that’s something that I found deeply alarming coming to Congress from a place of having been a non-partisan national security official for the country.”

Kim says Congress has to think “more strategically and holistically about these massive problems and not to try to oversimplify them for partisan purposes.” Of course, we have to finish litigating who won the 2020 election first.

Fargo police take down Syrian asylum seeker Mohamad Barakat on his way to commit 'mass casualty attack' in new bodycam footage

Source: <https://www.dailymail.co.uk/news/article-12417691/Officials-discuss-video-evidence-Fargo-shooting-ambush.html>



Barakat's terrifying arsenal of weapons. He had 1,800 live rounds, an AK-47, tactical gear, explosives and a grenade

Aug 17 – Bodycam footage has emerged of a Fargo police officer taking down a Syrian would-be mass murderer armed with an AK-47, 1,800 rounds of ammunition, a grenade and enough explosives to obliterate a crowd in what would have been a catastrophic domestic terrorist attack last month had it not been thwarted.

Gunman Mohamad Barakat, who moved to the US in 2012 as an asylum seeker, was on his way to carry out an attack in Fargo at a parade on July 14 when he opened fire on police officers responding to a car crash.

Police say they have not found any evidence that he was a religious fanatic, and believe instead that he was motivated purely by hate and fascinated by mass shootings. He became a naturalized US citizen in 2019. Neither the FBI nor the



Department of Homeland Security has confirmed whether or not he was on any kind of watchlist.

The day before the shooting, he Googled: 'area events where there are crowds' which led him to an article about the Downtown Fargo Street Fair.

He'd also Googled 'explosive ammo', 'incendiary rounds' and 'mass shooting events'.

In his two-minute rampage, Barakat killed 23-year-old rookie cop Jake Wallin, an Afghanistan and Iraq veteran who'd only been on the job for three months, and critically injured two others before being shot dead by 32-year-old Officer Zach Robinson.

The full details of the terrifying incident emerged yesterday at a press conference where North Dakota officials also released Officer Robinson's bodycam footage.

Robinson, coming under fire himself, shot Barakat 31 times in total.

The gunman somehow survived the majority of the shots and continued to reach for his weapon before eventually being taken out.

The planned attack would have been so deadly that North Dakota officials say there wouldn't have been enough medical and emergency personnel in three states to respond to it adequately.

In addition to the weapons in his car, Barakat also had three canisters of gasoline and two propane tanks filled with Tannerite - a highly explosive material.

Before the incident, he had no criminal record, but police had visited his home to inquire about his weapons twice. They found them to have all been legally acquired.

EDITOR'S COMMENT: A Syrian, asylum seeker, with a big collection of guns and ammo but it is OK if they are legal (?). Too much adherence to law and human rights is bad for public health and the life of policemen! Stupidity should be included in the WMDs list!

America has lost the war against Islamist terror in Africa

By Nick Turse

Source: <https://www.spectator.co.uk/article/america-has-lost-the-war-against-islamist-terror-in-africa/>

Aug 20 – After 9/11, the US built a network of military outposts across the northern tier of Africa to fight a shadow war against Islamist groups, and Niger became central to the effort. From Base Airienne 201, known to locals as 'Base Americaine', US drones were sent across the region to track down Islamist terrorists. The coup against President Bazoum marks another disruption in this long-running, mostly secret, war on terror. American troops in Niger are currently confined to their bases. The future of America's two-decade counterterrorism campaign there is in doubt.

In 2008, about 2,600 US military personnel were deployed in Africa, but today, there are around 6,500 troops and civilian contractors. The US government couldn't identify even one transnational terror group in sub-Saharan Africa after the Twin Towers attacks but embarked nonetheless on wide-ranging counterterrorism efforts there. Over the years, America has conducted drone strikes in countries like Libya and Somalia, and its commandos have fought in countries including Burkina Faso, Cameroon, Kenya, Libya, Mali, Somalia, and Tunisia. Just over half of the US forces are stationed at Camp Lemonnier, a sprawling base in the tiny nation of Djibouti in the Horn of Africa. More than [1,000 are still deployed in Niger](#). Personnel rotate in and out of that country like they would in any other war zone.



After two decades of failing to crush terrorism in Africa, the US has quietly admitted that things are going wrong. An [assessment](#) last year by one of the Pentagon's own research institutions couldn't be grimmer. The number of Islamist terror attacks in the western Sahel (the strip of Africa between the Sahara Desert in the north and the tropical savannas to the south) has quadrupled since 2019, it said, and the violence had 'expanded in intensity and geographic reach.' The researchers found fatalities linked to militant Islamist groups in the Sahel jumped from [218 in 2016](#) to [7,889 in 2022](#). An increase of more than 3,000 per cent in six years.



Exactly what American special forces are doing in Africa is a secret

America's war in Africa uses a significant proportion of America's most elite troops – Army Green Berets, Navy Seals, and Marine Raiders. Around 14 per cent of US commandos dispatched overseas in 2021 were sent to Africa, more than anywhere in the world except for the Middle East. Special Operations forces were sent to Benin, Botswana, Burkina Faso, Chad, Côte D'Ivoire, the Democratic Republic of Congo, Djibouti, Egypt, Ghana, Guinea, Kenya, Malawi, Mali, Mauritania, Morocco, Mozambique, Niger, Nigeria, Senegal, Somalia, Tanzania, and Tunisia in 2021. But exactly what they were doing there is a secret. The US government only provides details about innocuous missions, like short-term deployments for training or to assess a nation's counterterrorism capabilities, but retired Army Brigadier General [Don Bolduc](#), who headed Special Operations Command Africa (SocAfrica) until 2017, says that US special forces have seen combat in at least 13 African nations in the last decade.

The US government did its best to hide its African war against terrorism, but secrecy became untenable as more and more Americans were injured and killed. Between 2015 and 2017, there were [at least 10 unreported attacks](#) on American troops in West Africa. In February 2017, US Marines [fought al-Qaeda militants](#) in a battle that Africom (America's African military command) still won't admit took place in Tunisia, near the border of Algeria. Just three months later, during an 'advise, assist, and accompany' mission, 38-year-old [Navy SEAL Kyle Milliken](#) was killed and two other Americans were wounded in a raid on a militant camp in Somalia. That same year again, in October, Africom was finally forced to abandon the fiction that US troops weren't at war on the continent after Isis militants ambushed American troops near Tongo Tongo, a village in Niger, killing four US soldiers. In 2020, one US soldier and two Pentagon contractors were killed when the Somali terror group al Shabaab attacked an American base in Manda Bay, Kenya.

'Combatting VEOs' – military slang for violent extremist organisations or terrorist groups – is 'critical to stability,' Kelly Cahalan, an Africom spokesperson, told me. 'It is a top priority... of many of our partners in Africa and they ask us for help solving this challenge.' The solution has not been forthcoming. Despite all the US military assistance, training exercises, advisory missions, base-building, drone surveillance, air strikes and ground combat, even the Pentagon's own assessments have been uniformly dismal. While Africom claims that it 'counters transnational threats and malign actors' to promote 'security, stability and prosperity' on the continent, it's been Africans, not just people in the Sahel, who have suffered. The Africa Center found that, across the continent, fatalities from militant Islamist violence have increased from about [3,000 in 2010](#) to [19,109 in 2022](#).

Niger was the West's only major ally left in the West African Sahel. Its neighbours – Burkina Faso and Mali – are beset by terror attacks and run by military officers who overthrew their governments. Niger was one of the only places where America could safely base its troops, and diplomats saw it as a fragile but critical partner in the campaign against Islamist terrorism in Africa. Now, the US has 'paused' security assistance to Niger, and when Pat Ryder, the Pentagon's top spokesman, was asked whether the US would be withdrawing its troops, he said they were planning for 'various contingencies'. The coup, and America's loss of one of its only Sahelian partners, is another setback in a long-running string of failures.

[Nick Turse](#) is an investigative reporter and a contributing writer at *he Intercept*. He is the author, most recently, of *Next Time They'll Come to Count the Dead: War and Survival in South Sudan*.

EDITOR'S COMMENT: I think the title of the article is not accurate! I tried to spot the wars that the US won after WWII but could not find any.

Al-Qaeda in the Arabian Peninsula's Drone Attacks Indicate a Strategic Shift

By Rueben Dass

Source: <https://www.lawfaremedia.org/article/al-qaeda-in-the-arabian-peninsula-s-drone-attacks-indicate-a-strategic-shift>

Aug 20 – Between May 12 and July 4, 2023, al-Qaeda in the Arabian Peninsula (AQAP) carried out seven attacks using armed [drones](#) in the Shabwa governorate of southern Yemen. The attacks were targeted primarily at members of the Shabwa Defense Forces, which are aligned with the Southern Transitional Council (STC), an organization that advocates for the secession of South Yemen. The exact type of drone used in the attacks remains unclear, though one [source](#) noted that in at least one case the drone appeared to carry an explosive projectile.

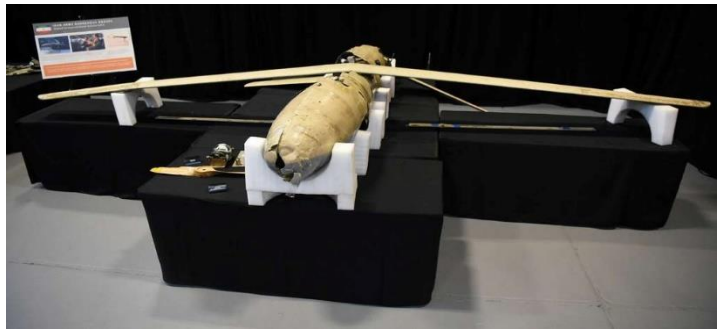
The attacks were claimed by AQAP on the organization's social media channels over the course of several weeks. The only other time that AQAP had used drones offensively was in an attack in April 2022, which was mentioned only in passing in their media channels. The sudden uptick in drone use by AQAP and the media attention the attacks have received indicate what AQAP expert Elisabeth Kendall has [described](#) as a "worrying



ICI C²BRNE DIARY – August 2023

escalation.” And the sustained use of the new technology suggests that AQAP has new partners and may be engaged in a strategic pivot.

The wreckage of an Iranian Shahed-123 drone recovered in Yemen is displayed at Joint Base Anacostia-Bolling in Washington, D.C., on Nov. 26, 2018. Photo credit: Lisa Ferdinando/Department of Defense photo



AQAP's Decade of Decline

AQAP was formed in 2009 when the Saudi and Yemeni branches of al-Qaeda merged. In 2011, it was [considered](#) to be the most active operational affiliate of al-Qaeda and one of the biggest threats to the U.S. homeland. Apart from local terrorist attacks in Yemen, AQAP was known for external operations and plots outside of Yemen. The group was behind several high-profile international terrorist plots, including an assassination attempt targeting Saudi prince Mohammed bin Nayef in August 2009, the December 2009 plot to blow up a U.S. plane with explosives that Umar Farouk Abdulmutallab had hidden in his underwear, and the October 2010 effort to blow up cargo planes bound for the United States using explosives smuggled in printer cartridges.

More recently, AQAP claimed responsibility for the 2015 attacks on the Charlie Hebdo offices in Paris and the 2019 shooting at the Naval Air Station in Pensacola. But the group's activity declined as U.S. drone strikes targeted its leadership. Anwar al-Awlaki, a prolific AQAP propagandist and operational planner, was killed in 2011, and successive leaders of the organization have also been successfully targeted—Nasir al-Wuhayshi in 2015 and Qassim al-Rimi in 2020. Today, AQAP has been [weakened](#) by sustained counterterrorism efforts and internal strife. Between January and February 2023, three more senior AQAP officials were killed by U.S. drone strikes, including two notable [explosives experts](#) and [Hamad al-Tamimi](#), the group's media chief and leader of its Shura Council. Recent data suggest that AQAP activity has diminished. The one exception to this trend is an uptick in violence corresponding to several offensives, named "[Arrows of the East](#)," launched by the STC against AQAP in August 2022. The STC offensives primarily targeted terrorist elements in Abyan and Shabwa governorates in an effort to secure the south of the country.

AQAP is also currently hindered by [internal conflict](#). The group is believed to be [divided](#) into three factions: a Yemeni faction led by Sa'ad Atef al-Awlaki, the group's emir in Shabwa province; a Saudi faction led by AQAP leader Khalid Batarfi; and an Egyptian faction led by senior AQAP official Ibrahim al-Banna and the son of the de facto leader of al-Qaeda Central, Saif al-Adel. There seems to be a conflict between the Yemeni and Saudi factions in particular. Batarfi was [alleged](#) to have isolated fighters in Shabwa by cutting off finances to them and preventing them from fighting against the Houthis. The policy of not fighting the Houthis might be indicative of an alliance between the Houthis and AQAP, which some security officials have [noted](#).

AQAP's Strategic Shift

The recent attacks in Shabwa can be seen in three related ways. First, they are a means to boost the group's image and influence, amid their waning strength in South Yemen. Second, they may reflect a strategic (and possibly temporary) rapprochement with the Houthis. And third, they indicate AQAP's shift in focus toward the STC.

Reports have [suggested](#) that the drones used in the Shabwa attacks were provided to AQAP by the Houthis. Given that AQAP has [limited](#) technical capability in developing their own drones, especially after the recent deaths of their explosives experts, external support for sourcing these weapons was probably crucial. The drones were reportedly [obtained](#) by Abu Osama al-Diyani, a Yemeni jihadi leader close to Batarfi who maintains a close relationship with the Houthis.

[Infighting](#) between Batarfi and AQAP leaders in the southern provinces had led to a cessation of offensive operations there. Unable to conduct military operations in the south, Batarfi instead [sought](#) Diyani's assistance to obtain drones and begin using them to carry out attacks. The drone strikes are [seen](#) as a new way for the group to conduct attacks despite diminished operational capacity, and as a significant image booster. These high-profile attacks demonstrate the strength of the group and boost troop morale. One report also [suggested](#) that the drone operations are an effort by Batarfi and leaders close to him to ensure their survival within the group. If the drones were in fact provided by the Houthis, this would clearly indicate that AQAP has shifted away from its conflict with them. Though AQAP fought the Houthis for most of the past decade, its recent offensives against the group have not been particularly effective and this has been exacerbated by the group's financial difficulties. Historically, AQAP and the Houthis have maintained some level of [pragmatic](#), tacit [cooperation](#). The Houthis have at times provided AQAP with [refuge](#) for some of their leaders and [weapons](#). The apparent cooperation also goes beyond the possible provision of drones—the groups also carried out a [prisoner swap](#) in February 2023. For their part, the Houthis [benefit](#) from continued instability in South Yemen. AQAP's operations provide plausible deniability for the Houthis' own operations and



provide an excuse for Houthi forces to continue their military operations in the area in the name of counterterrorism. Whether this current AQAP-Houthi arrangement is just a [short-term](#) strategy remains to be seen.

The decision by AQAP to shift their attention to the south, Shabwa and Abyan in particular, coincides with the group's [refocusing](#) of its efforts against the STC forces. One reason for this shift may be the relative strength of their current capabilities in the area. Shabwa and Abyan governorates represent [historical strongholds](#) for AQAP, and data suggest that members of the group seem to have [mostly retreated](#) to those provinces. Sources also suggest that the group has [little operational capability](#) in other provinces. The focus on the STC might also have [ideological motives](#), as AQAP has always viewed the southern forces as apostates.

In January 2023, Batarfi, the head of AQAP's Saudi faction, [met](#) with AQAP leaders asking them to prepare for attacks against the STC in the south and halt any attacks on the Houthis. In February 2023, Awlaki, the head of the Yemeni faction, issued a [call](#) to tribesmen from Abyan and Shabwa to join AQAP against the STC and Arab-led coalition. The drone attacks may indicate that AQAP is ramping up their retaliatory efforts against the STC's Arrows of the East campaign, as part of their own offensive, "[Operation Arrows of Righteousness](#)," which they announced in September 2022.

This strategic shift away from targeting the Houthis and toward the STC is in line with directives from al-Qaeda Central. Saif al-Adel has [advocated](#) for an increased focus on attacks against Western interests, Saudi-led coalition forces, and anti-Houthi forces, and is seen to have an [increasing](#) influence on AQAP. Adel has [attempted](#) repeatedly to move to Yemen and shift al-Qaeda Central's command there.

The Dangers of AQAP-Houthi Cooperation

The recent use of drones by AQAP in Shabwa is likely an attempt by the group to remain relevant despite its waning strength, and to [reassert](#) its influence in South Yemen. The attack may also be a sign that AQAP is shifting in its priorities to the south and away from hostility with the Houthis. Whether this will be a new trend in AQAP's playbook is something to be watched closely. This sudden, sustained use of drones almost certainly requires some form of external support for sourcing the technology. If the Houthis are in fact providing AQAP with drones and this relationship continues, possibly more sophisticated drone attacks are likely in the future. The Houthis have significant experience carrying out sophisticated drone attacks, and selective cooperation between the two groups may open channels for additional transfers of technology and weapons from the Houthis to AQAP.

Rueben Dass is a senior analyst with the International Centre for Political Violence and Terrorism Research at the S. Rajaratnam School of International Studies in Singapore. His research interests include terrorist use of innovative technologies—including drones, 3-D printing, and the use of chemical, biological, and radiological weapons—and counterterrorism in Southeast Asia. His work has been published in the Journal of Policing, Intelligence and Counter Terrorism, Terrorism and Political Violence, and Studies in Conflict and Terrorism, as well as in media and security outlets such as Defense Post and The Diplomat.

The author would like to thank Mina al-Lami from BBC Monitoring and Daniele Garofalo for their insights, and Ahmad Helmi bin Mohamad Hasbi from RSIS for his assistance in translating Arabic texts and articles.

Terrorist use of Fire in Attacks

ProtectUK publication date: 19/04/2023

Source:

Headline Assessment

- *Terrorists have been using fire in attacks for decades. No special skill or training is required and the materials needed to produce fire are widely available.*
- *The likelihood of terrorists using fire in an attack will vary depending on ideology. In the UK, such an attack is more likely to be perpetrated by Extreme Right-Wing (ERW) Terrorists.*
- *Over the last five years, attacks planned or carried out using only fire have been confined to those with an ERW ideology, although the tactic has been used by Anarchists and Animal Rights activists in the past.*

How and why do terrorists use fire in attacks?

The deliberate setting of fires, to damage, destroy property or to target those within, is not a new phenomenon and has been used by armies, criminals and others for centuries. Likewise, terrorists have been using fire in attacks (colloquially known as 'Fire as a Weapon' (FAW) for decades. No special skill or training is required and the materials needed to produce fire are widely available. Fire is one of several simple methodologies



promoted by terrorist groups in recent years that can be used alongside other methodologies, or as an alternative to more sophisticated methodologies.

Terrorists can use fire in attacks in a number of different ways:

Arson – primarily considered a crime against property in the UK, arson for example, has previously been used by animal rights activists to target laboratories and premises perceived to be engaged in experiments involving animals. As these attacks were likely planned to avoid casualties, they would not now reach the threshold for terrorism.

Pyro-terrorism – a term derived from the Greek word for fire to describe the use of incendiary attacks to intimidate or coerce a government, the civilian population, or any segment thereof, to advance political or social objectives. This can range from large-scale attacks using fire such as the deliberate setting of wild and forest fires, to attacks using incendiary devices in so-called 'letter bombs'.

Fire as a Weapon - refers to the deliberate use of fire against people to cause injury (as opposed to arson which targets buildings, infrastructure or property), usually as part of a complex marauding terrorist attack (MTA), but also used on its own.

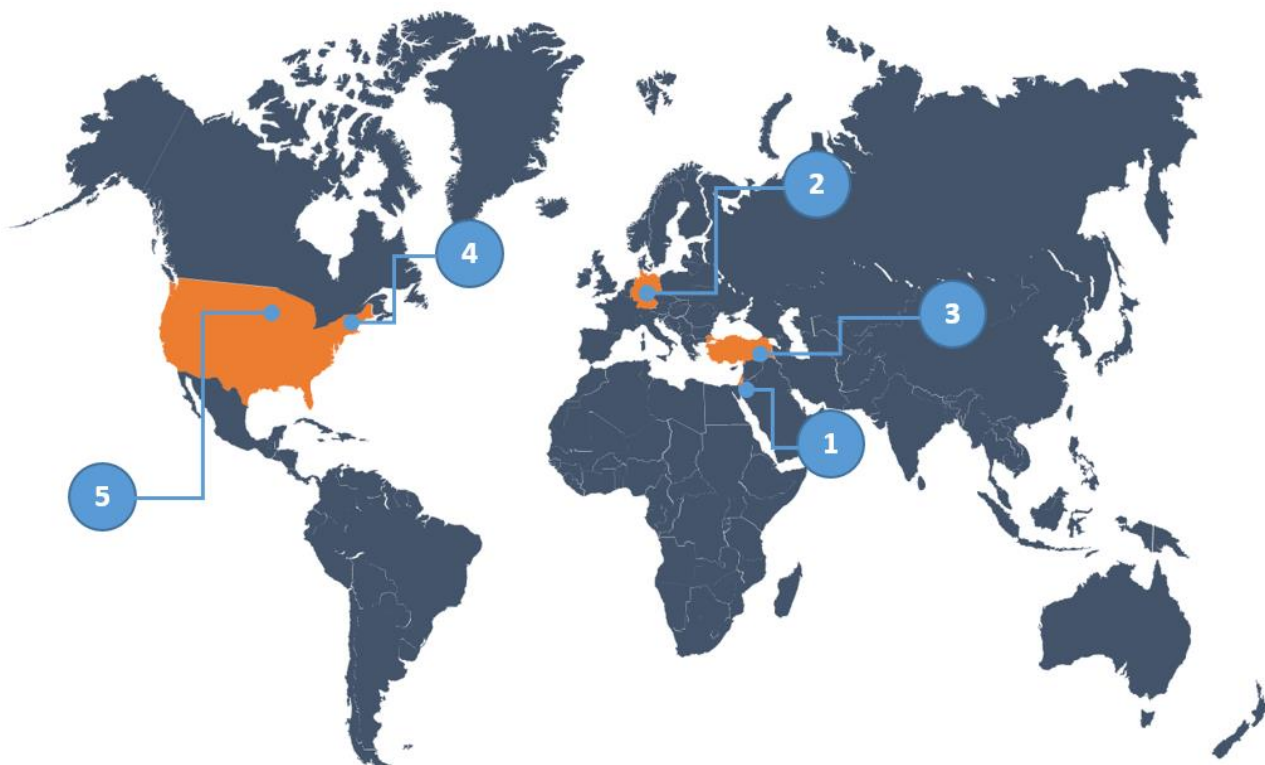
Does this differ between ideologies?

The likelihood of terrorists using fire in an attack will vary depending on ideology. In the UK, such an attack is more likely to be perpetrated by Extreme Right-Wing Terrorists (ERWT), who are likely to view buildings associated with specific communities, such as mosques, synagogues and immigration centres, as credible targets. Despite propaganda from Islamist Terrorist groups advocating the use of fire in attacks against the West, Islamist Terrorists in the UK are less likely to favour this tactic.

Additionally, for some terrorist ideologies, fire can have symbolic meaning. These cultural, historical, spiritual, or religious connotations may influence whether, and how, fire is used by terrorists of differing ideologies in propaganda and in practice. Specific fire-related imagery or beliefs are unlikely to be directly indicative of extremism. However, extremists appropriate and share images and symbols which exist within wider, non-extremist cultures.

When have terrorists used fire in attacks?

There are a number of recent examples of when terrorists have used fire in attacks around the world. These include:



ICI C²BRNE DIARY – August 2023

- 1 In August 2021, terrorists in Gaza launched balloon-borne incendiary devices into southern Israel causing several fires. This tactic has been used on previous occasions including in June 2018, when more than 450 fires were caused which burned at least 7,000 acres of land, resulting in over \$2 million in economic loss.
- 2 In May 2021, flammable liquids were used to set fire to a number energy cables which supplied the construction site of a new US electric vehicle factory near Berlin, Germany, causing 200 000 Euros of damage. A left-wing extremist group claimed responsibility, stating that the electric vehicle company 'is neither green, ecological nor social'.
- 3 In October 2020, forest fires broke out in multiple locations in Hatay province in southern Turkey. Responsibility for these fires was subsequently claimed by a group, linked to separatist terrorist group PKK. Whilst forest fires are not unusual in Turkey during the hot summers, similar outbreaks in 2021 are suspected to be arson attacks by the PKK.
- 4 In April 2020, a White Supremacist was charged with attempted arson after trying to use petrol to start a fire at a Jewish assisted living centre in Massachusetts, in the United States.
- 5 In January 2018, a student at St. Catherine University in St. Paul, Minnesota was charged with setting eight fires around campus in response to the destruction of schools in Iraq and Afghanistan.

How does this manifest in the UK?

Over the last five years, attacks planned or carried out using only fire have been confined to those with an ERW ideology.

- In 2022, a 66-year old man fire-bombed an immigration processing centre in Dover, Kent, then took his own life. The attack, which caused minor injuries to two members of staff, is assessed to have been motivated by an extreme right-wing ideology.
- In 2019, a 24-year old white nationalist plotted to burn down a mosque in Fife Islamic Centre in Glenrothes, Scotland.
- In 2018, a white supremacist accidentally set himself on fire while attempting to burn down the Exeter Synagogue.
- In February 2018, a 31-year old '-sympathiser' was sentenced to eight years imprisonment for threatening to attack mosques with petrol bombs in the wake of the Manchester Arena bombing.

Although there have been no such attacks motivated by an Islamist ideology, it is noteworthy that in at least one case the use of fire was planned for, but not actually used.

- After the London Bridge attack in June 2017, when three marauding Islamist terrorist killed eight and injured dozens more, the abandoned van used in the attack, was found to contain a stock of unused Molotov cocktails.

Whilst there have been no LASIT attacks in the UK using FAW in the past 5 years, the tactic has been used by Anarchists and Animal Rights activists in the past.

- In 2013, anarchists claimed responsibility for an arson attack against partially built police firearms training centre in Bristol.
- In 2014, a home-made incendiary device gutted the front and lobby of North Avon Magistrates' Court. The attack was attributed to the so-called 'Bristol Unabomber' an anarchist who is believed to be responsible for a series of arson attacks in the south-west region.

Although these attacks are examples of politically-motivated violence, they would likely not meet the current threshold for terrorism.

What does this mean for business and the Public?

The impact of any future use of fire by terrorists in the UK will depend on whether fire is used as the sole method of attack or is used in concert with other methodologies. Nevertheless, as well as the obvious threat to life that fire can pose, it can also cause significant damage to buildings and infrastructure.

Additional guidance can be found in the Purple Guide but also in 'Fire as a Weapon - Guidance on the mitigation of the risks' published by the Centre for the Protection of National Infrastructure (CPNI) – now known as the National Protective Security Authority (NPSA).

EDITOR'S COMMENT: In 2011, late Turkish PM Mesut Yilmaz declared that fires that broke out in Rhodes Island, Greece, in the period 1995-97 were the result of arson by Turkish MIT agents. He later recanted his statements, but what he said has always been an argument for those who argue that some of the fires breaking out, especially in critical areas of the country, may be the work of Turkish agents. This might be the case for the wildfires Greece is experiencing in August 2023 at least in the far north land borders with Turkey and





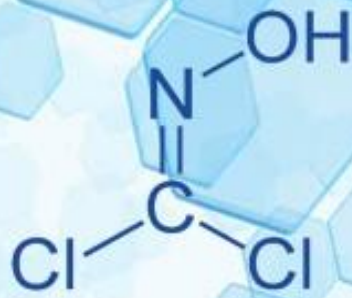
certain islands facing Turkey (Rhodes, Lesbos) this time via illegal immigrants facilitated to cross Greek borders by Turkish security forces. At least 18 illegal immigrants recovered charred in the Dadias' Forest (22/8) – an area that is seldomly used as a passage to enter Greek mainland. In addition, sudden wildfires in almost everywhere in Greece with no apparent reason are giving ground for an hybrid attack from another neighboring nation. **"Pyroterrorism"** or **"Pyro-Terrorism"** is the act of setting fire to large amounts of land and/or property for political reasons, usually in a systematic or random approach to



escape capture from authorities. The purpose of pyroterrorism is to destroy a particular country or region's local economy and kill innocent civilians in a way that prevents the would-be arsonist from being easily identified or captured. In ancient times pyroterrorism was used as a war tactic to raze crops and destroy an enemy's ability to feed themselves, thus weakening the foe. And if you think of that, burned forests are ideal for attacking drones in case of a conflict!!



ICI
International
CBRNE
INSTITUTE



C²BRNE
D I A R Y



CHEM NEWS



The truth behind suspicious overseas parcels must be swiftly uncovered

Source: <https://www.donga.com/en/article/all/20230724/4309444/1>



July 24 – Suspicious international shipping parcels of unknown origin are being randomly distributed across the country. In Ulsan, it came to light that individuals who opened these unidentified overseas packages were subsequently taken to the hospital due to symptoms such as **dizziness, shortness of breath, and numbness in their hands and feet**. This has led to speculations that the parcels might contain harmful gaseous substances. The police received reports of over 3,500 such suspicious mails over the past three days.

Most postal mails were addressed in **Taipei, Taiwan, while some were discovered in Malaysia and Uzbekistan**. Based on information provided by the Taiwanese authorities, these mails originated from Shenzhen, Guangdong Province, China, and entered Korea through Taiwan. This suggests that someone might have deliberately manipulated the envelopes to appear as if they were sent from Taiwan, rather than China, with Taiwan listed as the sender. In response, Taiwan's delegation to Korea and the deputy prime minister-level executive vice president of the Executive Council expressed their commitment to thoroughly investigate the matter until the truth is fully uncovered. This likely takes into account the potential diplomatic implications that this incident could have.

Most of the reported mails consisted of small products, such as lip balm, while some parcels were completely empty. This has raised the possibility that the incident could be a 'brushing scam.' In this scam, online shopping platforms send unordered items to anonymous recipients to manipulate their performance metrics and ratings. Interestingly, reports indicate that the addresses of certain Taiwanese mail items matched those previously identified in Canada and elsewhere during the 'brushing scam' incidents in 2020. However, upon analysis, no chemical, biological, or radioactive substances were detected in the white dough or powder found within the Ulsan package.

The significant volume of suspicious international mail currently circulating is understandably causing public anxiety. Even a package containing hazardous chemicals or explosives could have severe consequences. A poignant example is the situation in the U.S. following the 9/11 attacks when anthrax-laden postal mail led to the infection of about 20 people and the tragic loss of 5 lives. Such biochemical terrorism using mail may recur at any time. Someone may take advantage of the loosened awareness because of the recurrence of the 'brushing scam' and use it for actual chemical terrorism.

The government must work closely with the relevant countries to thoroughly ascertain the sender of these mails, the method of their entry into South Korea, and their intended purpose. This is a critical moment where finger-pointing between the ruling and opposition parties over the purported weakening of the National Intelligence Service's anti-aircraft investigation capability or the government's response should be set aside. Instead, efforts should be focused on fortifying the customs clearance inspection system for overseas postal items. With the surge in international parcels due to the rise in overseas direct purchases, it is essential to prevent them from becoming a medium that jeopardizes the safety of the people.



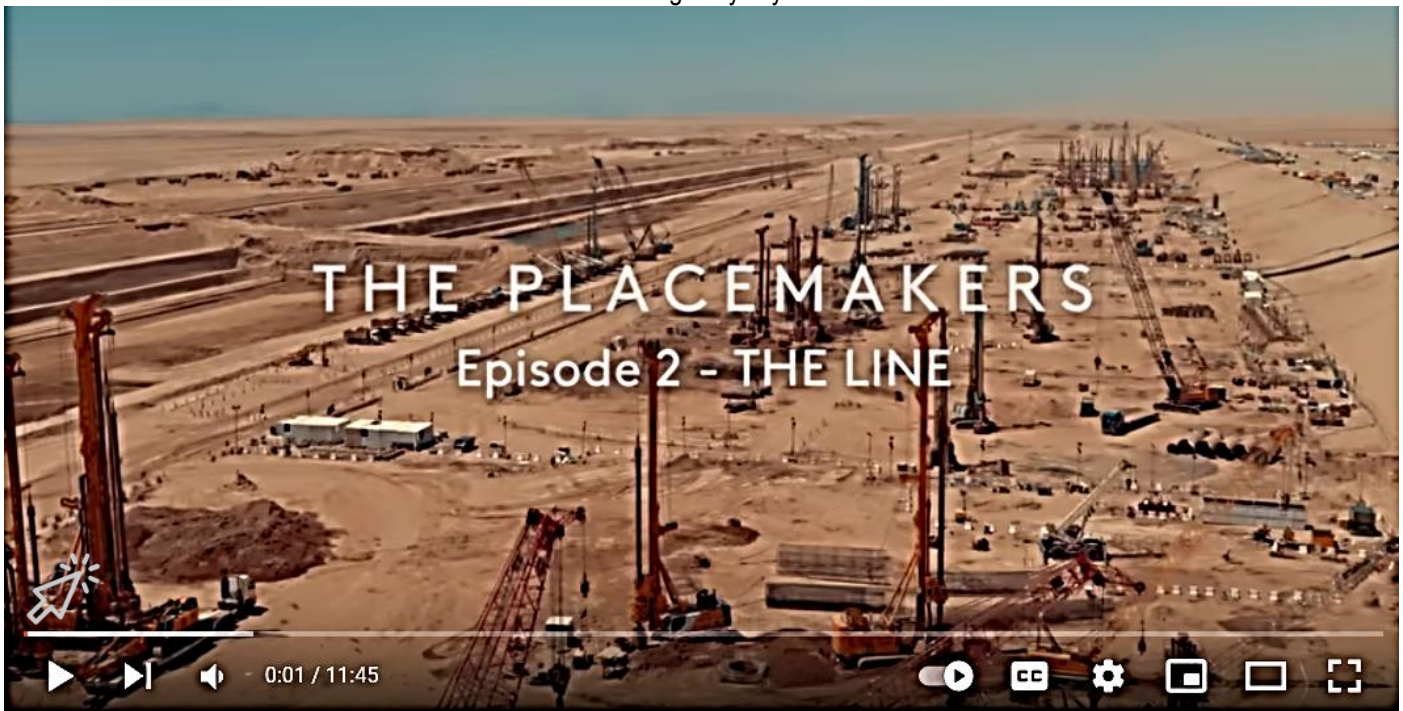
NEOM The Line – CBRN Challenges

By the Editor-in-Chief



In the April 2023 issue, there is an extensive reference to the mega CBRN challenges mega projects in the GCC area might face in the future. I was expecting to get a reply; something like “We have it under control” or alike. I did not and this is normal because CBRN threats are not included in the design of mega or giga projects like NEOM The Line or Mukaab Cube. The main reason is that architects and civil engineers are convinced that the civil defense authorities will deal with the problem. Besides, it is such an “exotic” threat, why bother? Along with “it will not happen to us!” No objection! It will happen to Yemenis or Somalis!

Recently I carefully watched the “Placemakers – Episode 2: The Line” video showing the progress made in this giga-project and I had the chance to see more insides of this wonder future zero-gravity city.



Watch at 4:23 the reference to “mobility corridors” that will connect subway lines at various heights. At the same time just think of ways CBRN First Responders will access a HotZone and how they will be able to cordon off the area or decontaminate victims involved. Think how authorities will manage to isolate a part of the city in case a deadly pathogen has been released. Imagine how mass evacuation might happen or what would be the effects of an electromagnetic pulse on the function and survival of The Line. CR agents in the air might be trapped in between the parallel sections of the city; so, practically there will be no contamination-free area to go to. These are some of the thoughts that should keep security officers awake at night but if you are not aware of the threat you can have a peaceful sleep.

As John Harvey-Jones (BBC “Troubleshooter”) quoted “Planning is an unnatural process; it is much more fun to do something. The nicest thing about not planning is that failure comes as a complete surprise, rather than being preceded by a period of worry and depression.”





CBRN Monitoring Belongs to Modern Shelters

Suddenly, We Invented the Shelters Again

Source: <https://environics.fi/blog/cbrn-monitoring-belongs-to-modern-shelters/#msdynttrid=xLZZMa0HcgewQ4QGecEXGoXvhH0kx2S0gcSGUWkpTal>

Shelters, their need and readiness for use under emergencies and military attacks have been set to the worldwide spotlight due to over one-year lasting war in Ukraine.

Shelters and hardened structures take many forms – they range from simple residential facilities to luxurious underground VIP bunkers, and from military command or data centers to governmental or public civil spaces and beyond.

They can be mobile or stationary structures, and they may not be only resting facilities used only during the time of emergencies, but for peace time activities, too. They contain specialized collection of doors, hatches, valves, wall sleeves, filtration units and live supporting and detection systems to provide blast proof, gastight spaces with uncompromised air quality for the specified number of occupants for a given sheltering period.

From Mass Civil Protection to High-end Hardened Structures

Finland as a Case of Shelter Preparedness

Civil defense shelters are the ones that provide essential protection for people against military threats in the areas of everyday living. They are intended to protect population against the effects of explosions and fragments, collapses, blasts, ionizing radiation and airborne substances hazardous to health.

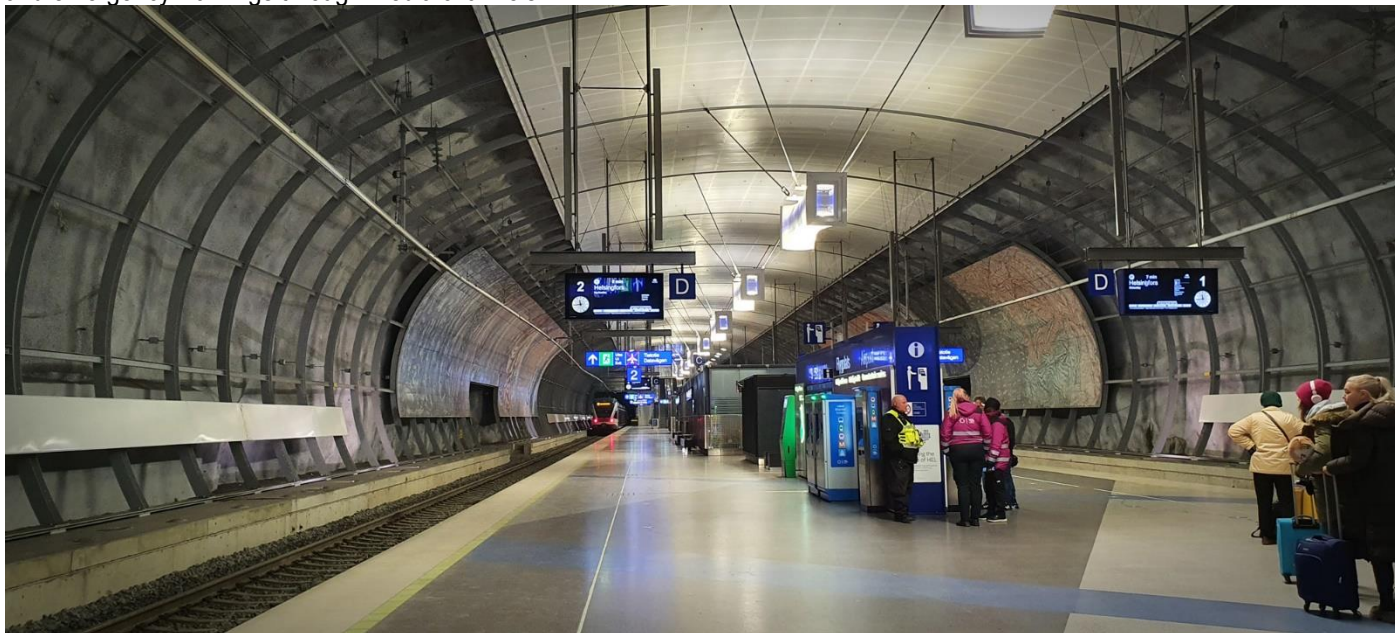
Since 1950s, Finland has shown forerunners' preparedness, activity and expertise in building civil defense shelters, based on the Rescue Act and Government Degrees on the Civil Defence Shelters and their Equipment and Supplies and Maintenance. Finland has also long and strong industrial tradition and expertise in the field. With its approximate of 50 500 civil defence shelters, Finland is capable of offering protection to nearly 4.8 million people. Most of these shelters are private, being reinforced concrete shelters located in individual buildings or joint bunkers for group of buildings.

Did you know that civil defence shelters take several other roles in normal conditions?

In Finland, your favorite underground sport hall, nearest metro station or an underground parking space in the middle of a city you stop by during your weekend shopping or the storage space in your apartment house is in fact – a civil defense shelter. Rules and regulation do not determine only their requirements for building codes, sizes and durability and equipment, but their readiness for the actual purpose – that shall take place within [72](#)



[hours from announced emergencies](#). A direct and imminent danger to the population is communicated with general alarm signals and emergency warnings through media channels.



Helsinki Airport train station — the world's northernmost underground railway station — opened in July 2015, and is a tunnel station located 45 meters underground. As many other structures in the capital of Finland, this train station also has a double role, being part of the city's network of tunnels and civil defence bunkers. Finland has built 500 bunkers in the capital Helsinki which can hold hundreds of thousands of people in the event of a war or nuclear disaster. The bunkers are connected by a vast network of underground tunnels with over 300km and have enough space and beds to hold all of Helsinki's 630,000 residents.

Due to the nature of the work conducted by the national safety and security professionals, protection of the governmental and military operators sets special flavor for equipping the respective class of shelters. The ones leading and defending sovereign nations are especially prone to hostile activities that aim to incapacitate and eliminate the key players. Sabotages, acts of terror and military attacks can take use of vaporized chemicals, airborne biological agents and ionizing radiation that stay unnoticed to human senses without CBRN detectors in place. From these, chemical agents will have their effects in minutes, but radiation and biological agents are silent and invisible devils that start to show symptoms after longer periods of time – when it is already too late.

CBRN Monitoring Systems in the Context of Shelters

When time is the valuable asset in fighting against CBRN threats, the indication for the need of sheltering shall be timely and reliable, and lead to feasible and sufficient actions.

This is the stage where CBRN monitoring systems come into the view: their role is closely related to the real-time situational awareness that enables smart and timely use of shelters. For activating and progressing from one sheltering mode to another, one must have an indication for the need for protection through the phases of preparation and close up to CBRN filtration mode, and again back to the normal through by-pass to post sheltering phases. Stationary CBRN monitoring systems provide the shelter operators with event & measurement information primarily on the outdoor environment and secondarily, on the indoor environment of shelters for informed decision making. In the first place, their role is to generate early-warnings alarms for the detected hazards and to trigger the sequence of activities in sheltering, and communicate the event information to Building Management System and to respective shelter control system. In addition to CBRN, monitoring of air quality sensors is typically an essential part of the sensor suites of shelters gathering masses of people under the same roof for long periods of time.

At their best, CBRN monitoring systems do not only provide early-warnings, but guidance at the threat events to the shelter operators. Furthermore, they help them to maintain operators' knowledge and skills that are essential for conducting the standard operational procedures on routine basis. Since maintenance of existing shelters and their equipment is as important as shelters' existence in general, an advanced CBRN monitoring system reminds the operators of the need for preventative and corrective maintenance that helps to keep the facilities prepared and running continuously, when needed. These elements of guidance, training and simulation and maintenance are typically inbuilt in the system software that acts as a frontline view for the operators in the control centers.



Summary

Shelter designs with their technical and functional requirements are reflected by several factors. CBRN monitoring systems are linked to the holistic security concepts, so shelter categories designed take into account:

- The type and the purpose of the shelters
- Threat scenarios and desired protection levels according to risk assessments
- National rules and regulations
- Functional modes, operational procedures and countermeasures during emergencies
- Networking and communication of real-time situation to all relevant stakeholders.

From a CBRN monitoring system point of view, it is essential to understand how the various aspects of safety are connected in a practical level in different shelter classes. Typically, a turnkey CBRN Monitoring System in a shelter target combines, in a variable degree, elements of...

- Timely situational awareness and guidance for the shelter operators
- Alarm information used for decision making on the use of the different sheltering modes and all the activities related
- Reporting and information flow to 3rd party systems manual or automatic shelter control systems

..and building management systems:

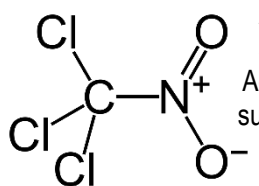
- Air quality monitoring
- Inbuilt simulation and training functions
- Maintenance management tools
- Complementing hand-held/portable CBRN instrumentation for confirmation & contamination control
- Optional CBRN monitoring system for perimeter protection

Environics & Shelter CBRN Monitoring

Environics operates in the field of [Building](#) and [Shelter CBRN Monitoring](#) with its proven and agile expertise of many decades. The newest launch, the X-System, represents a scalable, modular and redundant CBRN Solution suitable for all shelter designs. Formed by the [ChemProX-DS](#) for chemical detection, the [RanidX](#) for gamma radiation and X-ray radiation detection and the [ENVI BioScout](#) for bioaerosol detection, the system offers cutting edge, reliable and complete set of early-warning instrumentation. Complemented with the [EnviScreen](#) system software, the turnkey solution provides real-time situational awareness, guidance and training & simulation tool for shelter operators.

Commander: Russia continues to use chemical weapons in Ukraine

Source: <https://kyivindependent.com/commander-russia-continues-to-use-chemical-weapons-in-ukraine/>



Aug 07 – Russian forces continue using chemical weapons in Ukraine, violating international conventions, [said](#) Oleksandr Tarnavskiy, the commander for the Tavria military sector.

According to Tarnavskiy, Russian troops fired two artillery barrages with munitions containing a chemical substance, presumably **chloropicrin**, on Aug. 6.

Exposure to chloropicrin's vapors [causes](#) severe irritation to the skin, eyes, and, if inhaled, to internal organs. This substance, widely applied during World War I, is no longer authorized for military use.

Tarnavskiy said the chemical weapons were used in the area of Novodanylivka but didn't specify the oblast. There are several settlements in Ukraine called Novodanylivka. Most likely, it was the one located near Orikhiv, Zaporizhzhia Oblast, as it lies the closest to the front line.

No casualties were reported after the shelling, the Ukrainian commander said. "The Russians are trying to do everything to stop our advance. But they won't succeed."

This is not the first time Russia has used chemical weapons in its war against Ukraine.

Ukraine's Border Service [said](#) on May 26 that the Russian military had fired munitions with irritant aerosols and chemical grenades near Avdiivka, Donetsk Oblast.

In December last year, Russian troops [reportedly](#) used Soviet-made K-51 tear gas grenades against Ukrainian soldiers fighting in the east. The 1925 Geneva Protocol prohibits using chemical and biological weapons in war.

Chloropicrin is harmful to humans. It can be absorbed systemically through inhalation, ingestion, and the skin. At high concentrations it is severely irritating to the lungs, eyes, and skin. In World War I, German



ICI C²BRNE DIARY – August 2023

forces used concentrated chloropicrin against Allied forces as a tear gas. While not as lethal as other chemical weapons, it induced vomiting and forced Allied soldiers to remove their masks to vomit, exposing them to more toxic gases used as weapons during the war.

Chloropicrin and its derivative phosgene oxime have been known to damage or compromise earlier generations of personal protective equipment. Allied forces were exposed to chloropicrin on the Italian front during WWII. Some of the soldiers attacked mentioned a white smoke emerging from their gas masks.

These smart glasses are out to replace all other fitness trackers

Source: <https://newatlas.com/wearables/minimis-smart-glasses/>

Aug 09 – While smart shades have not had the best run (sorry, not sorry, [Google Glass](#)), there have been aspects of the technology that have nonetheless offered potential when the focus has been on functionality over fad.

Minimis Glass is stepping up to do just that, with the world's first standalone smart shades designed for fitness tracking, health monitoring and navigation.



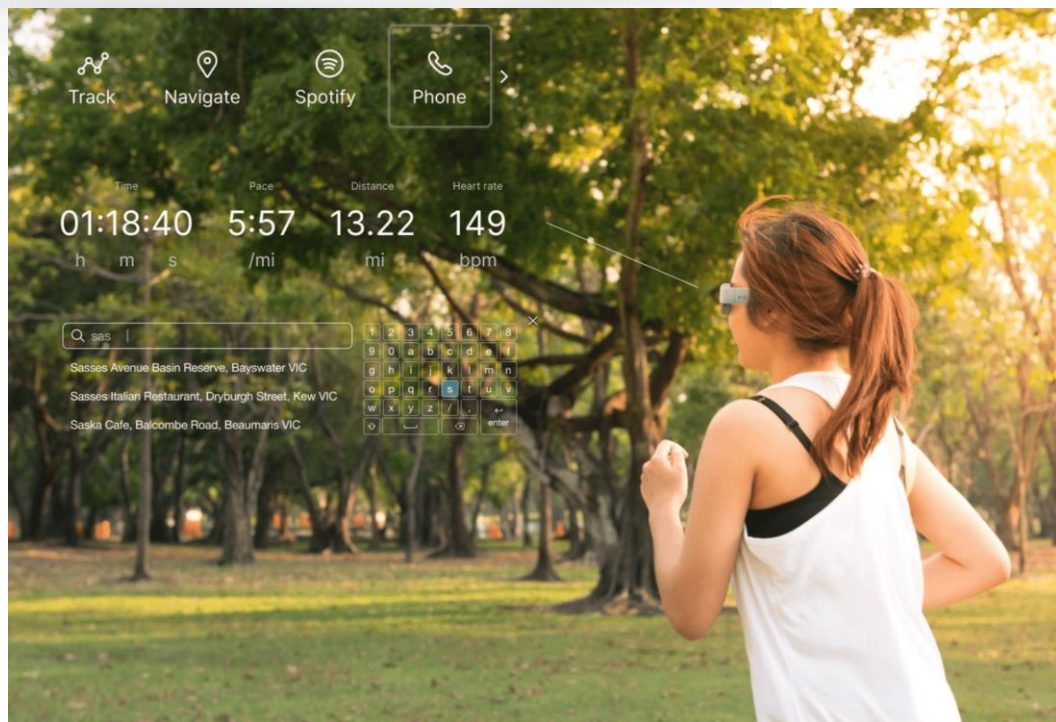
The streamlined glasses, which weigh 90 g (3 oz), don't require a secondary device to operate and can provide workout data and navigational maps in real time. They also can tap into your Spotify account, pairing with Bluetooth earbuds or headphones.

Designed by a fledgling company out of Sydney,

Australia, Minimis founder Joseph Guo wanted to create something perfect for runners and cyclists, removing the need to check a phone screen or wrist tracker for performance stats or route maps.

At 90 g, the glasses should seamlessly slot into your workout routine – Minimis

"I started this to scratch my own itch," said Guo. "I despise sticky running watches and also hate carrying my phone on workouts. I think bike computers are an ugly relic of the last century. It can be dangerous looking down and traveling blind for several meters at a time. The current endurance sporting experience is just so needlessly cluttered and outdated, and there's no alternative. So I made one."



“This is the beginning of a new era for sports wearables; one day we’ll look back at running watches and bike computers as we do now with floppy disks and pagers. How the hell were we content with that?”

While a clear field of view is vital for activities such as running, walking and cycling, Minimis Glass keeps everything clean and simple with an OLED microdisplay in high-definition in the upper third of the glasses screen, ensuring your sight of the road ahead and around you is never obscured.

The shades take an eSIM, are equipped with Wi-Fi and Bluetooth capabilities, and run off a custom Android OS platform. They also feature a heart-rate monitor that tracks your vitals at your temple.

You can expect to get around seven hours of battery life from the two 650-mAh batteries (one in each arm), if you have the glasses powered on continuously, or 11 hours if you’re using them more intermittently.

And as you might expect from a product designed by athletes, the simple things are also provided to make an active life easier: anti-fog, water resistance, ultraviolet ray protection and transition lenses that adjust to your surroundings.

The glasses can be charged with a USB-C cable, but also come with a portable charging case if you become an early adopter (reserve a pair before August 29).

The reserve for Minimis Glass is AU\$699 (**US\$460**), which is 36% off its expected retail price tag and comes with a bonus charging case.

EDITOR’S COMMENT: CBRN First Responders might be interested in this product.

The QUIXOTE Project: “QUICK XOR Technology for BC cold plasma decontamination”

By Karel Mazaneca, and Roman Šmída

Source: <https://hazmat-protect.sujchbo.cz/wp-content/uploads/2019/02/Hazmat-article-Mazanec.pdf>

Abstract

The QUIXOTE project was aimed to develop a Biological and Chemical decontamination equipment form “state of the art” of Non Thermal Plasma, NTP (or also called “cold plasma”) technology, and setting out the technique’s feasibility and scalability as well as evaluating its effectiveness compared to existing responses. The developed NTP devices enable to act effectively on all types of biological and chemical threat agents, in extreme operational environment, over diverse type of samples (surfaces or substrates) by using different “cold plasma” techniques: Atmospheric Pressure Plasma Chamber (APPC) and Atmospheric Pressure Plasma Jet (APPJ). The project has been financed by the CBRN-JIP (contract A-1152-RT-GP). Six consortium members from the military and civilian spheres were carefully selected on the basis of specialist skills and areas of technical expertise deemed ‘key’ to project outcomes, and representing Spain, Poland, Czech Republic and Austria. The technology is clean and green with a bare minimum of environmentally damaging by products. Military Research Institute, was responsible for evaluation of the decontamination efficiency of the developed prototype using 5 different real CWA. The obtained results are presented in the article.



Innovative characteristics:

- Renders standard small- / middle-sized objects safe
- Keeps decontaminated object functionality
- Avoids liquid-based solvents
- Negligible harmless by-products
- Optimized power consumption
- No additional gas in chamber, just atmospheric air

APPC — Atmospheric Pressure Plasma Chamber

The cold-plasma-based decontamination prototype basically consists of a closed chamber containing air at atmospheric pressure. During operation, the



air inside the chamber is energized to generate cold plasma, which produces an atmosphere of highly-reactive species. As a consequence, the long-lived species diffuse from the plasma-generating electrodes across the chamber atmosphere to reach the exposed object surfaces. Therefore, the excited species attack the chemical compounds or living agents that are adsorbed on them and neutralize the hazard.

●► Read also: [QUIXOTE II](#)

Inactivation of ricin by constituents present in a skin decontamination lotion

By R M van den Berg, M J A Joosen, V Savransky, L Cochrane, and D Noort

Chem Biol Interact. 2022 Sep 25;365:110055

Source: <https://pubmed.ncbi.nlm.nih.gov/35963314/>

Abstract

Ricin is a proteinaceous toxin, listed on the schedules of both the chemical and biological weapons conventions. The ease of accessibility to the *Ricinus communis* plant and toxin extraction makes ricin a viable concern for use of intentional release and causal effects. The adverse effects following exposure to the toxin are caused by the bipartite molecular structure of ricin which allows binding to the mammalian cell surface, enter via endocytic uptake, and deliver the catalytically active polypeptide into the cell cytosol where it irreversibly inhibits protein synthesis, causing cell death. In the present study, the inactivation effectiveness of RSDL® (**Reactive Skin Decontamination Lotion**) and its individual inactivating constituents (Potassium 2,3-butanedione monoximate (KBDO) and 2,3-butanedione (DAM)) was evaluated for ricin using a number of read out systems including a cytotoxicity assay, quantitative sandwich ELISA test, and a mass spectrometry-based assay. The results demonstrate that RSDL is able to abolish ricin activity after an incubation time of 30 min as determined in the cytotoxicity assay, and after 2 min as determined in the ELISA assay. Mass spectrometric analysis provided evidence that RSDL is able to induce cleavage of the disulfide linkage between the A- and B- polypeptide chain of ricin which is crucial to the inactivation of the toxin, but this seems not the only mechanism of inactivation. Follow on studies would assist to elucidate the details of the toxin inactivation because it is possible that additional generic mechanisms are in place for denaturation with the RSDL lotion components. This may also provide a promise for testing and inactivation with RSDL of other protein toxins.



Sample processing approach for detection of ricin in surface samples

By Staci Kane, Sanjiv Shah, Anne Marie Erler, and Teneile Alfaro

Journal of Immunological Methods | Volume 451, December 2017, pp. 54-60

Source: <https://www.sciencedirect.com/science/article/abs/pii/S002217591730203X?via%3Dihub>

Abstract

With several [ricin](#) contamination incidents reported over the past decade, rapid and accurate methods are needed for environmental sample analysis, especially after decontamination. A sample processing method was developed for common surface sampling devices to improve the limit of detection and avoid false negative/positive results for [ricin](#) analysis. Potential assay interferences from the sample matrix (bleach residue, sample material, wetting buffer), including reference dust, were tested using a Time-Resolved Fluorescence (TRF) [immunoassay](#). Test results suggested that the sample matrix did not cause the elevated background fluorescence sometimes observed when analyzing post-bleach decontamination samples from ricin incidents. Furthermore, sample particulates (80 mg/mL Arizona Test Dust) did not enhance background fluorescence or interfere with ricin detection by TRF. These results suggested that high background fluorescence in this [immunoassay](#) could be due to labeled antibody quality and/or quantity issues. Centrifugal [ultrafiltration](#) devices were evaluated for ricin concentration as a part of sample processing. Up to 30-fold concentration of ricin was observed by the devices, which serve to remove soluble interferences and could function as the front-end sample processing step to other ricin analytical methods. The procedure has the potential to be used with a broader range of environmental sample types and with other potential interferences and to be followed by other ricin analytical methods, although additional verification studies would be required.





Hazmat Girl Power in Europe, Middle East

Source: <https://www.hazmatnation.com/hazmatters/hazmat-girl-power-in-europe-middle-east/>



May 04 – In 2019 a small group of women set out to take on a big hazmat problem — CBRN. The 10-member CBRN Women are co-located in **Norway and Lebanon** and tout their passion for the work, their wide knowledge of CBRN and their broad reach being from multiple countries and nationalities.

The group is trained in medical preparedness and CBRN incident response.

One of the group's goals is to draw more women into the CBRN-response field, especially in the Middle East. It is a challenging field and the group says it is most proud of its ability to improvise to get the job done.

CBRN Women train no less than three times per year as a team, and they cross train with as many different stakeholders as possible. For example, the team recently completed advanced training in Spiez, Switzerland with the Swiss Army.

One of CBRN Women's biggest challenges is having enough personal protective equipment. Some of that challenge stems from their members being from so many different countries with different cultures.





RiVax Ricin Toxin Vaccine

Source: <https://www.precisionvaccinations.com/vaccines/rivax-ricin-toxin-vaccine>

Soligenix, Inc. RiVax® vaccine is a proprietary heat-stable recombinant [subunit vaccine](#) developed to protect people against exposure to ricin toxin. [RiVax](#) contains a genetically altered version of a Ricin Toxin A (RTA) chain containing two mutations that inactivate the ricin molecule's toxicity, invented initially at the University of [Texas Southwestern](#).

[RiVax](#) primarily consists of two components: 1.) A modified form of the A-chain of the ricin toxin. The modifications have removed the biological activity of the protein while still retaining its shape to trigger an effective antibody response; 2.) Aluminum ("alum") as an adjuvant. RiVax induces human [adaptive immune systems](#) to produce antibodies that recognize and bind ricin toxin, preventing it from getting inside cells and killing them. After intramuscular injection with RiVax, IgG and other antibodies are produced, circulate within the body, and can mop up ricin whether inhaled, eaten, or injected.

RiVax uses [Soligenix's](#) proprietary [ThermoVax®](#) technology that creates a thermostabilized vaccine candidate that can be stored at room temperature for extended periods, making it compatible with U.S. government stockpiling requirements. The [thermostabilized](#) version of RiVax is produced by [lyophilizing](#) (freeze-drying) the vaccine in individual vials to form a solid white cake. This removes water and other components from the material, which would otherwise destabilize the protein. Instead, by using a proprietary process, the protein-aluminum combination remains intact.

The solid, [lyophilized](#) material can then be returned to a liquid form immediately before use by adding sterile water and mixing before injection. Because sterile water is also widespread and very stable, this results in an extremely convenient product that can be stored for extended periods. Long-term storage and ease of use are key attributes for a product that may be stockpiled.

Approval for RiVax is being developed under the U.S. Food and Drug Administration (FDA) "[Animal Rule](#)," which is applied to products where testing in clinical efficacy trials would be unethical.

RiVax received [Orphan Drug](#) and Fast Track designations from the FDA. In addition, RiVax has received an Orphan Drug designation from the [European Medicines Agency](#). As a new chemical entity, an FDA-approved RiVax vaccine has the potential to qualify for a biodefense PRV, which allows the holder an accelerated review of a drug application. On December 20, 2022, the Company announced RiVax®-Vaccinated NHP survival was statistically significantly correlated with an epitope-specific serum assay ([EPICC](#)) prior to challenge. The journal *npj Vaccines* published a related [study](#) on December 16, 2022. The development of RiVax® has been funded through a series of [grants](#) from both the National Institute of Allergy and Infectious Diseases (NIAID) and the U.S. FDA, and ongoing development is sponsored by NIAID contract #HHSN272201400039C.

[Soligenix, Inc.](#) is a late-stage biopharmaceutical company (Nasdaq: [SNGX](#)) focused on developing and commercializing products to treat rare diseases where there is an unmet medical need.



RiVax Indication

[RiVax](#) Ricin Toxin Vaccine is indicated to prevent death following exposure to a lethal dose of ricin toxin that [causes cell death](#) once it penetrates the cell membrane. **Ricin toxin can penetrate cells within four hours of exposure.** Depending on the route of exposure (ingestion, inhalation, or injection), ricin toxin has different initial symptoms. Regardless of the initial route of exposure, ricin poisoning results in death with sufficient exposure.

The Company [says](#) the successful development of an effective vaccine against ricin toxin may act as a deterrent against the actual use of ricin as a biological weapon and could be used to vaccinate military personnel and civilian emergency responders at high risk of potential exposure in the event of a biological attack. There are [no FDA-approved](#) prophylactic or post-exposure therapies for ricin toxin exposure.

RiVax Dosage

RiVax is administered as an [intramuscular injection on 2 or 3](#) occasions, resulting in the adaptive immune system mounting an antibody response. After intramuscular injection with RiVax, IgG and other antibodies are produced and circulate within the body and can mop up ricin whether it was inhaled, eaten, or injected.

●► Read also: [Soligenix](#)



New products by Kappler



DuraChem® 200

DuraChem 200 is multi-hazard High-Visibility apparel that combines FR protection with protection against Chemical, Arc Flash, Steam and Hot Water, and Molten Metal Flash hazards in one cost-effective coverall or ensemble.

[FIND OUT MORE →](#)



DuraChem® 500

Certified to NFPA 1990 (1994) Class 1 Class 1 and Class 2, the only NFPA tactical style CBRN response suit to offer the combined benefit of maximum protection with an affordable price. Available in Tan and Navy.

[FIND OUT MORE →](#)



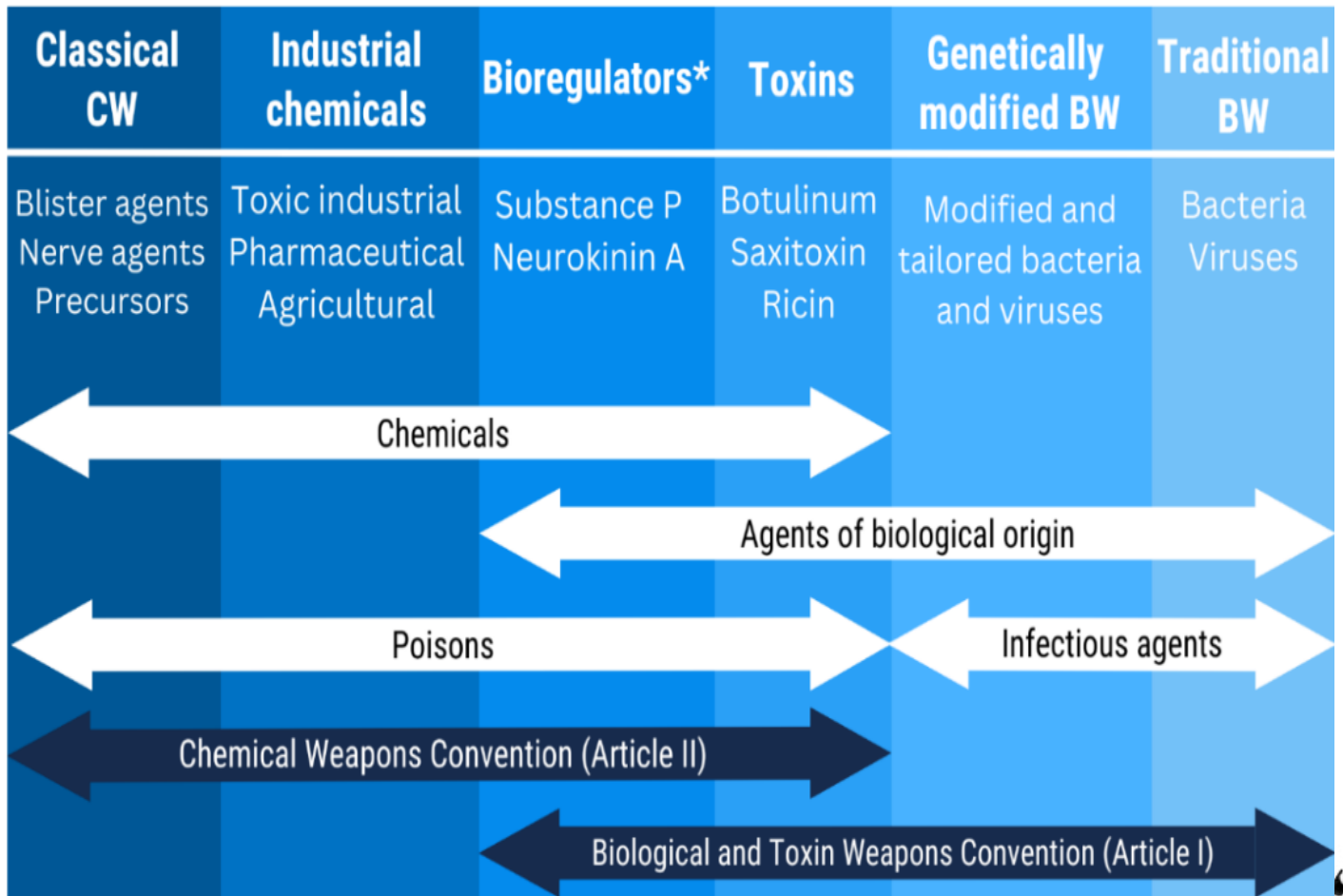
HazMatch™ 4.0

The latest app and online version of Kappler's suit selection tool helps you make informed protective apparel decisions. Includes suit details recommendations and details plus current list of chemicals tested.

[FIND OUT MORE →](#)



Chemical and Biological Conventions



Visual representation of the spectrum of agents covered by the CW Convention and the BTWC



Nigerian humor?



Britain underprepared for chemical and biological attacks, experts say

Source: <https://www.telegraph.co.uk/global-health/terror-and-security/britain-underprepared-for-chemical-or-biological-attack-exp/>

Aug 16 – The Government needs to do more to prepare for chemical and biological attacks, two of Britain’s leading experts have warned.

Daniel Kaszeta, a former White House advisor for chemical and biological preparedness and an associate fellow at the Royal United Services Institute, told the Telegraph that the country’s public services are ill-equipped to respond to such an emergency.

“Police, fire brigades, and NHS organisations that are barely capable of doing their job on a good day, due to systemic running-down of their resources and hence their resilience, are going to struggle with chemical or biological terrorism happening on their patch,” he said.

“We simply do not do emergency planning well and we generally lack resilience.”

Earlier this month, the Government released the 2023 National Risk Register, designating chemical, biological, radiological and nuclear (CBRN) attacks as a serious threat.

Such attacks include the use of chemicals, bacteria, viruses, toxins, or poisons to injure or kill soldiers or civilians.



In the event of a biological or chemical attack, Cobra, the government's emergency situation committee, would be notified and mobilised. Police would lead and coordinate the overall response, relying on the fire brigade and NHS.

Hamish de Bretton-Gordon, former British Army colonel and expert on CBRN and biosecurity, also expressed concern at Britain's capabilities to handle an attack, adding that the threat has never been higher due to the impact of the coronavirus pandemic.

"What Covid-19 has done is brought biological threats into the real world," he said.

"Bad actors are now aware of the potential of a bio-attack to create global mayhem and terror."

He added that "bad actors" could include Isis, who "likely harbours the desire to use them," alongside "lone wolves" who may have technical skills in this area.

"Al Qaeda and Isis are still our greatest threat," he said. "They might be down at the moment, but absolutely not out... We also have Iran and North Korea. Then Russia, who is prepared to do virtually anything and has no regard for collateral damage, or civilian casualties."

Concerns have been heightened by the war in Ukraine, tensions with China, and recent major incidents, including the poisoning of Sergei and Yulia Skripal in 2018.

Colonel de Bretton-Gordon said cities including London, New York and Paris are the most obvious targets. In 1995, the Tokyo subway attack saw the release of Sarin gas on public transport, killing 13, severely injuring 50, and causing temporary vision problems for nearly 1,000 others. A lone wolf killed five people and infected 17 in the United States in 2001 after letters containing anthrax were sent to several news media offices and to Senators Tom Daschle and Patrick Leahy.

Perhaps Britain's best known attack was that in Salisbury in 2018, where the poisoning of Sergei Skripal, a former Russian military officer and double agent for the British intelligence agencies, and his daughter, Yulia Skripal, accidentally killed civilian Dawn Sturgess. However, experts fear that a biological attack, rather than a chemical one, is likely to cause more damage and disruption due to the possibility of a genetically modified infectious agent spreading among a wide number of people.

"From the health side, synthetic biology and manipulation of the genome is not science fiction," said Colonel de-Bretton Gordon, who was involved in a tabletop exercise with academics from Cambridge University which assessed the impacts of a genetically engineered virus that combined the transmissibility of Covid-19 with the pathogenicity of Lassa fever.

"You can imagine if you splice them together, you get a very transmissible, very virulent, agent," Colonel de-Bretton Gordon said. "If that had been Covid, eight million people would have died in this country."

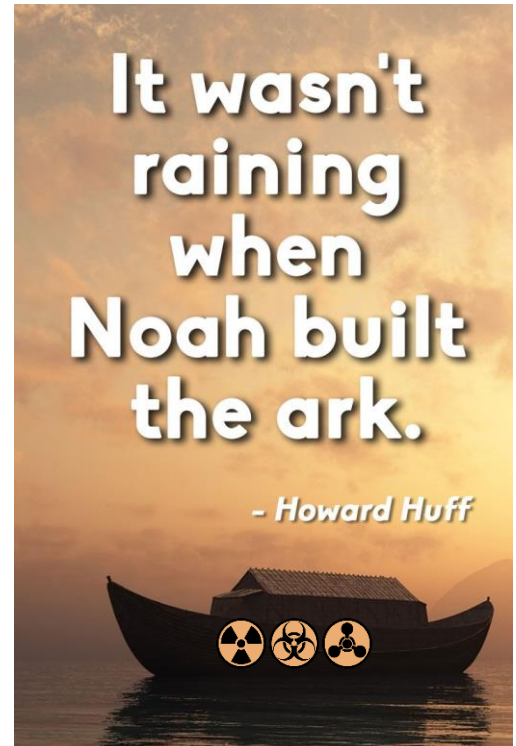
Mr Kaszeta said that it is likely a biological attack may not be noticed at the time.

"The first indication of biological attack may be the sudden onset of sick people in GP surgeries, NHS111, and A&E," he said.

Colonel de-Bretton Gordon said that a global monitoring system, which would track pathogens around the world, could give governments actionable intelligence, so they can make decisions in real time rather than after an attack.

But ultimately, he believes that such a system will not be prioritised by the Government as it is "not an election winner".

"A year after the end of Covid, does the government really want to spend a couple of million pounds setting up a network of sensors in order to prevent the next pandemic? They're all looking at next year's election. Is bio-surveillance going to be an election winner? Probably not."



Training for Hazardous Tasks in Virtual Environments

By Ryan Putman

Source: <https://domesticpreparedness.com/articles/training-for-hazardous-tasks-in-virtual-environments>

Aug 16 – Public safety trainers have been using simulations for as long as public safety has been training. Firefighters do not learn how to pull a hose, raise a ladder, or rescue a child from a window at their first house fire. Paramedics do not acquire the skills to intubate when encountering their first unconscious patient. And police officers do not learn how to make high-risk traffic stops by pulling over their first speeding car. Instead, public safety instructors have used various methods to teach skills and evaluate candidates in simulated exercises. Advances in computerized training, particularly in virtual and augmented reality systems, give instructors new tools to train the next generation.



Background

According to [2022 research](#) by Eduardo Herrera-Aliaga and Lisbell D. Estrada at the Universidad Bernardo O'Higgins in Chile, the first full-body simulator used for training nurses debuted in 1911. CPR class participants are likely familiar with the modern-day equivalents of that first simulator. The aviation industry has been using flight simulators for nearly a century. The Link Trainer is often credited as the first commercially built flight simulator, with more than half a million airmen learning to fly in a Link Trainer during WWII. However, the first customers of the Link Trainer were not



the military but amusement parks, which used these [simulators as rides](#) to attract customers seeking new and thrilling entertainment experiences. Today, it is easier to find a virtual reality (VR) system at an arcade than at the local training grounds.

HazMat Training in Virtual Reality

In 2019, the Hazardous Materials Section of the Utah State Fire Marshal's Office ("the office") learned about a hazardous materials training program that [360 Immersive](#) created for the Rocky Mountain Center for Occupational and Environmental Health. This mobile app program simulated walking through several locations with various hazards, including hazardous materials. By turning the mobile device, the user scanned areas of the scene to spot the dangers.

Based on this experience, the office explored the potential virtual and augmented reality systems available to improve hazardous materials training. One reason the office recognized that hazardous materials training could benefit from virtual and augmented reality systems was due to the cost and complexity of staging simulated exercises. For example, to conduct training exercises on, say, a DOT-406 tank truck hauling gasoline, the office either needed a real DOT-406 tank truck or a mock-up at the training grounds. Even then, it is unlikely the office could set the truck on fire. And while live fire training on transportation props is available at some larger training centers, agencies need personnel and scheduling flexibility to cover shifts in order to get their trainees there. Perhaps a virtual re-creation could help bridge the gap between training conducted during a regular work shift and full-scale exercises at a few specially equipped training centers.

The office explored similar solutions for industries already adopting virtual and augmented reality training. Reading through research papers, the office recognized several benefits: VR training was more effective in [maintaining the trainee's attention and concentration](#) (a real struggle for instructors), and immersive learners [retained 75%](#) of what the training taught in comparison to a 10% retention rate from reading and traditional presentations. Beyond the time and cost savings when trying to recreate complex hazardous materials incidents on the training ground, students could be better prepared using virtual and augmented reality.

The office looked at several VR companies already developing professional training programs. After going through its procurement process, the office started working with [PIXO VR](#) to further develop and adapt a proof-of-concept simulation it had created for Concordia University involving an overturned over-the-road tank truck on fire. That initial proof of concept put the trainee on the scene with the enflamed tank truck. No matter what the trainee did, the tank truck would explode at the end of the scenario.

The office and PIXO VR adapted that first scenario by adding a menu for the instructor to select the type of transport vehicle, chemicals involved, and other container types that might be involved. Then, they added the ability to choose a day or night scene with or without fire. Trainees are expected to don personal protective equipment, identify the material involved using clues such as the vehicle type, container type,



ICI C²BRNE DIARY – August 2023

size, and construction features, and placards, labels, and markings to identify the correct initial isolation distance and public protective measures from the DOT Emergency Response Guidebook (ERG). Trainees could even simulate a water application to control the fire. Up to four participants could be in the simulation simultaneously to work as a crew. After securing additional funding, they were also able to develop a train derailment scenario with standard references available.

Students who used the simulator provided revealing feedback. One interesting note was that many trainees, including experienced firefighters, felt too close to the scene (even though the scenario distances were based on the ERG). This revealed that many experienced responders may be unfamiliar with the initial isolation distances in the ERG and tended to stage much farther away from the scene than recommended.

Another apparent issue of concern is that not everyone is comfortable wearing VR goggles. Problems included the discomfort of having screens strapped to their faces, general aversion toward technology, nausea, motion sickness, and other effects. The VR training roll-out, which coincided with the emergence of the COVID-19 pandemic, compounded problems. Sterilizing the VR goggles between uses became a major deployment factor.

The office also faced difficulty deploying the simulator to other training sites. Because of the limitations of early VR hardware systems available in 2019, the office had to use VR headsets tethered to gaming PCs. This process involved setting up tracking sensors, headsets, and gaming PCs for each training session in a new location, and each training system required a fair amount of space and setup time. The latest generation, which utilizes stand-alone headsets, is much more capable and adaptable. There are trade-offs though. The resolution in the simulation is not as robust. The systems do cost less, and the setup is much simpler.



Look Ahead

Virtual and augmented reality training for first responders continues to grow. The office partnered with BadVR Inc. on the CommandING Tech Challenge, an open innovation prize competition sponsored by National Institute of Standards and Technology (NIST), helping advise on their [Augmented Reality Operations Center](#) product. The challenge tasked participants with creating an incident command dashboard that integrated video feeds, live tracking of responders, building information systems and 3D LIDAR point clouds, and combining it into a single interface for incident commanders. One potential use case for these digital incident command dashboards is tabletop exercises, as they provide an excellent tool with which to do them. Instead of exercise injects utilizing presentation slides, the incidents can be programmed



to occur at pre-set times or after certain actions are taken (or not taken). Several exercise participants can view the scene in real-time together, with the incident progressing in the background as it would in real life.

NextGen Interactions has also participated in prize challenges from NIST, and NIST funding has created [HazVR](#). Participants in HazVR are given a handheld multi-gas meter and must identify sources and concentrations of gas releases. The behavior of gasses released in the simulation is based on the same models that hazardous materials planners currently use for consequence analysis for chemical facilities. Hence, the concentrations and locations are realistic. The handheld multi-gas meters are tracked and can be played back later to show where participants were holding their meters and for how long. During playback, the gasses can also be visualized (even if they were not visible during the training).

Participants have told NextGen Interactions that they now understood after using the system that “low to the ground” meant inches off the ground, not waist level like they had been doing throughout their careers. Tracking how long a meter was held in one location can help teach trainees to slow down as they use their meters. Most people move and walk faster than their meters can accurately measure the atmosphere. This means they could be well into a hazardous atmosphere before their meters tell them it is unsafe.

Conclusion

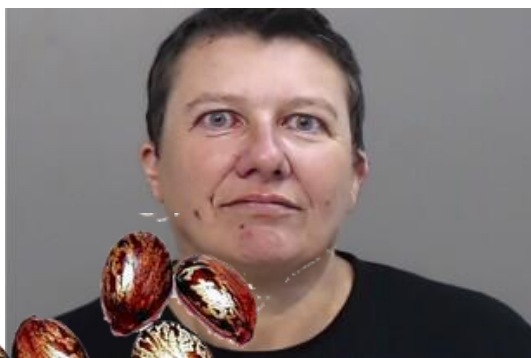
Virtual and augmented reality systems offer new tools to improve the training experience for first responders. Commercial off-the-shelf solutions are available. As more people accept and adopt virtual and augmented reality as a training tool, more solutions are sure to follow.

Like any other technology or training device, virtual and augmented reality systems have advantages and disadvantages. How these technologies improve training will depend on the solutions available to the training agencies and input from the instructors and training programs. These training devices are not a replacement for gifted and competent instructors, hands-on skills development, or traditional practical exercises. Rather, virtual and augmented reality systems provide another tool in the instructor’s toolbox. The success of these training platforms depends on quality instructors who understand how to best leverage new technology to complement their training programs.

Ryan Putman is a deputy fire marshal for the Utah State Fire Marshal's Office. Ryan has over 16 years of public safety experience, working for private emergency medical services (EMS) agencies, and volunteer, part-time/full-time combination, and career fire departments. He started with the State Fire Marshal's Office in 2016 as a hazardous materials instructor and now performs hazardous materials code enforcement and fire investigations for the fire marshal's office. Ryan started the fire marshal's uncrewed vehicle program and is a nationally recognized expert on the use of uncrewed vehicles in hazardous environments, with several published papers and speaking invitations across North America. He also started the virtual reality training program at the fire marshal's office and was a public safety partner for NIST's Public Safety Communications Research CommanDING Tech Challenge. Ryan earned his Associate of Science from Weber State University, Bachelor of Science in Environmental Management from Columbia Southern University, and Master of Science in Management and Leadership from Western Governors University.

Canadian woman sentenced to nearly 22 years for 2020 ricin letter sent to Trump in White House

Source: <https://apnews.com/article/threatening-letter-ricin-donald-trump-white-house-canadian-10666b80df1c0beaf6c48bf4c453a47a>



Aug 17 — A Canadian woman was sentenced to nearly 22 years in prison in Washington Thursday in the mailing of a threatening letter containing the poison ricin to then-President Donald Trump at the White House.

Pascale Ferrier, 56, had pleaded guilty to violating biological weapons prohibitions in letters sent to Trump and to police officials in Texas, where she had been jailed for several weeks in 2019.

Her defense attorney Eugene Ohm said Ferrier has no criminal record prior to that and is an “inordinately intelligent” French immigrant who had earned a master’s degree in engineering and raised two children as a single parent.

But in September 2020, prosecutors said Ferrier made the ricin at home in Quebec and mailed the potentially deadly poison derived from processing castor beans to Trump with a letter that referred to him as “The Ugly Tyrant Clown” and read in



part: “If it doesn’t work, I’ll find better recipe for another poison, or I might use my gun when I’ll be able to come. Enjoy! FREE REBEL SPIRIT.” The letter from Pascale Ferrier, which also told Trump “give up and remove your application for this election,” [was intercepted](#) at a mail sorting facility in September 2020, before it could reach the White House.

She [was arrested](#) trying to enter a border crossing in Buffalo, New York, carrying a gun, a knife and hundreds of rounds of ammunition, authorities said. Investigators also found eight similar letters to law enforcement officials in charge of a Texas jail where she was held after she refused to leave a park area as it closed.

In a winding speech, Ferrier told the judge that she considers herself a “peaceful and genuinely kind person,” but gets angry about problems like unfairness, abuses of power and “stupid rules.” She spoke about feeling like she had done little to support her values while her children were young, and considered herself to be an “activist” rather than a “terrorist.” She expressed little remorse but said, “I want to find peaceful means to achieve my goals,” she said.

U.S. District Judge Dabney Friedrich handed down the 262-month sentence outlined in a plea agreement with prosecutors, which also would expel Ferrier from the country once she is released and require her to be under supervised release for life if she ever returns. The judge noted a “real disconnect” between the Canadian grandmother who has worked toward another degree while behind bars and the crimes Ferrier pleaded guilty to. She pushed back on Ferrier’s framing of her actions. “That isn’t really activism,” she said. “I hope you have no desire to continue on this path.”

Prosecutor Michael Friedman said the sentence was an “appropriately harsh punishment” that sends a clear message.

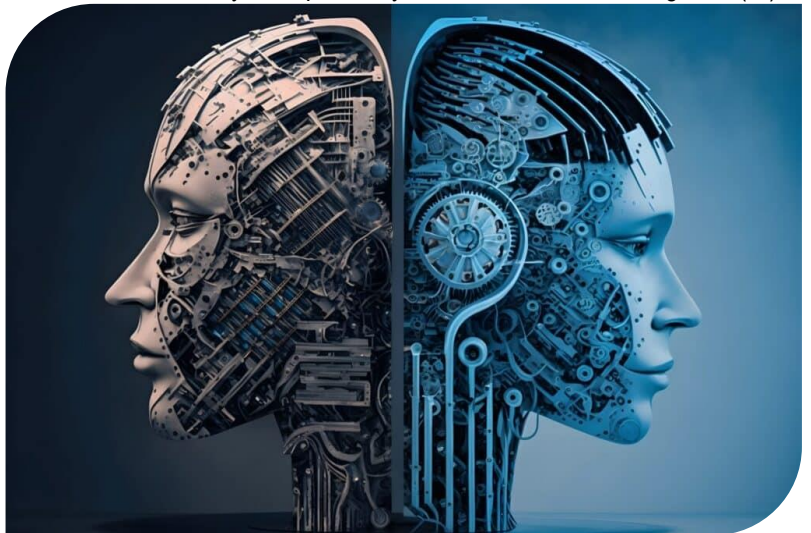
“There is absolutely no place for politically motivated violence in the United States of America,” he said. “There is no excuse for threatening public officials or targeting our public servants.”

Convergence: Artificial intelligence and the new and old weapons of mass destruction

By Emilia Javorsky and Hamza Chaudhry

Source: <https://thebulletin.org/2023/08/convergence-artificial-intelligence-and-the-new-and-old-weapons-of-mass-destruction/>

Aug 18 – Last October, congresswoman Anna G. Eshoo issued an [open letter](#) to the national security advisor and the Office of Science and Technology Policy (OSTP) urging them to address the biosecurity risks posed by the use of artificial intelligence (AI) in both civilian and military applications. She wrote: “AI has important applications in biotechnology, healthcare, and pharmaceuticals, however, we should remain vigilant against the potential harm dual-use applications represent for the national security, economic security, and public health of the United States, in the same way we would with physical resources such as molecules or biologics.” At the UN Security Council’s historic first meeting on the impact of AI on peace and security in July, Secretary General António Guterres echoed this concern, noting that the “interaction between AI and nuclear weapons, biotechnology, neurotechnology, and robotics is deeply alarming.”



The field that explores how the dual-use nature of AI systems can amplify the dual-use nature of other technologies—including biological, chemical, nuclear, and cyber—has come to be known as convergence. Policy thought leaders have traditionally focused on examining the risks and benefits of distinct technologies in isolation, assuming a limited interaction between threat areas. Artificial intelligence, however, is uniquely capable of being integrated with and amplifying the risks of other technologies. This demands a reevaluation of the standard policy approach and the creation of a typology of convergence risks that, broadly speaking, might stem from either of two concepts: convergence by technology or convergence by security environment.

Policy thought leaders have traditionally focused on examining the risks and benefits of distinct technologies in isolation, assuming a limited interaction between threat areas. Artificial intelligence, however, is uniquely capable of being integrated with and amplifying the risks of other technologies. This demands a reevaluation of the standard policy approach and the creation of a typology of convergence risks that, broadly speaking, might stem from either of two concepts: convergence by technology or convergence by security environment.

Convergence by technology. The direct interactions between AI and developments in other technological domains create unique benefits and risks of their own. Examples of this type of convergence



include the interaction of AI with biosecurity, chemical weapons, nuclear weapons, cybersecurity, and conventional weapons systems.

AI and biosecurity. In the context of [evaluating](#) the relative utility of risk assessment frameworks for mapping the convergence of AI and biosecurity risk, researchers John T. O'Brien and Cassidy Nelson define convergence as “the technological commingling between the life sciences and AI such that the power of their interaction is greater than the sum of their individual disciplines.” Their work surveyed potential interactions between domains that could considerably increase the risk of deliberate or accidental high-consequence biological events. This includes, for instance, AI-assisted identification of virulence factors in the *in silico* (via computer simulation) design of novel pathogens. Subsequent work highlighted the [applications of deep learning](#) in genomics, as well as cyber-vulnerabilities within repositories of high-risk biological data. Several recent [articles](#) in the *Bulletin of Atomic Scientists* have identified additional ways in which developments in AI may be accelerating biological risks.

AI and chemical weapons. As part of a convergence initiative at the Swiss Federal Institute for Nuclear, Biological, and Chemical (NBC) Protection, a computational toxicology company was asked to investigate the potential dual-use risks of AI systems involved in drug discovery. The initiative [demonstrated](#) that these systems could generate thousands of novel chemical weapons. Most of these new compounds, as well as their key precursors, were not on any government watchlists due to their novelty. This development must be viewed in light of the advent of large language model-based artificial agents. These are agents that understand how to change open-source drug discovery programs in a similar way, how to send emails and payments to custom manufacturers, and how to hire temp workers to accomplish compartmentalized tasks in the physical world.

AI and nuclear weapons. A [growing amount](#) of [research](#) and [advocacy](#) has highlighted the potentially destabilizing consequences of AI integration into nuclear weapons command, control, and communications (NC3), which are illustrated in the Future of Life Institute film [Artificial Escalation](#). A high-level [discussion](#) involving senior AI experts and government officials broadcast at the Arms Control Association in June laid bare many of the security concerns from this integration. These concerns include an inability to verify and scrutinize AI decision making, a higher risk of the accidental use of autonomous weapons, and an increased likelihood of conflict escalation.

AI and cybersecurity. In the field of cyberspace, [reports](#) have [pointed](#) to the ways that artificial intelligence systems can make it easier for malevolent actors to develop more virulent and disruptive malware. They also help adversaries automate attacks on cyberspaces via novel zero-day exploits (previously unidentified vulnerabilities) targeting command and control, phishing, and ransomware. Autonomously initiated hacking is also expected to be a near-term emergent capability given the current trajectory of AI development.

AI in conventional weapons systems. A key feature of AI is that it enables a single actor to perform activities at scale and at machine speeds. [It has been argued](#) that applying this paradigm to AI integration into conventional weapons systems, such as [antipersonnel drones](#) and drone swarms, creates a new category of weapons with the potential for mass destruction. Further, the United States' [Joint All Domain Command and Control](#) initiative seeks to integrate all aspects of the conventional command and control structure into a single network powered by AI, which carries many risks, including one of [accidental escalation](#). Each of these examples explores interactions between AI systems and specific technologies, but the reality of this landscape is even more complex. For example, how do AI, cybersecurity and nuclear weapons command, control, and communications (NC3) all interact? How does one think about combinations of the above in conjunction with threats to critical infrastructure, such as hacking and disabling power grids or water treatment facilities? How does one evaluate the risks posed by advanced AI systems in connection with traditional security threats and other emerging technologies?

Convergence by security environment. Beyond these questions of direct interaction, it is also critical to consider how an environment in which widespread use of AI systems results in misinformation and increasing deference to technology affects the barriers to weapons of mass destruction (WMD) development and use. Convergence by security environment encompasses situations in which technology developments change the security environment as a whole, creating indirect effects that accentuate overall risks. The impacts here will likely be harder to investigate. Nonetheless, foreseeable examples abound.

One could imagine, for instance, that the development of AI systems that make it easier to craft disinformation and deepfakes could increase misperceptions on the international stage. This would reduce the possibility of successful attribution of biological incidents. There could be an increase in nuclear risk due to the rise of informational asymmetries and signalling failures. Runaway competitive dynamics between two nations on AI development could also push one actor to consider using a weapon of mass destruction or conducting conventional attack on the other.

Beyond typology, another relevant macro question remains: whether to examine convergence risks holistically or to craft individual research spaces for each aspect of convergence. For instance, borrowing from the interdisciplinary [project](#) on biosecurity set up by the Stockholm International Peace Research



Institute (SIPRI) titled “BIO Plus X,” there could be a large field of study titled “AI + X,” which evaluates the impact of AI systems on other technologies and weapons of mass destruction threats holistically, investigating common pathways and remedies. At the same time, it could be that the differences between each convergence pathway (like AI and bio versus AI and nuclear) are so significant that important nuances may be lost in examining these risks together. The likely answer is some mixture of both, but its makeup deserves important consideration.

The different schools of thought on convergence

At face value, the different schools of thought on convergence broadly parallel the division of camps on technological progress. The techno-optimist framing would argue that AI systems would maximize the benefits of these technologies and could help minimize their risks. Benefits include more robust nuclear command and control, speedier vaccine development, and better-trained cyber software; the optimists could make the case that regulation would delay or impede these benefits.

Those with a safety mindset could weigh the concerns discussed in this article much more heavily, reasoning that unregulated AI developments are likely to lead to net reductions in international and national security.

A third camp, wed to the status quo, would point to the lack of empirical research on both the benefits and downsides of convergence and cast doubt more generally on the transformative power of AI systems in either direction.

Given the rapid pace, scale, and ubiquity of AI development and deployment, it is imperative that experts start with a safety mindset. All these technologies have wide dual-use applications, and accelerated development could deliver both benefits and harms. It is already a question of great empirical difficulty to evaluate the benefit-risk balance of each of these technologies. This problem is further compounded by convergence and underscores the need for further research to quantify the upsides and downsides and to investigate frameworks that could accommodate this complexity.

As research is conducted, however, studies demonstrate that defensive technology is often disadvantaged compared to offensive technology in many high-risk arenas. For instance, a very lethal pathogen will generally outcompete the development of a vaccine. It is critical to investigate the balance at the intersection of each of these technologies, but the tendency for emerging defensive technology to lag emerging offensive technology requires that policy makers use the utmost caution in regard to convergence threats.

Policies to safeguard against convergence risks

In addition to further research, there is much that can be done in the policy realm to reduce convergence risks.

First, it is critical for the government to dedicate funding to institutes, such as the National Science Foundation, to improve our understanding of the risks from convergence. This should include exploration of technology convergence in specific domains and security environment convergence, as well as more holistic investigation of the dynamics of threat convergence independent of the technological domain.

Second, Congress may consider a growing roster of policy recommendations already in the public sphere on mitigating risks from specific AI pathways. A recent [report](#)—the culmination of a meeting of high-level experts on AI-bio convergence, convened by the Helena organization in May—provides several recommendations. These include testing large-language models for biological misuse, mandating DNA synthesis screening, and expanding biosecurity and biosafety guidance to include AI-enabled biology. A new [bill](#) in the Senate has built on policy recommendations to prevent the integration of advanced AI into nuclear weapons command, control, and communications (NC3) systems. The National Security Commission on AI [released](#) guidance on strategies to mitigate risks associated with AI in weapons systems, such as proliferation and escalation. As the risks from other convergence pathways are better understood, it is likely that many more high-value policy recommendations will emerge.

Importantly, many of these convergence pathways can likely be narrowed through common policy mechanisms that generally apply to advanced AI systems. For instance, a comprehensive approval process for the deployment of advanced artificial intelligence systems, including mandatory independent auditing and red teaming, could help prevent misuse and unintended consequences by withholding approval for the deployment of systems with a high risk of convergence dangers. Legal liability frameworks to hold AI developers accountable for harms resulting from the systems they create also hold promise for incentivizing major labs to adequately test for and mitigate convergence risks by design. Finally, more coordination and cooperation across different companies and countries to establish common safeguards for AI development are likely to reduce geopolitical tensions and dissuade relevant actors from driving the military use of their AI technologies.

As developments in all these technologies accelerate and nuclear tensions stand at a near-unprecedented high, investigating the convergence of old and new threats will become vital to upholding and advancing national and international security.



Emilia Javorsky MD, MPH is the Director of the Futures Program at the Future of Life Institute. She is also a scientist and mentor at the Wyss Institute at Harvard University.

Hamza Chaudhry is a US Policy Specialist at the Future of Life Institute. Based in Washington DC, his role involves driving engagement with the US Government and other relevant stakeholders on artificial intelligence and other risks from emerging technologies. Hamza previously worked on biosecurity risks at the Nuclear Threat Initiative and Council on Foreign Relations and engaged with AI governance issues as a Harvard AI Safety Fellow. His work on these issues has been featured in *The Lancet*, *Foreign Affairs*, and the United Nations. He is also currently a Youth Biosecurity fellow at the United Nations Office for Disarmament.

CBRN Challenges in Floating Cities

By the Editor-in-Chief



In parallel with vertical cities like NEOM The Line, there is a new trend to construct floating cities due to the threat of rising sea levels attributed to the climate crisis. These innovative projects face new CBRN challenges never addressed before.

Dogen City | Japan



The floating city of Dogen City is a Japanese start-up's response to climate change and the rising sea levels threatening many cities. And it may, if it is ever completed, be the world's healthiest city.

Dogen City is committed to the NEW OCEAN, an ocean business innovation promoted by industry, academia, and government. This has both a social impact (e.g., responding to natural disasters, improving the marine environment, and accommodating climate refugees) and an economic impact (development using new technologies and businesses in addition to traditional shipping, resources, and national defense).

Dogen City is 1.58 km in diameter and approximately 4 km in circumference. This size corresponds to the Japanese concept of "1 ri, 1 hour. With about **10,000 residents** (daytime population: 30,000), the city functions at a city level, but the livability of the city is like that of a small village.

Dogen City self-defines itself as a smart healthcare city floating on the sea that integrates food, architecture, data, energy, and ocean resources with a **focus on healthcare**. The designers of Dogen City are the start-up N-ARK, members of the NEW OCEAN consortium, made up of companies, academics, and government.



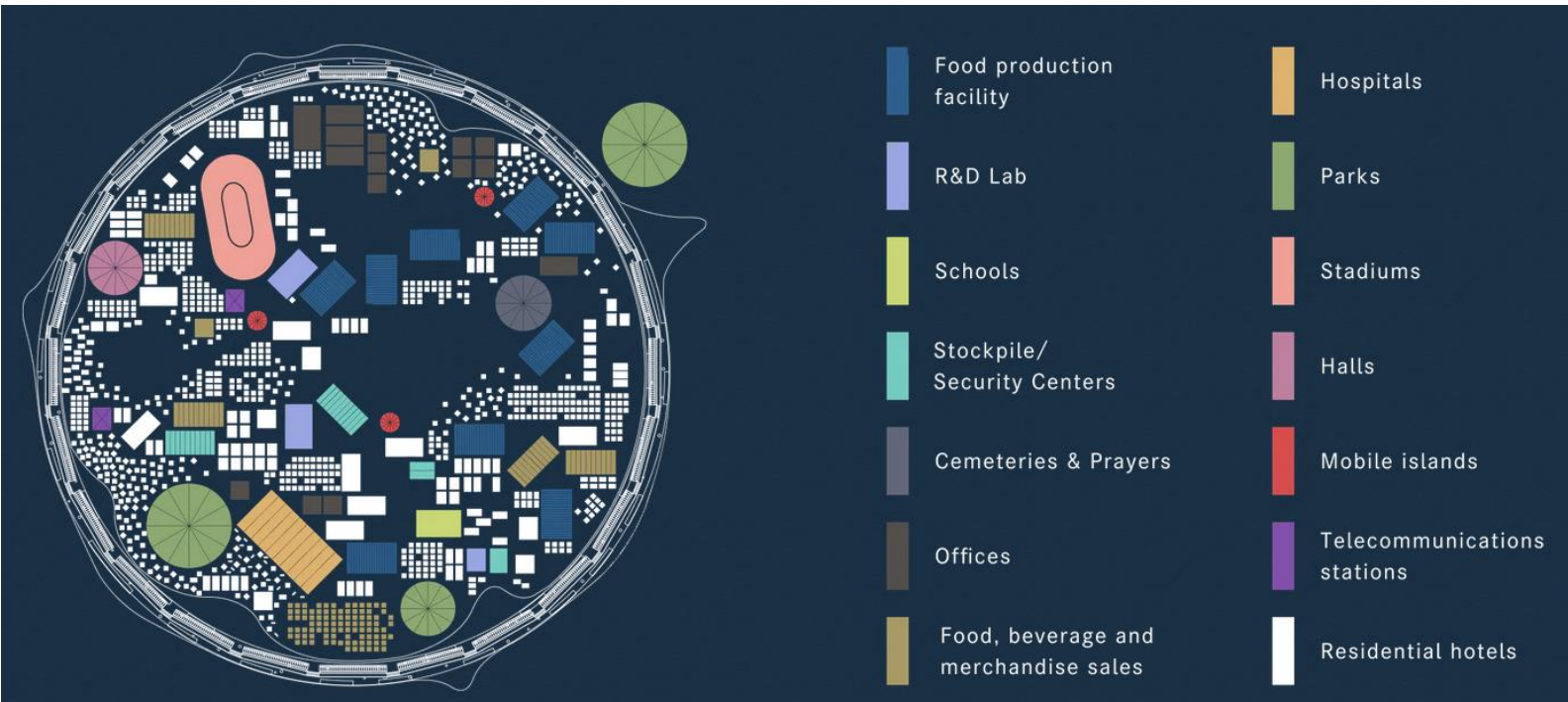
ICI C²BRNE DIARY – August 2023

The aim is to create a maritime economic zone that generates a new economic ecosystem made up of maritime cities and sustainably using the resources offered by oceans.

There will be two aspects to Dogen City, a **social aspect** since it will function as a response to natural disasters and will accommodate climate refugees, and an **economic aspect** with a commitment based on new technologies and business.

Little is known at the moment regarding the exact location and the architectural details of Dogen City, but some information has been disclosed.

The foundations of the Japanese [floating city are being built](#) in the city of **Hamamatsu**, a port located approximately 200 km southwest of Tokyo. The corporation began operations during the second half of 2021, with the development of "Green Ocean", a marine farm based in Lake Hamana.



Dogen City is a sustainable city designed to function as a smart healthcare floating city in peacetime and as a stand-alone city in the event of a natural disaster.

Undersea Edge Data Center: Cooled underwater, it provides high value-added services such as urban management OS, healthcare data analysis, and drug discovery simulation while reducing energy consumption.

Security: EMP attack response, cyber-terrorism response. EMP defense, cyber-terrorism, and stealth functions based on submarine technology.

Healthcare: Residents of Dogen City can receive telemedicine daily by managing and analyzing their living area data through the urban OS "Dogen" from ring devices, blood samples, and genome analysis. Furthermore, when combined with medical data and genome data, the health status of individuals can be more accurately evaluated. Advanced medical care, such as drug discovery simulations and remote robotic surgery, can also be received through computational processing at the undersea edge data center.

CBRN challenges

This floating city has no roads or cars. Given the shape and the size of the island, cars can be substituted by vessels that can approach almost all areas of the island and transfer first responders as close as possible to the incident site. Sea water can be used for decontamination of the population while smart emerging structures can provide decontamination capabilities on-site of mass gathering places. One problem might be the contaminated wastewater management but plasma torch technology can be a solution. The same for the cold plasma technique made for handling big quantities of contaminated water.

Since technological – smart – cities run under unified ventilation/AC systems acquiring access to these centralized systems might be used for spreading CWAs and BWAs to the residencies, offices, and public facilities. Special focus should be given to the training and equipment of the healthcare personnel that by themselves are priority targets – imagine what will be the fate of victims if hospitals are contaminated or



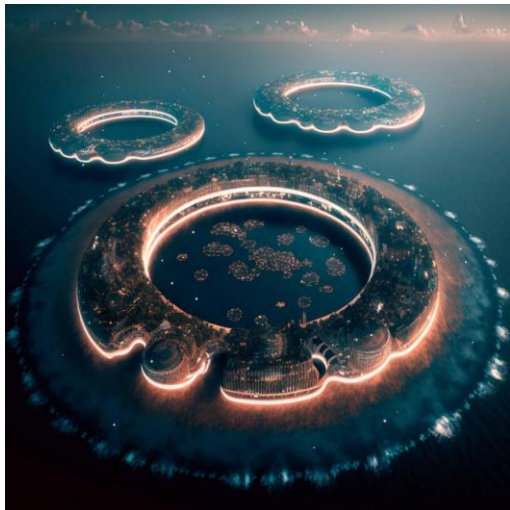
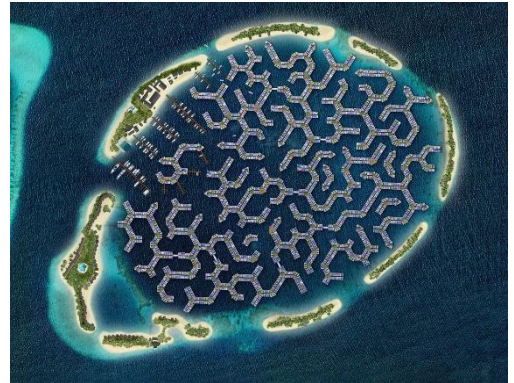
cyber-attacked or both. Such an isolated environment might be ideal for food/water contamination with chemicals or toxins that can survive countermeasures and contaminate the population. In addition, since the floating city is an autonomous community, it should have a specialized pharmaceutical stockpile able to cover its needs for at least 72 hours before organized assistance arrives for the homeland. Since part of the floating city will be “underground” it should be remembered that certain CWAs (i.e., nerve agents) are heavier than air and tend to occupy basements and underground areas heavily affecting people working there. It would be ideal if both residencies, offices, and labs are equipped with filtering systems (HEPA) in specially designed “safe rooms” able to provide protection-in-place for families and workers for 24 hours more. Finally, the entire population of Dogen City should be submitted to specialized training regarding CBRN threats and how to counter them. People (and officials) should understand that “floating cities” are landmarks and as such they are targets as well. Prepare for the unexpected to have a pleasant sleep at night – i.e., have piracy in mind!

Other floating architectures

The floating city concept is not new. Numerous ongoing projects aim to prove that self-sufficient floating cities can be built in the sea.

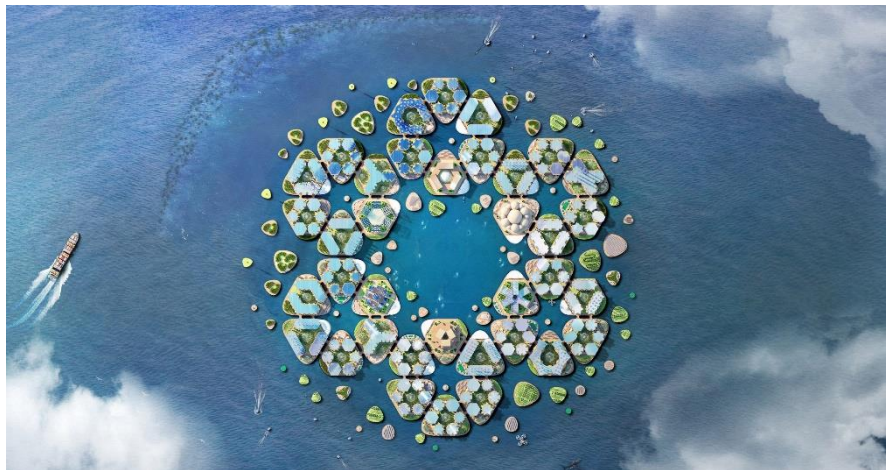
The Maldives floating city

Based on the shape of a local coral called brain coral, and just a ten-minute boat ride from the capital Malé, 5,000 adjoining units will float on one of its 200-hectare lagoons. The Dutch architects Waterstudio and Dutch Docklands, specializing in water-based urban planning solutions, are behind the project.



Polimeropolis

The project proposes the **urbanization of the Great Pacific Garbage Patch** situated in the Pacific Ocean, with an estimated surface area of between 710,000 km² and 17,000,000 km², with a series of giant floating islands that clean the ocean, built from self-capturing recycled plastic. Presented as a scalable staged model of a city, the conceptual project comprises a sequence of mixed-use urban 'rings', each of which houses a cluster of habitats while enclosing a huge oceanic lagoon. The Focaccia Prieto Firm designed it.



Oceanix

In Busan, South Korea, Bjarke Ingels Group (BIG) is designing a floating city prototype, which was first revealed to the world in 2019. Made up of a series of hexagonal platforms, the city is designed to withstand natural disasters such as flooding, tsunamis, and hurricanes. It is initially expected to house around 10,000 residents, but more modular platforms will be added over time. Apart from being protected from flooding, the city will produce its own food, energy, and freshwater with the integration of zero waste and closed-loop systems.

The Inevitable Never Happens
And The Unexpected Always
Happens

~~UNEXPECTED~~



Blood Simple. Several Russian journalists and activists were poisoned in Europe

By Michael Weiss

Source: <https://theins.press/en/politics/264280>

Elena Kostyuchenko, Natalia Arno, and Irina Babloyan, have long worked to expose the Kremlin's lies. While traveling through Europe in the last year, each was poisoned by unknown toxins. Their cases remain unsolved. Why?



Aug 15 – “You cannot return to Russia. You will be killed here.”

Dmitry Muratov, the editor-in-chief of Novaya Gazeta, didn't explain how he came to this dire conclusion, but he said he wasn't taking any chances. His foreign correspondent, Elena Kostyuchenko, who had documented Russian war crimes in occupied Ukraine, had already been warned that she was in danger and he advised her to stay in Europe. Muratov was right.

Six months later, Kostyuchenko would find herself suffering from an acute pain in her abdomen, insomnia, nausea and an extreme case of anxiety. Her face, fingers and toes swelled; her palms turned red and ballooned in size before returning to normal. Something was seriously wrong with her but she didn't know what.

Kostyuchenko was very likely poisoned.

That, at least, is the conclusion of a half dozen doctors, scientists and chemical weapons experts whom The Insider has consulted about her case, which has not been publicized until now. And Kostyuchenko isn't the only suspected poison victim. She is part of a trio of muckraking Russian journalists and dissidents — all of them women, all outspoken critics of Vladimir Putin's regime, and all living and working in different countries outside of Russia — who in the past year have succumbed to a similar set of strange and alarming physical ailments, with circumstantial evidence suggesting foul play. They've found their hotel doors mysteriously prised open, unusual smells lingering in the air of their living quarters, or emanating from their own bodies, as well as meals they've eaten utterly lacking in taste. The European and American authorities these women have relied on for answers have been unable (or unwilling) to do so.



Their unsolved cases, which have all begun after Russia's full-scale invasion of Ukraine on February 24, 2022, follow series of uncannily similar poisonings of other enemies of the Kremlin over the past decade with targets as diverse as Emilian Gebrev, a Bulgarian arms dealer; Sergei Skripal, a British spy who years earlier defected from the GRU, Russia's military intelligence agency; Alexei Navalny and Vladimir Kara-Murza, Russian opposition figures who canvassed and agitated extensively around Russia. These poisonings, as *The Insider* was the first new outlet to determine, were conducted with the military-grade nerve agent Novichok and perpetrated by operatives from the Russian special services.

To hear the 36 year-old Kostyuchenko tell it, her story begins on March 28, 2022, the day *Novaya Gazeta*, one of the last remaining (at least partly) independent news outlets in Russia, published a dispatch from occupied Kherson about the torture and kidnapping of Ukrainian civilians at the hands of Russian soldiers: her subjects were handcuffed to radiators and beaten with rifle butts, their children dragged away with bags over their heads. Two days after her story was published, *Novaya Gazeta*, founded in 1993, decided to close up shop after receiving a second notice issued to it by Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media, Roskomnadzor. Two notices from this bureaucracy usually indicate that a criminal proceeding is imminent. Given the Russian penalty for spreading "disinformation" about the war in Ukraine — which basically amounts to telling the truth about it — is up to 25 years in prison, Muratov preemptively "suspended" the newspaper whose pathfinding investigative reporting won him a Nobel Peace Prize in 2021. A total of seven *Novaya Gazeta* journalists, among them Anna Politkovskaya, [Yuri Shchekochikhin](#), and [Anastasia Baburova](#), have been murdered over the years for their investigative spadework.

The shuttering of her newspaper did not deter Kostyuchenko.

[Elena Kostyuchenko](#)



She was then based in Zaporizhia, in southeast Ukraine, and planned to travel to Mariupol, then still a fiercely contested port city in Donetsk, to chronicle more of the Russian army's activities. But on March 30, Kostyuchenko received a call from another *Novaya Gazeta* colleague. "My sources contacted me. They know that you

are going to Mariupol. They say the Kadyrovites have an order to find you," the colleague told her, referring to Chechen fighters loyal to Ramzan Kadyrov, the warlord president of the Republic of Chechnya.

Kostyuchenko's travel, of which she had only informed two people — Muratov and her editor Olga Bobrova — was evidently also known to nefarious actors within Russia's military presence in Ukraine. As proof, her colleague played an audio tape of Kostyuchenko discussing her trip to Mariupol with a third party, an obvious sign her lines were tapped, most likely by the Federal Security Service, or FSB, which had purview over Russia's occupation zones.

Kostyuchenko recalled an odd sight from her time in Kherson: that of a car parked for two nights in a row — both nights arriving after the 11 p.m. curfew the occupiers implemented — outside the apartment she'd stayed at. The car's headlights were on. At some point on one of the nights, a man exited the car and seemed to be surveilling Kostyuchenko's building. By the time the car was gone, she'd noticed a convex piece of equipment installed on the roof, like a satellite dish, with a long antenna sticking out of it.

Less than an hour after that colleague's call, a source from Ukrainian intelligence got in touch with Kostyuchenko. The murder of a *Novaya Gazeta* journalist was being planned in Ukraine, the source told her. Her name was now given to every checkpoint on the route she'd have to take from Zaporozhye to Mariupol. Muratov rang her next. "You can no longer go to Mariupol. You must leave Ukraine right now." Confronted with such an array of alerts, Kostyuchenko decided not to take chances by staying in Ukraine any further. She reckoned she could wait out the threat in Europe and also finish the book she'd begun writing on "how Russia came to fascism."

She chose Germany as her new home, a country in the heart of Europe where she thought she'd be safe, even though Russian assassins have plied their grim trade there, too, most recently with the August 2019 daylight murder of Chechen dissident Zelimkhan Khangoshvili, who was shot at point-blank range by [Vadim Krasikov](#), an asset of the FSB, in Berlin's Tiergarten park.

Kostyuchenko's calm existence did not last long. In April 2022, Muratov called again with the news that she could not return to Russia for the foreseeable future. If she did, she'd be killed.

So Kostyuchenko rented an apartment in Berlin and found a new job in journalism, working for the independent, Vilnius-based, Russian news site Meduza. Her first planned foreign assignment for the outlet was going to be in Iran. "I had been to Iran and knew how to work there," Kostyuchenko said. "I found



people who would help me, got a visa, and bought clothes. We decided that the second business trip would be Ukraine.” Her prospective travel to Ukraine was hampered by a cyberattack on the Ukrainian embassy in Berlin, which temporarily disrupted the processing of visa applications. This meant that Kostyuchenko had to travel to Munich to get a visa — now required for all Russian citizens — from Ukraine’s consulate. It was 9:30, on the evening of October 17, and Kostyuchenko boarded the night train to Munich. She took off her shoes in the car, and lay down on the seats to sleep for the five-hour journey.

The following morning, Kostyuchenko arrived in the city and met a female friend at the latter’s apartment, where she slept for another hour before making her appointment at the consulate. The same friend (whose name The Insider has agreed to withhold at Kostyuchenko’s request) picked the journalist up by car. The two went to lunch at a local cafe and sat outdoors. The food had no taste, according to Kostyuchenko; she left half her plate untouched. During the course of the lunch, three of the friend’s acquaintances turned up at the cafe, a man, and then two other women. Kostyuchenko remembers wondering if Munich is such a small town that so many familiar people could saunter past the same cafe in the space of an afternoon. Elena excused herself to use the bathroom, perhaps more than once — she can’t quite remember. At around 3:30 p.m. Kostyuchenko and her friend drove back to the train station. During the car ride, Kostyuchenko detected a weird smell coming from her body, not typical body odor. Her friend, normally shy and polite, told her, “You know, you smell bad. I’ll look for deodorant.” But she couldn’t find any.

Kostyuchenko boarded her return train and went to the toilet. Her friend was right about the odor; “I soaked the paper towels and began to dry off,” Kostyuchenko recalled. “It turned out I was sweating a lot. The smell of sweat was sharp and strange -- the smell of rotten fruit.”

The train left Munich station at 4 p.m.. She flipped open her laptop and began to edit the text of her manuscript. Before long, she realized that she was rereading the same paragraph over and over again. Her head was pounding and she couldn’t concentrate. At first, Kostyuchenko thought maybe she’d contracted Covid again. She’d tested positive for the virus three weeks earlier. Another bout would surely scupper Kostyuchenko’s planned trip to Iran, as her girlfriend Yana told her on the phone.

At 8 p.m. her train pulled into Berlin. As Kostyuchenko stepped onto the platform, she realized her strength was gone, as was her ability to focus. With great difficulty she found her way from the station to the subway, and from there to her stop in the German capital. The walk from the subway station, normally no more than five minutes, took fifteen, as Kostyuchenko found her bag enormously heavy and also that she was short of breath. “On the platform, I burst into tears,” she said. “I didn’t understand what direction to go. Other passengers helped me.”

As soon as she reached her apartment, she collapsed on her bed and fell asleep. Kostyuchenko’s girlfriend Yana told The Insider that she looked normal when she arrived, just very tired, and her heart was beating very fast.

The next morning, Kostyuchenko awoke with a severe pain in her abdomen, a bit higher than her stomach. The pain radiated to her spine and she experienced such bad vertigo that she couldn’t get up from bed. Her worst symptom would be insomnia; on the rare occasion that she did get some sleep, the pain in her body would put an end to any respite. Kostyuchenko was also nauseated and sometimes threw up. Rather than call an ambulance, she made an appointment with a clinic, who saw her 10 days later, on October 2. Two doctors informed her she was probably suffering aftereffects of Covid and that she’d recover in six months. They performed an ultrasound and took some blood. Kostyuchenko, her blood screening found, had elevated liver enzymes Alanine transaminase (ALT) and Aspartate transaminase (AST) — five times higher than normal and not associated with Covid. She also had blood in her urine, another condition not linked with the pandemic.

Kostyuchenko was tested for viral hepatitis, in case it was acquired from her foreign travels, but the result was negative. In time, the pain in her abdomen and the dizziness subsided; Kostyuchenko just felt weak and nauseated. Although now new symptoms appeared including palmar-plantar syndrome, the discoloration and swelling of her palms. “The swelling got bigger, my jaw line disappeared, my face was not my face,” Kostyuchenko remembered. “In front of the mirror, I needed time to recognize myself.” She couldn’t get a decent night’s sleep.

One Russian doctor in Berlin, who had previously tended to victims of Russia’s state-sponsored poisoning program including Alexei Navalny and popular author Dmitry Bykov, studied her case at the request of Kostyuchenko’s employers at Meduza. The doctor, who has requested we not name him out of safety concerns, first suggested Kostyuchenko may not be suffering from any natural ailment. As she drove home from the hospital, the doctor texted her: “Is there a possibility you might have been poisoned?” She wrote back: “No, I’m not that dangerous.”

But by November, all other explanations for why she felt so sick were tested and dismissed. On December 12, Kostyuchenko’s ALT level was now seven times higher than normal. Doctors said she had one recourse left, to get tested by specialists at the Charité university hospital in Berlin, the same hospital that treated Navalny after his poisoning in 2020.

In order to test for toxins, however, Kostyuchenko had to file a criminal report with the Berlin police, which she did. She was interrogated for nine hours; her case was handled by the same German investigator who examined the evidence of Khangoshvili’s assassination. He also investigated the poisoning of Pyotr



Verzilov, the producer of punk activist group Pussy Riot, who was exposed to a nerve agent in September 2018 after he ran through the soccer field during the World Cup final match, chased by Russian police in a Benny Hill-like sequence in front of Putin, who was watching in attendance.

The investigator was annoyed that Kostyuchenko waited so long to contact law enforcement; now, two and a half months after her initial symptoms, it would be almost impossible to find any traces of toxins in her body. Kostyuchenko's refusal to accept that she might be the target of an attempted assassination exasperated the German investigator. "That's what you're pissing us off. You arrive



here and think you are on vacation. It's like paradise here. You don't think that you need to be careful. We have political killings here. We have Russian special services. Your carelessness, yours and your colleagues, is beyond [comprehension]."

Kostyuchenko's apartment and belongings were checked for radiation, as was she. "They took away the things I was wearing in Munich," she said. Two days before Christmas, at the prompting of Berlin police, Kostyuchenko was checked into Charité. Doctors there took blood in sufficient quantities to be able to conduct several screenings at once. But when Kostyuchenko requested the results of the tests from the police, they said there'd be a miscommunication and her blood had only been tested for alcohol, narcotics and a concentration of the antidepressants Kostyuchenko was taking. Kostyuchenko's lawyer asked if the doctors

would continue to test her blood, this time for toxins. The police answered that there weren't enough samples left in Charité's laboratory for a new analysis. On January 23, an expert invited by the police tried four times to take Kostyuchenko's blood, each time finding that her blood was "too thick" to take a sample. When Kostyuchenko asked the clinic to find her another expert, the police told her that looking for one would be a "bureaucratic nightmare" and asked Kostyuchenko if her supervising doctor could take blood samples and pass them to the police. Doctors at the clinic Elena had been treated at said they are not able to comply with the legally required chain-of-custody rules and that it was up to the police to organize another testing.

By February 20 the police had given up, telling Kostyuchenko's lawyer that too much time had passed since the possible poisoning for adequate forensic analysis. On May 2, the German prosecutor's office informed the lawyer that they were closing the case due to lack of evidence for a criminal investigation. On July 21, the office reopened it pending additional tests.

The Insider spoke to a host of medical experts, doctors and chemists experienced in diagnosing poisonings including a former lead chemist at the Organization for the Prohibition of Chemical Weapons, the international watchdog. All agreed that Kostyuchenko's symptoms cannot be explained by anything other than exogenous poisoning. Her toxicology indicated acute damage to the liver (thus the significant increase in ALT and AST enzymes) and kidneys. The experts believe Kostyuchenko was exposed to some kind of organochlorine compound, such as dichloroethane. And they further suggest that the poison was absorbed through the skin or ingested.

"I thought I had a toothache and needed to go to the dentist," Natalia Arno told The Insider. "I wasn't even thinking about poisoning." The 47 year-old president of the Washington, D.C.-based Free Russia Foundation, a U.S. non-governmental organization that supports Russian activists, journalists and pro-democracy organizations, has built one of the most effective American NGOs advocating on behalf of dissidents, not just Russians but Belarusians and Kazakhs in exile. The foundation also works to get Ukrainian prisoners of war released from Russian captivity.



The Free Russia Foundation was already declared both an "undesirable" organization in Russia before it played an instrumental role in helping the U.S. government develop a sanctions regime against Putin's entourage. "We were told our sanctions report was on Putin's table in early February," Arno said. Her vice president, Vladimir Kara-Murza, a fellow Washington, D.C. resident, was [poisoned](#) twice with Novichok while traveling through Russia. In April, Kara-Murza was [sentenced](#) to 25 years in prison after having been arrested months earlier for speaking out against the war in Ukraine on the American cable news channel MSNBC.

On May 2, 2023, Natalia Arno participated in a private event in Prague, after which, at around 7:30 p.m. she returned to her hotel, the Garden Court Hotel in the city center. Arno at once noticed the door to her room was open and she'd remembered closing it. Nothing was missing and everything seemed as she'd





left it except for a strange odor resembling perfume, which hadn't been there before. Reception told her the maid had probably left the door open and promised to look into it. Arno went to sleep at around 2 a.m.

[The Garden Court Hotel in Prague](#)

At 5 a.m., she awoke in agonizing pain. Her teeth and tongue were especially sore, and she figured she had a dental problem. She took painkillers, but they didn't work. A few hours later, the pain began to spread further, as if "wandering" through her body: it was in her ears, chest, armpits, and spine. Arno also noticed a "stone" or mineral taste in her mouth. Her vision got blurry. Then her arms and legs went numb.

This wasn't the first time Arno had returned to a hotel room that bore signs of trespass. At the end of July 2021, she attended an event in Vilnius, where she met with activists. While on that trip, she also detected a perfumey smell in her room, albeit weaker than what she experienced now. In Vilnius, she'd broken out in a fever and felt weak, as if stricken with the flu or a cold. The rash soon spread all over her body and she has no known allergies.

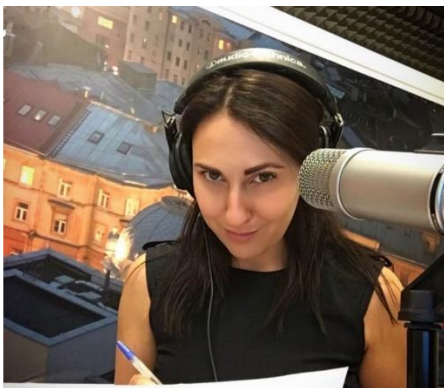
Like Kostyuchenko, Arno waited before seeing a physician, and she didn't see one in Prague. "If I had the slightest suspicion about poisoning I wouldn't have done the transatlantic flight, but went to the clinic in Prague and to the U.S. Embassy in Czechia," she told *The Insider*. Instead, she changed her tickets to catch an earlier flight home to Washington, where she immediately sought medical help. She checked into Inova Alexandria Hospital, in Alexandria, Virginia.

On May 4, she passed all her blood tests, but the oddity of her symptoms added to the suspicious state of her hotel room convinced her to contact the FBI. "They took my blood work, did some other tests and questioned me several times," Arno said. "They took my suitcase and the clothes I was traveling in. One thing they found was an increased level of lead, which may have been due to environmental reasons. They came back a few weeks ago, took more of my clothes and toothpaste and promised to finish the investigation as soon as possible. The first time they came with experts from their chemical laboratory; recently, they brought guys from the biological laboratory. The FBI didn't say this publicly at time but when they first came to the ER in early May and took the first batch of tests, they said it wasn't Novichok."

While the FBI may have ruled out that family of Soviet-developed nerve agents, Arno's doctors maintain she was indeed poisoned, specifically by "nerve toxins."

In mid-October, Irina Babloyan, a 36 year-old journalist with Russian radio station Ekho Moskvyy, relocated from Moscow to Tbilisi, Georgia. She moved into the King Tamar Hotel. On the evening of October 25, Babloyan felt lousy. The next morning she woke up with severe weakness and dizziness.

That night, her palms turned purple and burned as if she were literally playing with fire: Babloyan, too, developed palmar-plantar syndrome, and it soon spread to her feet. Paying little mind to her symptoms, she decided to stick with a planned holiday in Yerevan, the Armenian capital, where she traveled from Tbilisi on the night of October 27. In the car, which someone else was driving, she



became very ill. Babloyan's mind was cloudy and she couldn't concentrate: "I had a feeling that my body was no longer mine; it felt like cotton and I experienced intense anxiety."

[Irina Babloyan](#)

Arriving at her hotel in Yerevan, Babloyan asked for a thermometer. She went up to her room, but couldn't fall asleep. She felt nausea and aching pain north of her stomach, the same as Kostyuchenko. There was a metallic taste in her mouth. Babloyan's skin on different parts of her body turned red. The pain, weakness and insomnia went away after about two days, but the redness persisted.

As with Kostyuchenko and Arno, Babloyan didn't panic enough to see a toxicologist right away. She limited her concerns to have herself tested for allergies. The tests came back negative.



After moving to Berlin a few months later, and having continuing symptoms such as rashes and insomnia, Babloyan submitted blood samples for toxicology testing at the Charité hospital. However, several days later the clinic told her that her samples had been “lost”. Irina was then approached by police investigators who questioned her about the events leading her to suspect poisoning. Following the alleged loss of the initial samples, Babloyan submitted tests anew (results are still pending at press time).

According to the experts interviewed by The Insider, the clinical picture described by Babloyan cannot be convincingly explained by a disease; exogenous poisoning seems to them the most reasonable diagnosis. The experts agree, however, that discovery of the toxin (or toxins) is now unlikely given the elapsed time period since the presumed exposure.

Although their ordeals in the last year remain unexplained, Kostyuchenko, Arno and Babloyan continue to work from abroad. Babloyan is still broadcasting for Ekho Moskvyy from Berlin. Arno remains in the U.S. but has traveled to Europe in recent months as part of Free Russia Foundation’s events, taking, as she told The Insider, the best possible security precautions under the circumstances. Kostyuchenko’s book on Russia’s descent into fascism is due out in a few weeks, and the German police have told her the publicity may do her no favors given that whoever was sent to kill her in Ukraine or Berlin could well be incentivized to try again.

Kostyuchenko has written her own recollection of her suspected poisoning in Russian for Meduza. She urges any other Russians who have fled their homeland and now reside overseas to be careful and to immediately report unusual physical symptoms to medical professionals — also to get in touch with The Insider, which is actively investigating all suspected cases of poisoning. It doesn’t pay to think oneself too harmless to be a target, Kostyuchenko now insists. “I want to live.”

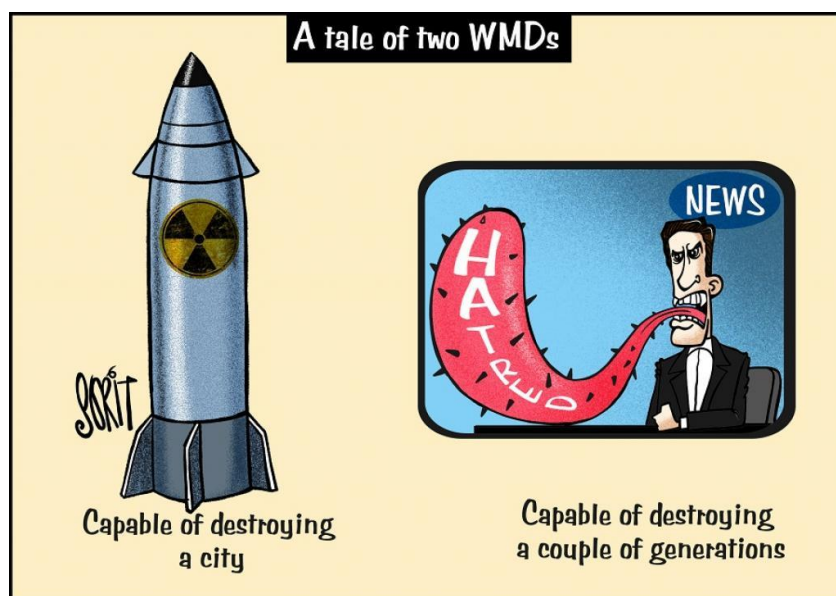


Osama Bin Laden’s Son, Omar: Al-Qaeda Tested Chemical Weapons on Animals in Afghanistan

Video: <https://www.memri.org/tv/bin-ladens-son-omar-al-qaeda-tested-chemical-weapons-animasl-wmd>

Omar Bin Laden, the son of Osama Bin Laden, said in an April 12, 2023 interview that aired on Al-Qabas TV (Kuwait) that Al-Qaeda had experimented with weapons of mass destruction and chemical weapons

in Afghanistan. He said that there was an Iraqi man who had tested such weapons on animals and that although he believes the experiment was successful, such weapons were never employed.



2023 CBRNE-RELATED CONFERENCES



<https://nct-events.com/event>

04-08 September: NCT USA
Aberdeen Proving Ground, Edgewood MD

04-11 November: NCT Asia
Kuala Lumpur, Malaysia



**Dubrovnik, Dubrovnik,
Croatia 23-27
October 2023**



CSCM February, 2022

Announcing the CBRNe Science and Consequence Management 2023 World Congress

<https://cscm-congress.org/conference>

The 2023 CSCM World Congress will be held at Hotel Croatia. Situated across the bay from the historic walls of Dubrovnik, Hotel Croatia is a leading five-star resort and conference hotel on the southern part of the Adriatic Sea. Hotel Croatia's architecture blends seamlessly with its natural surroundings. Shaded by a pine tree forest, while offering spectacular sea views, all 487 rooms feature balconies, which overlook the Adriatic Sea or Cavtat Bay. State-of-the-art facilities include numerous gourmet restaurants, a spa center, and two beaches. Hotel Croatia is ideal for a broader experience of the Dubrovnik Riviera. Suited for business and relaxation alike, the Hotel Croatia serves as an excellent base for exploring the city of Dubrovnik and the Dubrovnik Riviera. The 2023 CSCM World Congress will be held under the auspices of the Government of the Republic of Croatia. In addition, we will enjoy active participation of the RACVIAC Center for Security Cooperation throughout the organization of the Congress as well as many other international and national organizations.



2023
SICC
CONFERENCE
3^o EDITION
SCIENTIFIC
INTERNATIONAL
CONFERENCE ON
CBRNE

CONTACT US :
siccseries@mastercbrn.it

MEET LEARN PUBLISH

SEPTEMBER
2023



İSTANBUL AYDIN ÜNİVERSİTESİ
KBRN
Kemayış, Biyolojik, Radyasyon ve Nükleer Tehditler
www.Istanbulkbrn.org



İSTANBUL AYDIN
ÜNİVERSİTESİ



İSTANBUL AYDIN ÜNİVERSİTESİ
Çevre ve İnsan
Sağlığı Merkezi



CBRN DEFENCE
KİMİKAL, BİYOLÖK, RADYOLÖK, NÜKLEER SAĞLIKAMA
POLİTİKALARI GELİŞTİRME MERKEZİ

<https://istanbulkbrn.org/>



Within the body of Istanbul Aydın University, under the coordination of Istanbul Aydın University Environment and Human Health Application and Research Center (ÇEVSAM) and CBRN Defense Policy Development Association the 1st of the "Istanbul CBRN Days" will be held. This meeting, which will provide the opportunity to share the knowledge and experience of very valuable participants on this subject in the



ICI C²BRNE DIARY – August 2023

national sense, will accelerate the development of scientific infrastructure and studies on CBRN DEFENSE in our country and related institutions and organizations, will ensure that experts and employees in this field get to know each other, share their work and contribute to the increase of cooperation between them. We hope to be found.

CBRN environment; It covers a large number of dead, injured, and environmental effects, especially those who have been infected with biological warfare agents, exposed to chemical warfare agents and/or toxins, and injured as a result of the effects of nuclear weapons and radiation. The COVID-19 pandemic, which has been affecting the whole world for almost the last 3 years, has enabled us to better understand the Biological threat of the CBRN concept, and in a sense, it has revealed how intense and difficult management of CBRN events can cause and can cause mass losses. The threat of CBRN weapons, which started with the terrorist attack of September 11, 2001, and made a name for itself in the recent Syrian internal conflicts in the Middle East geography, including our country, has taken its place in the asymmetric war, and unfortunately, these agents are expected to be used in both war and terror environment in the future.

We think that this meeting, which will bring together many scientists, public and private sector representatives, will bring together many scientists, public and private sector representatives, based in Istanbul, which is the apple of the world's eye, and present the latest developments and technologies in the field of CBRN DEFENSE, and we think that this meeting will partially fill the deficiency of our Istanbul in this field. At the end of the event, we hope to see all the participants among us who will contribute to the "1st Istanbul CBRN Days", where we aim to raise awareness about CBRN threats and dangers.

You can find more detailed information about the KRBN Days, which we plan **to be held in Florya (Halit Aydın) Campus of Istanbul Aydın University on October 20 – 21, 2023**, and which we think will create an important added value for our country, at <https://istanbulkbrn.org/>














*Advancing Technology
for Humanity*

Galveston Bay Section

ISMCR 2023

25th International Symposium on Measurement and Control in Robotics

Iasi, Romania, September 21 – 22, 2023

TC17

<http://ismcr.org/2023-ismcr/>

This symposium will focus on various aspects of research, applications and trends of robotics, advanced human-robot systems and applied technologies, e.g. in the fields of robotics, telerobotics, autonomous vehicles, simulator platforms, as well as virtual/augmented reality and 3D modelling and simulation. Like its previous editions, ISMCR 2023 serves as a forum for the exchange of recent research results and novel ideas in robotic technologies and applications; this time with specific reference to smart mobility.

TOPICS

We are looking for original, high-quality contributions addressing (but not limited to) the following topics:



- | | |
|--|--|
| <ul style="list-style-type: none"> • Robot Design Innovations; • Sensors/Smart Sensors their Integration/Fusion; • Advanced Controls and Actuators; • Methods of Artificial Intelligence in Robotics; • Humanoid, Climbing/Walking, Service, and Autonomous Robots; • Anthropomorphic Robots/Mobile Robots; • Teleexistence/ Telepresence; • Augmented Reality/Mixed Reality/Virtual Reality (VR); • Communication with Realistic Sensations; • Intelligent CAD and IMS; • Visual/Auditory/Tactile/Force Displays; • Tools and Techniques for Modeling VR Systems; | <ul style="list-style-type: none"> • Software Architectures for VR; • VR Interaction and Navigation Techniques, Distributed VR Systems and Motion Tracking; • VR Input and Output Devices; • Innovative Applications of VR; • Human Factors in VR; • Evaluation of VR Techniques and Systems; • Internet and VRML Application of VR in all areas; • Interactive Art and Entertainment; • Education and Entertainment Robots; • Medical and Healthcare Robots; • Micro and Nano Robots; • Innovative Robotics Applications. |
|--|--|

NATO EOD Demonstrations and Trials 2023

Future EOD development in light of the modern conflicts and technological progress

11 - 12 OCTOBER 2023
INCHEBA EXPO Bratislava, Slovakia

Defense & Security 2023 Tri-Service Asian Defense & Security Exhibition Conference and Networking Event

Power of Partnership

6-9 November 2023

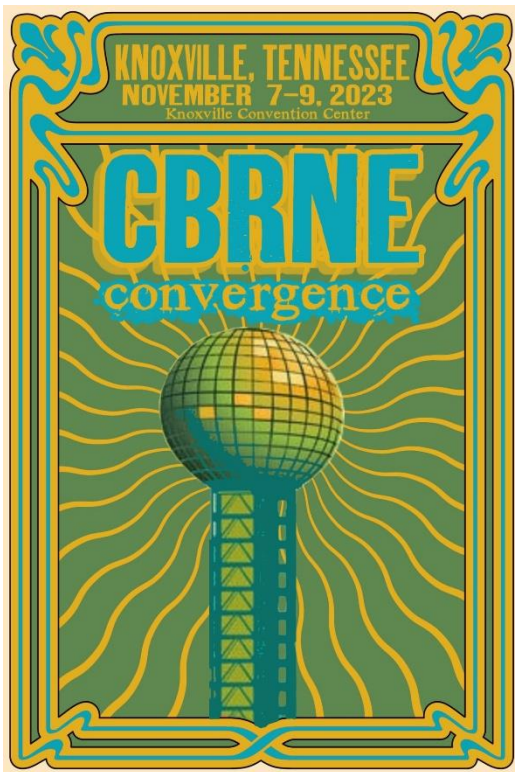
IMPACT, Muang Thong Thani, THAILAND

EGYPT
DEFENCE
EXPO

4-7 DECEMBER 2023

EGYPT INTERNATIONAL EXHIBITION CENTRE





<https://cbmeworld.com/events/knoxville>

2023 sees us back in the great state of Tennessee! 2019's Nashville event was a crowd favourite, and this year will see us move from the home of country music to the home of radiation detection – Knoxville! Knoxville is the host city to the world famous Oak Ridge National Laboratory/Y12 facilities, and we'll be bringing chemical and biological defence to match their nuclear excellence!

This will be our traditional two day conference and exhibition, with streamed sessions to allow delegates to choose their learning path. We're also planning on two pre-event workshops, more information will be announced soon, but one will be on 'Improved radiological response.'

The exhibition already promises to be the largest in the US in 2023, with space for over 70 vendors, covering all aspects of CBRN response. As usual the programme has some of the most knowledgeable CBRN speakers from around the world, more information on which can be found on the [speakers page](#).

We are excited to be working with the [Oak Ridge Enhanced Technology and Training Center \(ORETTC\)](#) for our pre conference workshop on the 7th November. Workshop attendees will have the rare opportunity to visit the Oak Ridge Enhanced Technology and Training Center (ORETTC)—part of NNSA's Y-12 National Security Complex. This is usually closed to international visitors, but CBRNe Convergence has negotiated a chance to be educated by some of the best rad/nuke professionals worldwide!

Delegates will learn about some of the latest radiological/nuclear response training methods and techniques being used in the newly-opened, state-of-the-art Emergency Response Training Facility (ERTF) on the ORETTC campus. The \$15.1M facility enables the development of innovative approaches for emerging technological challenges and risk mitigation for critical infrastructure. ERTF provides local, state, national, and international organizations and government agencies with access to hands-on experience in high-consequence operations, emergency management, state-of-the-art technology, training evaluation and performance testing, and other advanced technical and tactical training areas.



<https://ciprna-expo.com/>

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.



Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as “critical infrastructure owners and operators”). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

The Critical Infrastructure Protection and Resilience North America conference will again bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing North America.

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

ISMCR2023 – 25th International Symposium on Measurement and Control in Robotics

Iasi, Romania, September 21 – 22, 2023

<https://ismcr.org/2023-ismcr/>



HYBRID EVENT: For those who, for many reasons, could not travel to Romania, online presentations will be possible

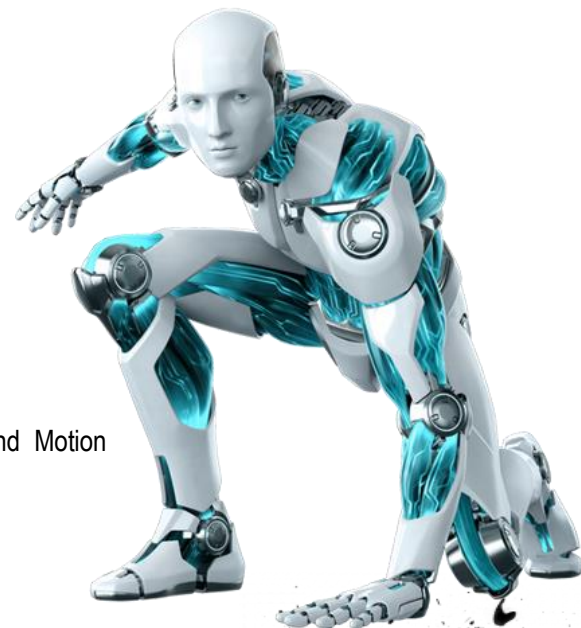
This symposium will focus on various aspects of research, applications and trends of robotics, advanced human-robot systems and applied technologies, e.g., in the fields of robotics, telerobotics, autonomous vehicles, simulator platforms, as well as virtual/augmented reality and 3D modelling and simulation.

Like its previous editions, ISMCR 2023 serves as a forum for the exchange of recent research results and novel ideas in robotic technologies and applications; this time with specific reference to smart mobility.

TOPICS

We are looking for original, high-quality contributions addressing (but not limited to) the following topics:

- Robot Design Innovations;
- Sensors/Smart Sensors their Integration/Fusion;
- Advanced Controls and Actuators;
- Methods of Artificial Intelligence in Robotics;
- Humanoid, Climbing/Walking, Service, and Autonomous Robots;
- Anthropomorphic Robots/Mobile Robots;
- Teleexistence/ Telepresence;
- Augmented Reality/Mixed Reality/Virtual Reality (VR);
- Communication with Realistic Sensations;
- Intelligent CAD and IMS;
- Visual/Auditory/Tactile/Force Displays;
- Tools and Techniques for Modeling VR Systems;
- Software Architectures for VR;
- VR Interaction and Navigation Techniques, Distributed VR Systems and Motion Tracking;
- VR Input and Output Devices;
- Innovative Applications of VR;
- Human Factors in VR;
- Evaluation of VR Techniques and Systems;
- Internet and VRML Application of VR in all areas;
- Interactive Art and Entertainment;



ICI C²BRNE DIARY – August 2023

- Education and Entertainment Robots;
- Medical and Healthcare Robots;
- Micro and Nano Robots;
- Innovative Robotics Applications.

Correspondence Address

- ✓ Prof. Ioan Doroftei: ioan.doroftei@academic.tuiasi.ro
- ✓ Prof. Yvan Baudoin: yvan.baudoin@ici-belgium.be



The escalating prevalence of natural, incidental, and intentional CBRNe (Chemical, Biological, Radiological, Nuclear, and Explosive) threats has underscored the crucial need to enhance risk analysis, preparedness, mitigation, response, and recovery capabilities in the face of unconventional events or incidents. In response to this demand, we are pleased to announce a comprehensive training course designed to equip participants with the essential knowledge and skills required for the effective management of CBRNe events at both regional and national levels. Moreover, the course goes beyond theoretical learning, offering a unique practical exercise conducted at the CBRN Department of University of Health Sciences. This activity will provide trainees with hands-on experience and practical insights, ensuring their preparedness to handle real-life scenarios.

Training program general objective: The Course covers an extensive range of essential subjects related to CBRNe materials, prevention, protection measures, medical procedures, risk assessment, response to CBRNe events/incidents, and inter-agency coordination and communication. Throughout the Course, attendees will actively participate in discussions and interactive sessions, fostering a dynamic learning environment. To ensure a comprehensive training experience, CBRN exercise simulations will be conducted using EMS training manikins, PPEs, gas masks, along with a decontamination station. The organizing institutions will issue a final certificate of attendance.

Target Group: This specialized course is tailored to cater to emergency management personnel, emergency medical services, fire service personnel, governmental administrative staff, healthcare professionals, law enforcement personnel, armed forces, public health officials, public safety communications experts, and public works personnel. By attending this comprehensive training program and participating in the practical exercise at the state-of-the-art facilities of the CBRN Department at the University of Health Sciences, participants will be equipped with the necessary expertise to confidently handle CBRNe events and effectively collaborate with diverse agencies during crises.

Course Main Topics:

- CBRNe risks and new threat scenarios.
- CBRN agents
- CBRNe detection
- CBRNe protection
- CBRNe decontamination
- CBRNe events medical management



ICI C²BRNE DIARY – August 2023

Place and Dates: 2-day training with tech lectures & live exercises by international experts at CBRN Department of University of Health Sciences, Ankara, Turkey. Dates: 19-20 Sept 2023. Working time: 09:00 a.m. - 12:00 p.m./01:00 p.m. - 05:30 p.m.

Directors: Prof. Levent Kenar (University of Health Sciences, Faculty Staff of CBRN Dept., Professor of CBRN Defence and Laboratory Medicine), Prof. Roberto Mugavero (President European Centre for Disaster Medicine – Observatory on Security and CBRNe Defence, Faculty staff University of the Republic of San Marino University of Rome “Tor Vergata” - DIE), Prof. Dr. Selçuk Kılıç (University of Health Sciences, Head of CBRN Dept.)

Course Fee: 300 Euro. Payment via bank transfer. Coffee breaks and lunch are included for both days of the Course.

●► Contact: via email cemec.info@iss.sm

ABSA INTERNATIONAL
The Association for Biosafety and Biosecurity

#BiosafetyNE2023 f t i

REGISTRATION NOW OPEN!

**66th Annual
Biosafety and
Biosecurity
Hybrid Conference**

Omaha, Nebraska, USA

October 13-18, 2023

CHI Health Center

The ABSA International Conference is the largest biosafety and biosecurity conference in the world! The conference will provide solutions to tackle your most challenging issues, present fascinating case studies, and showcase the latest developments in biosafety and biosecurity. ABSA International's educational sessions offer insights into the ever-changing world of biosafety and biosecurity, keeping you updated on the latest techniques and best practices. You'll have opportunities to network with your peers and discuss common issues, share advice, and exchange ideas. There will also be commercial exhibits showcasing the latest technologies in biosafety and biosecurity.



ICI
International
CBRNE
INSTITUTE



BIO NEWS



The pandemic
is OVER!

Pandemic by numbers (as of August 24, 2023)

	CASES	DEATHS	COUNTRIES & TERRITORIES	MOST AFFECTED COUNTRIES*
COVID-19	(689,124,038) 694,122,809	(6,881,401) 6,910,119	229	USA, India, Brazil, France, Germany, Japan, S. Korea

* over 30 million cases | numbers in parenthesis are patients of previous month

100-Year-Old Treatment Inhibits COVID-19 Infection

Source: <https://news.rpi.edu/content/2023/07/24/100-year-old-treatment-inhibits-covid-19-infection>

July 24 – A team of researchers led by Rensselaer Polytechnic Institute's [Jonathan S. Dordick, Ph.D.](#), Institute Professor of Chemical and Biological Engineering, has illuminated a new possibility for the treatment and prevention of COVID-19 in research published in [Communications Biology](#).

The team found that **suramin**, a 100-year-old drug still used for human sleeping sickness that has many other potential applications, inhibits the infection of SARS-CoV-2.

"Suramin binds to the ACE2 and cell surface heparan sulfate binding sites on the receptor binding domain (RBD) of the viral spike (S) protein in vitro," said Dordick. "Both ACE2 and heparan sulfate help the coronavirus infect cells. Suramin, therefore, shows great promise as a treatment for COVID-19." Heparan sulfate and suramin had enhanced preferential binding for the S-protein RBD of the omicron variant, and suramin was most effective against the live SARS-CoV-2 omicron subvariant (B.1.1.529) when compared to wild type and delta (B.1.617.2) subvariants in vitro. Interestingly, it had been shown previously in the literature that suramin inhibits the virus RNA-dependent RNA polymerase, a target for the antiviral agent Remdesivir. Thus, the drug's new S-protein target suggests a broad and independent mechanism of action, which may be an advantage in antiviral therapy. "Suramin and other polysulfated molecules, which target S-protein binding, should be further explored for their potential to inhibit SARS-CoV-2 infection," said Dordick. "Importantly, as the SARS-CoV-2 virus continues to evolve, it appears to obtain even greater affinity for target cell heparan sulfate, which makes suramin even more effective in blocking this interaction. This is hypothesized to be the reason suramin is more effective on omicron than on delta or the original (wild-type) S-protein."

Currently, suramin is not approved in the United States due to toxicity concerns. Further studies may demonstrate the effectiveness of repurposed suramin as a COVID-19 therapeutic or as a post-exposure prophylaxis such as a nasal spray.

Dordick, who is a member of the Shirley Ann Jackson, Ph.D. Center for Biotechnology and Interdisciplinary Studies, was joined in the research by Rensselaer's Robert J. Linhardt, Shirley Xu, Seok-Joon Kwon, Andre L. Rodrigues, Maisha Feroz, Keith Fraser, Peng He, and Fuming Zhang; University of Washington's Paul S. Kwon; and Korea Research Institute of Bioscience and Biotechnology's Hanseul Oh and Jung Joo Hong.



Frozen Pathogens Are Waking Up, And Scientists Say the Risk Is Real

By Corey J. A. Bradshaw and Giovanni Strona

Source: <https://www.sciencealert.com/frozen-pathogens-are-waking-up-and-scientists-say-the-risk-is-real>

July 28 – Science fiction is rife with fanciful tales of deadly organisms emerging from the ice and wreaking havoc on unsuspecting human victims. From [shape-shifting aliens](#) in Antarctica, to super-parasites emerging from a [thawing woolly mammoth](#) in Siberia, to exposed [permafrost in Greenland](#) causing a viral [pandemic](#) – the concept is marvellous plot fodder.

But just how far-fetched is it? Could pathogens that were once common on Earth – but frozen for millennia in glaciers, ice caps and [permafrost](#) – emerge from the melting ice to lay waste to modern ecosystems? The potential is, in fact, quite real.



Dangers lying in wait

In 2003, [bacteria were revived](#) from samples taken from the bottom of an ice core drilled into an [ice cap](#) on the [Qinghai-Tibetan plateau](#). The ice at that depth was more than 750,000 years old. In 2014, a giant "zombie" Pithovirus sibericum [virus](#) was [revived from](#) 30,000-year-old Siberian permafrost. And in 2016, an outbreak of [anthrax](#) (a disease caused by the bacterium *Bacillus anthracis*) [in western Siberia](#) was attributed to the rapid [thawing of *B. anthracis* spores](#) in permafrost. It killed thousands of reindeer and affected dozens of people. More recently, scientists found [remarkable genetic compatibility](#) between [viruses](#) isolated from lake sediments in the high Arctic and potential living hosts. Earth's climate is warming at a [spectacular rate](#), and up to four times faster [in colder regions](#) such as the Arctic. Estimates suggest we can expect [four sextillion](#) (4,000,000,000,000,000,000,000) microorganisms to be released from ice melt each year. This is about the same as the estimated number of stars [in the Universe](#).

However, despite the unfathomably large number of microorganisms being released from melting ice (including pathogens that can potentially infect modern species), no one has been able to estimate the risk this poses to modern ecosystems.

In [a new study](#) published today in the journal *PLOS Computational Biology*, we calculated the ecological risks posed by the release of unpredictable ancient viruses. Our simulations show that 1% of simulated releases of just one dormant pathogen could cause major environmental damage and the widespread loss of host organisms around the world.

Digital worlds

We used a software called [Avida](#) to run experiments that simulated the release of one type of ancient pathogen into modern biological communities. We then measured the impacts of this invading pathogen on the diversity of modern host bacteria in thousands of simulations, and compared these to simulations where no invasion occurred. The invading pathogens often survived and evolved in the simulated modern world. About 3% of the time the pathogen became dominant in the new environment, in which case they were very likely to cause losses to modern host diversity. In the worst (but still entirely plausible) case scenario, the invasion reduced the size of its host community by 30% when compared to controls. The risk from this small fraction of pathogens might seem small, but keep in mind these are the results of releasing just one particular pathogen in simulated environments. With the sheer number of ancient microbes being released in the real world, such outbreaks represent a substantial danger.

Extinction and disease

Our findings suggest this unpredictable threat which has so far been confined to science fiction could become a powerful driver of ecological change. While we didn't model the potential risk to humans, the fact that "time-travelling" pathogens could become established and severely degrade a host community is already worrisome. We highlight yet another source of potential species extinction in the modern era – one which even our [worst-case extinction models](#) do not include. As a society, we need to understand the potential risks so we can prepare for them. Notable viruses such as [SARS-CoV-2](#), [Ebola](#) and [HIV](#) were likely transmitted to humans via contact with other animal hosts. So it is [plausible](#) that a once ice-bound virus could enter the human population via a [zoonotic pathway](#).

While the likelihood of a pathogen emerging from melting ice and causing catastrophic extinctions is low, our results show this is no longer a fantasy for which we shouldn't prepare.

[Corey J. A. Bradshaw](#) is a Matthew Flinders Professor of Global Ecology and Models Theme Leader for the ARC Centre of Excellence for Australian Biodiversity and Heritage at Flinders University

[Giovanni Strona](#) is a Doctoral program supervisor at the University of Helsinki.

Ancient Worm Resurrected After 46,000 Years of Death-Defying Limbo

Source: <https://www.sciencealert.com/ancient-worm-resurrected-after-46000-years-of-death-defying-limbo>



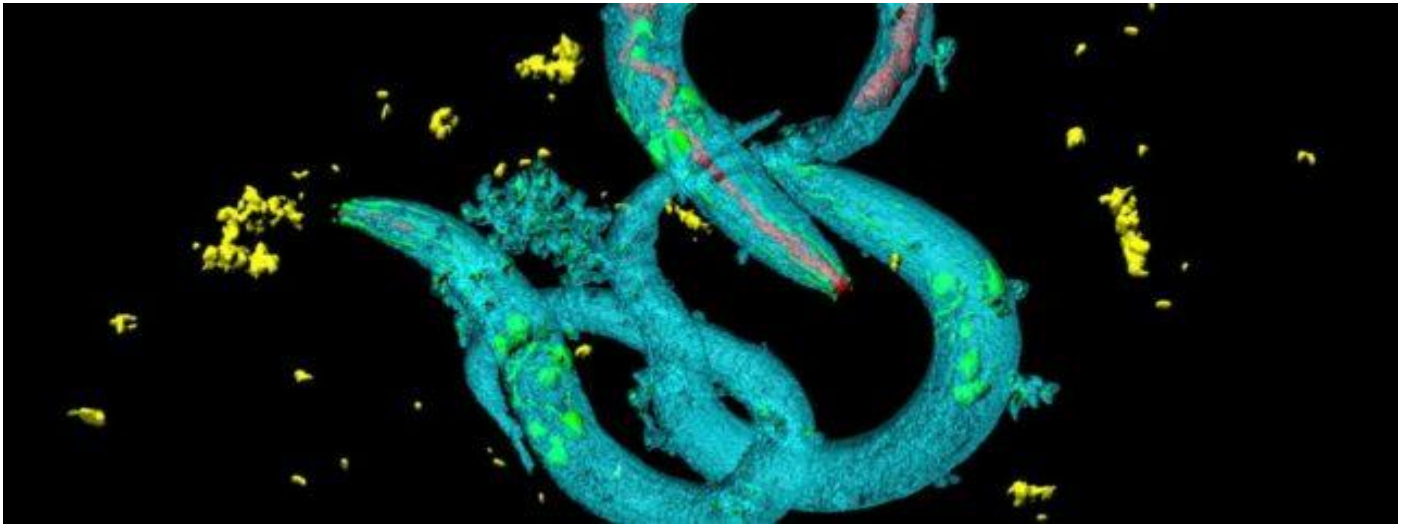
July 28 – An international effort to revive an ancient roundworm, frozen in Siberian permafrost for millennia, has unleashed a lifeform even older than scientists once thought.

[In 2018](#), several resurrected nematodes, of the genus *Panagrolaimus*, were dated to around 32,000 years old. But now, more precise radiocarbon dating suggests these soil worms have remained 'dead awake' in parts of Siberia since at least the late Pleistocene, around 46,000 years ago.

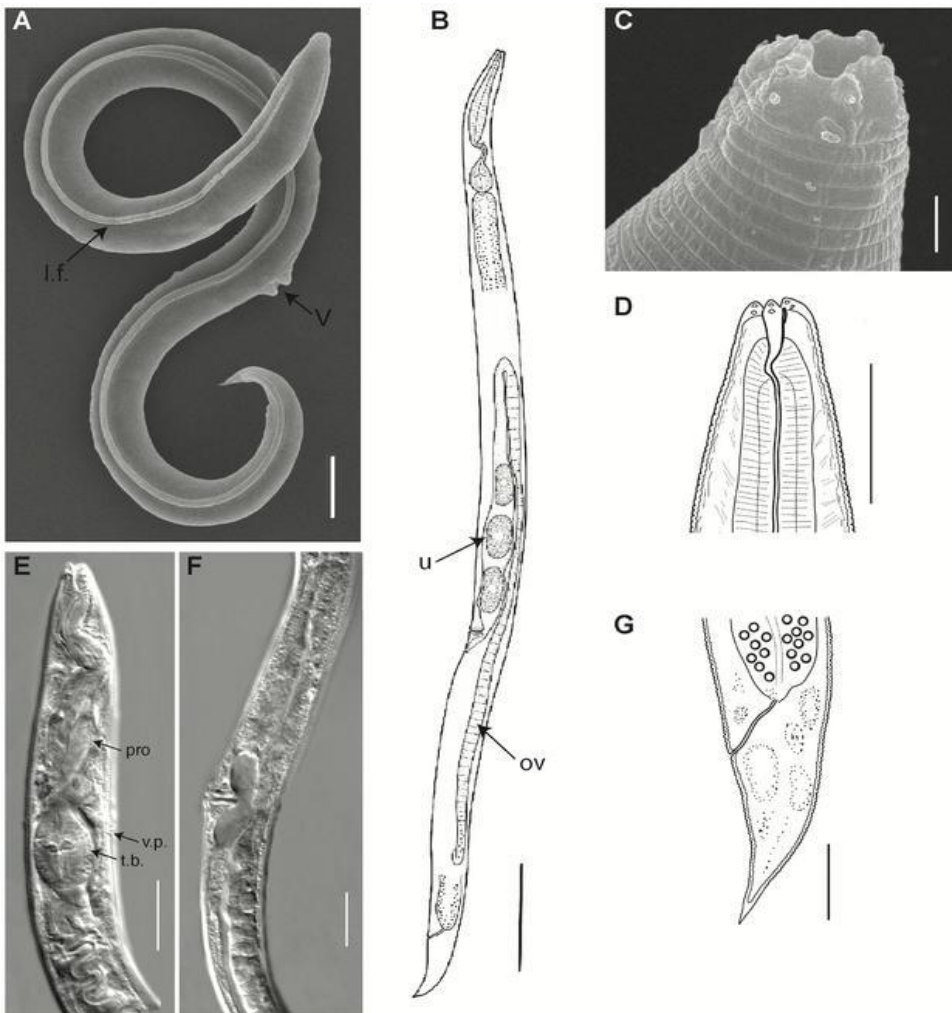
If correct, the record absolutely smashes the longest known state of extreme inactivity observed among animal life, a phenomenon known as cryptobiosis.

After reviving the frozen worm in the lab and cultivating it for over 100 generations, researchers, led by experts at the Max Planck Institute in Germany, ran a genome analysis.





C. elegans. (HeitiPaves/Getty Images)



They claim this creature is a newly recorded species, which they call *Panagrolaimus kolymaensis*. To date, scientists know of very few animals capable of suspending themselves in a limbo-like state in response to tough environmental conditions.

The general morphology of *P. Kolymaensis*, (Shatilovich et al., *PLOS Genetics*, 2023/CC-BY 4.0)

Tardigrades, nematodes, and microscopic aquatic organisms, called [rotifers](#), are just a few of the animals known to enter cryptobiosis. For all we know about the unique state of life, these animal could very well remain in this desiccated, or dried out, state 'indefinitely' – or at least until conditions are better for survival. The longest recorded time spent in cryptobiosis among living worms is only 39 years.

Even tardigrades have only re-entered their normal metabolic state [after 30 years](#) of a frozen one.

The new cryptobiosis queen is tens of thousands of years older than that.

The ancient worm was found in Siberian permafrost, roughly 40 meters deep. When researchers dated some plant material found near the creature, they settled on an initial freezing period somewhere between 45,839 and 47,769 years ago. This beats another ancient roundworm, of the genus *Plectus*, which was also found frozen in Siberia and which was [dated to around 42,000 years ago](#) in 2018. Both nematodes are nearly twice as old as an ancient rotifer from Siberia, which was [recently revived after 24,000 years of cryptobiosis](#).



When researchers compared the genomes of *P. kolymaensis* to one of its living relatives, *Caenorhabditis elegans*, they found a lot of overlapping genes between the soil worms. Many of the shared genes are tied to mechanisms involved in surviving harsh environmental conditions. This is interesting, as *C. elegans* is usually found in temperate regions, hiding in rotting fruit or plants. The authors of the study [say](#) their findings "indicate that by adapting to survive cryptobiotic state for short time frames in environments like permafrost, some nematode species gained the potential for individual worms to remain in the state for geological timeframes". The team now wants to figure out what role these shared genes play in cryptobiosis, and whether there is an upper limit to how long nematodes can remain in this mysterious state.

"These findings have implications for our understanding of evolutionary processes, as generation times may be stretched from days to millennia, and longterm survival of individuals of species can lead to the refoundation of otherwise extinct lineages," the authors of the paper [write](#). There's even a chance that unlocking the secrets of long-term cryptobiosis could provide scientists with a better way to store cells and tissues over long periods of time.

●► The study was published in [PLOS Genetics](#).

EDITOR'S COMMENT: Could the worm be revived without human intervention? Or the "cold" pathogens in the previous article? One day we might dearly regret this scientific curiosity...

AI chatbots may help criminals create bioweapons soon, warns Anthropic CEO

By Zohaib Ahmed

Source: <https://indianexpress.com/article/technology/artificial-intelligence/ai-chatbots-bioweapon-warning-anthropic-ceo-8866807/>

July 29 – The generative AI landscape has been evolving rapidly since ChatGPT's debut in November last year. Despite the growing concerns from regulators and experts, many new chatbots and tools have emerged with enhanced capabilities and features. However, these chatbots may also pose a new threat to global security and stability.

Dario Amodei, the CEO of Anthropic, warned that AI systems could enable criminals to create bioweapons and other dangerous weapons in the next two to three years. Anthropic, a company founded by former OpenAI employees, recently shot into the limelight [with the release of its ChatGPT rival, Claude](#).

The startup has reportedly consulted with biosecurity experts to explore the potential of large language models for future weaponisation.

At a hearing on Thursday, Amodei testified before a US Senate technology subcommittee that regulation is needed desperately to tackle the use of AI chatbots for malicious purposes in fields such as cyber security, nuclear technology, chemistry, and biology.

"Whatever we do, it has to happen fast. And I think to focus people's minds on the biorisks, I would really target 2025, 2026, maybe even some chance of 2024. If we don't have things in place that are restraining what can be done with AI systems, we're going to have a really bad time," he testified at the hearing on Tuesday.

This isn't the first time an AI company has acknowledged the dangers of the product they're themselves building and called for regulation. For instance, Sam Altman, the head of OpenAI, the company behind ChatGPT, urged for international rules on generative AI during a visit to South Korea in June.

In his testimony to the senators, Amodei said that [Google](#) and textbooks only have partial information for creating harm, which needs a lot of expertise. But his company and collaborators have found that current AI systems can help fill in some of those gaps.

"The question we and our collaborators studied is whether current AI systems are capable of filling in some of the more difficult steps in these production processes. We found that today's AI systems can fill in some of these steps – but incompletely and unreliably. They are showing the first, nascent signs of risk."

He went on to warn that if appropriate guardrails aren't introduced, AI systems will be able to fill in those missing gaps completely.

"However, a straightforward extrapolation of today's systems to those we expect to see in two to three years suggests a substantial risk that AI systems will be able to fill in all the missing pieces, if appropriate guardrails and mitigations are not put in place. This could greatly widen the range of actors with the technical capability to conduct a large-scale biological attack."

Amodei's timeline for the creation of bioweapons using AI may be a bit exaggerated, but his concerns are not unfounded. Deeper information for creating [weapons of mass destruction](#) such as nuclear bombs usually rests in classified documents and with highly specialised experts but AI could make this information more widely available and accessible.



It's unclear exactly what methods the researchers used to elicit harmful information from AI chatbots. Chatbots like ChatGPT, Google Bard, and Bing chat usually avoid answering queries that involve harmful information, such as how to make a pipe bomb or napalm. However, researchers from Carnegie Mellon University in Pittsburgh and the Centre for AI Safety in San Francisco recently discovered that [open-source systems can be exploited to develop jailbreaks for popular and closed AI systems](#). By adding certain characters at the end of prompts, they could bypass safety rules and induce chatbots to produce harmful content, hate speech, or misleading information. This points toward guardrails not being fully foolproof.

Moreover, these dangers are amplified by the increasing power of open-source large language models. An example of AI systems being used for [malicious purposes is FraudGPT](#), a bot making a buzz in the dark web for its ability to create cracking tools, phishing emails, and other offences.

Light-activated antibacterial foil claimed to outperform HEPA filters

By Ben Coxworth

Source: <https://newatlas.com/health-wellbeing/lumaflo-antibacterial-foil/>



In lab tests, LumaFlo reportedly eradicated 99.997% of airborne Staphylococcus bacteria (pictured) in just 90 minutes

July 28 - Although HEPA filters and ultraviolet lighting systems are effective at neutralizing bacteria in hospitals, homes and other settings, they do have their drawbacks. A new light-activated material known as LumaFlo, however, is claimed to have them both beat.

One problem with HEPA filters is the fact that the filtration media eventually becomes saturated with trapped airborne pathogens, so it needs to be regularly replaced. Additionally, microbes may remain alive in that media for quite some time, plus the filters can impede airflow in a building's HVAC (heating, ventilation and air conditioning) system.

Ultraviolet light doesn't have these drawbacks, but direct exposure to it is harmful to humans. This means that it can only be utilized at times (or in places) when no people are present.

That's where [LumaFlo](#) is designed to come in.



ICI C²BRNE DIARY – August 2023

Created by an Israeli startup of the same name, it takes the form of a thin black photocatalytic foil made up of "a specially activated carbon" (currently carbon nanotubes, but that could change) and a metal oxide. When the material is exposed to any type of artificial or natural light, it reportedly decomposes any airborne organic molecules and organisms that touch it while flowing past.

The company suggests that it be applied like a decal to surfaces such as HVAC vents, fan blades, or even just walls that are in the path of a room's airflow and which are exposed to light. LumaFlo chairman Harry Yuklea tells us that based on current simulation models, the material should only need to be replaced once a year in relatively clean environments – that's about half as often as filter mats should be changed.

In tests performed at the FDA-approved Aerosol Research and Engineering Laboratory (ARE) in Kansas, LumaFlo foil is claimed to have eradicated 99.997% of airborne *Staphylococcus* bacteria within 90 minutes. The EPA's minimum requirement for HEPA filters is 99.97%. Additionally, because air just has to pass over the material instead of through it, LumaFlo is said to operate up to six times faster than filter-based systems.

"For normal residential environments we estimate that a LumaFlo DIY kit of 100 square centimeters (five strips of 2 cm x 10 cm) per room will guarantee the performance level proved by the reported ARE test," said Yuklea.

The planned price of such a kit, which should be commercially available by the first quarter of next year, is US\$49.

Freakishly Large Viruses With Arms And Tails Found in Massachusetts

By Felicity Nelson

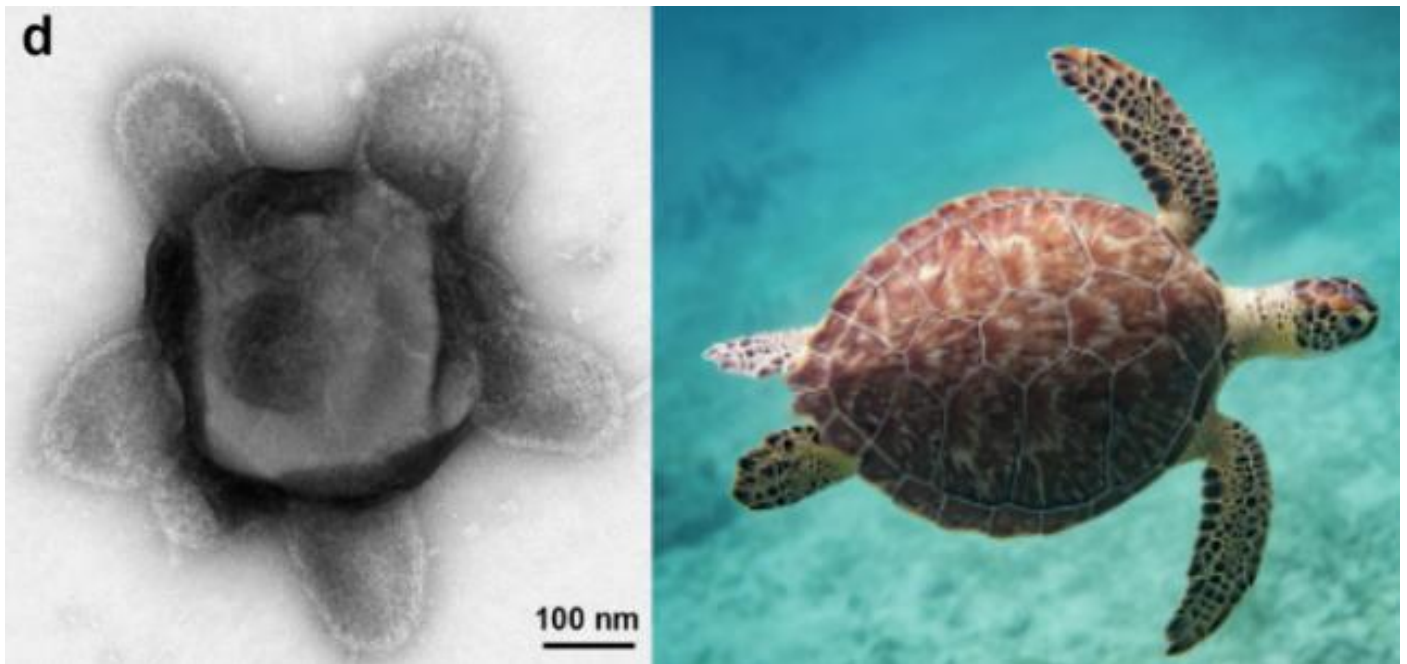
Source: <https://www.sciencealert.com/freakishly-large-viruses-with-arms-and-tails-found-in-massachusetts>



July 31 – Scientists have discovered an "[astounding diversity](#)" of giant [viruses](#) taking on "[previously unimaginable](#)" shapes and forms in just a few handfuls of forest soil.

These giant viruses have alien-looking appendages and internal structures that have never been seen before.

The soil sample was collected in 2019 from Harvard Forest, a short drive from Boston in the US.



Left: Giant 'turtle' [virus](#) (380-nm-wide) found in the Harvard Forest soil; Right: A turtle. ([Blanchard et al./bioRxiv](#), [Trey Thomas/Getty Images](#))

It was flown to the Max Planck Institute in Germany, where it was examined using transmission electron microscopy, a process that magnifies objects using a beam of electrons.

This revealed that the soil was packed with giant viruses up to 635 nanometers in width.

These giants are smaller than the [largest virus ever discovered](#) (which is [1,500 nm wide](#)) but much larger than the viruses that humans usually encounter ([COVID-19, for instance, is 50–140 nm](#)).



ICI C²BRNE DIARY – August 2023

The researchers [could be](#) "quite confident" that they were looking at viruses (rather than structures discarded from cells) because the shells, called capsids, have distinctive shapes, including the unmistakable icosahedral shape of a [20-sided](#) polygon.

"Transmission electron microscopy ... revealed an astounding diversity of virus-like particles," [write](#) the researchers.

"Amazingly, we found that a few hundred grams of forest soil contained a greater diversity... than... all hitherto isolated giant viruses combined."

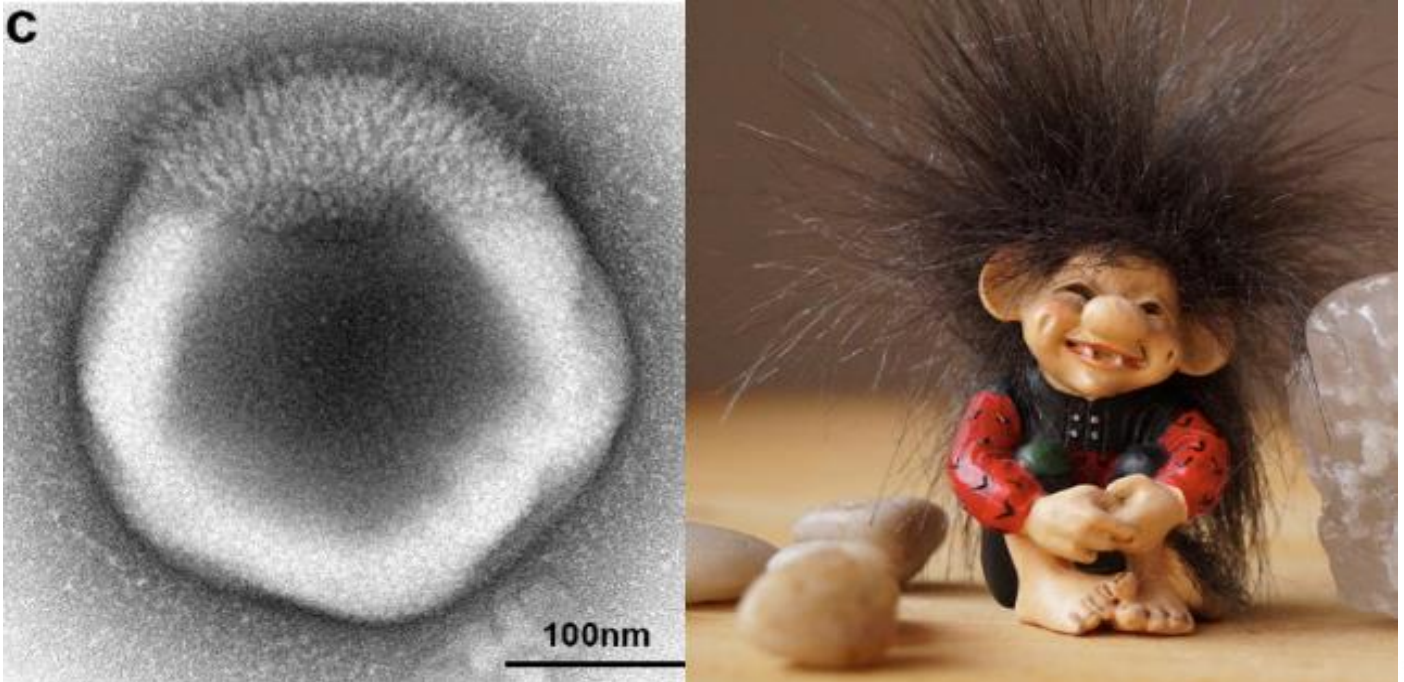
One of these exotic giant viruses had large limbs arranged in a symmetrical pattern, which the researchers described as a 'turtle' morphology.

Another virus has long tubes emerging on all sides, calling to mind the ancient Greek mythology figure of Medusa. Fittingly, the scientists named this structure '[Gorgon](#)', the creature that Medusa and her two sisters were called.



Left: Giant 'gorgon' virus (410-nm-wide) found in the Harvard Forest soil; Right: A statue of Medusa. ([Blanchard et al./bioRxiv](#), PaoloGaetano/Getty Images)

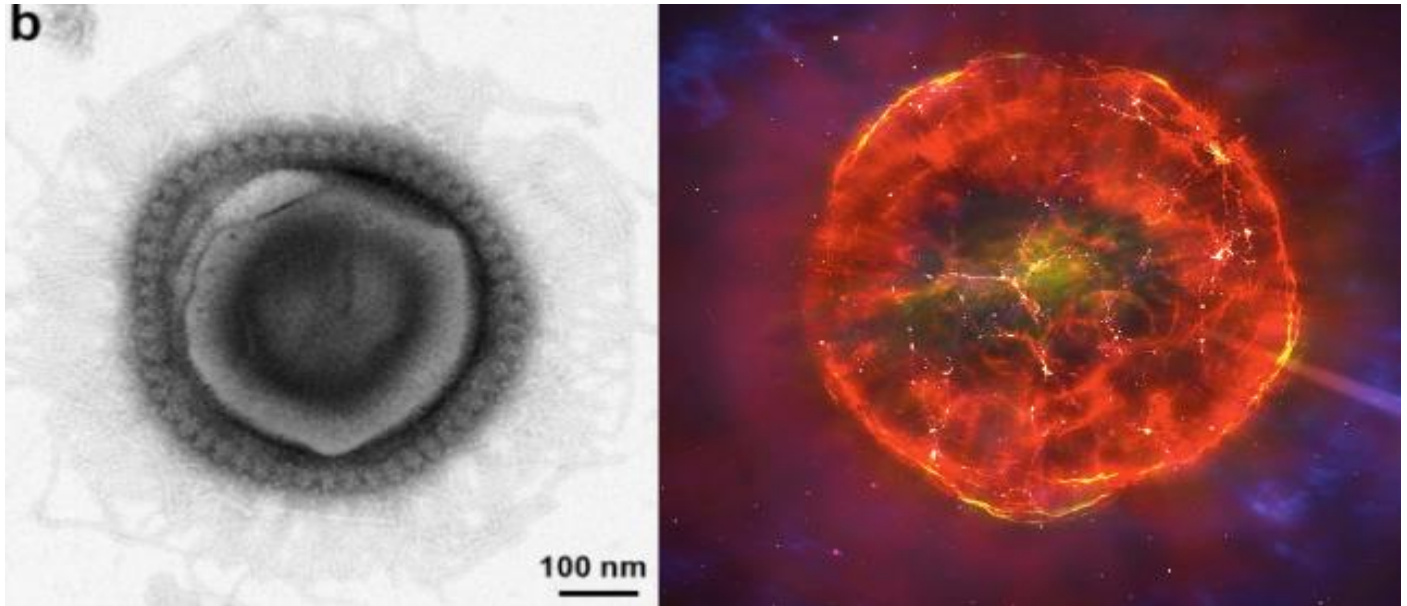
Another category called 'haircut' describes a family of large viruses with messy heads of different-length fibers (which looked like a troll doll).



Left: Giant 'haircut' virus found in the Harvard Forest soil; Right: A troll doll. ([Blanchard et al./biorxiv.org](#), ramonageorgescu/Getty Images)

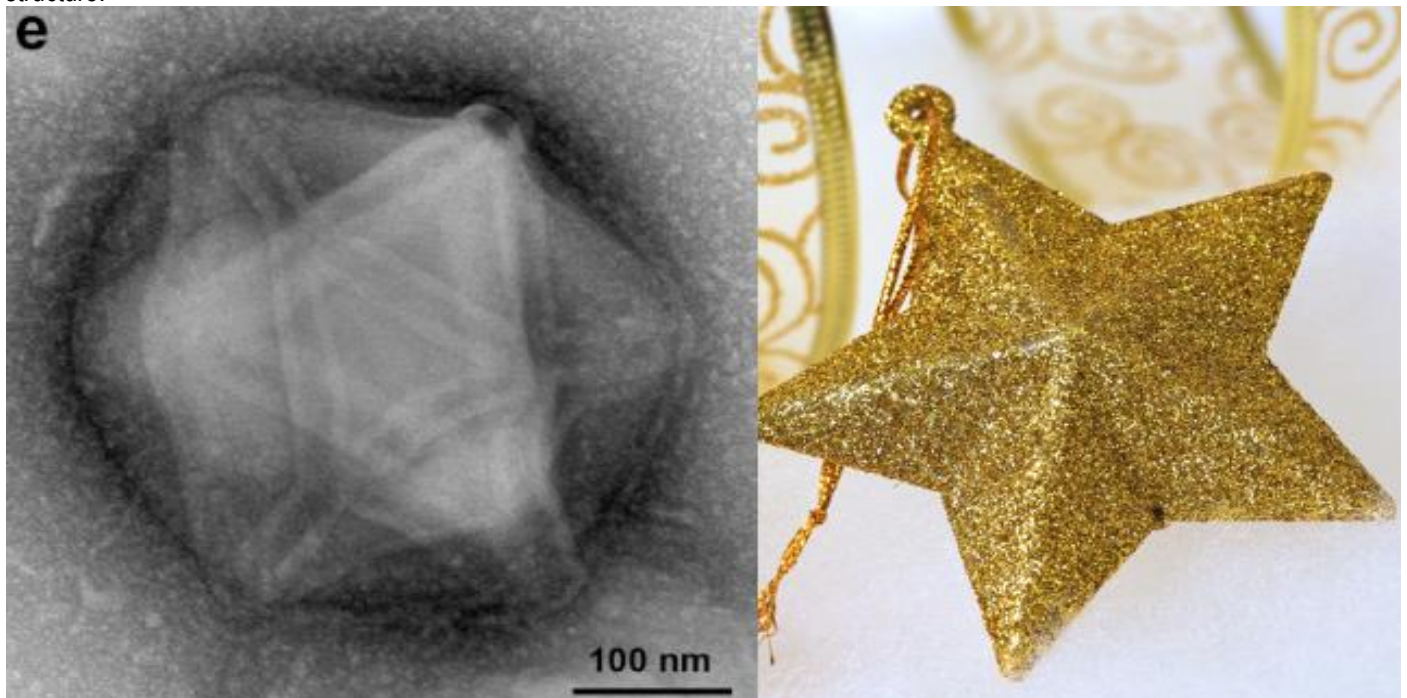


The 'supernova'-shaped giant viruses had a thick tangle of fibers close to the capsid shell and a thick layer of regularly arranged tendrils further out.



Left: Giant 'supernova' virus (490-nm-wide) found in the Harvard Forest soil; Right: An artist's depiction of a supernova. (Blanchard *et al./bioRxiv*, Mark Garlick/Science Photo Library/Getty Images)

The 'Christmas star' viruses had a double-layered shell resembling two interlocking triangles, and the 'falcon' viruses had a beak-like structure.



Left: Giant 'Christmas star' virus found in the Harvard Forest soil; Right: A Christmas tree star. (Blanchard *et al./bioRxiv*, 123ArtistImages/Getty Images)

"This fascinating window into the complex world of soil viruses leaves little doubt that the high genetic diversity of giant viruses is matched by diverse and previously unimaginable particle structures, whose



ICI C²BRNE DIARY – August 2023

origins and functions remain to be studied," [write](#) microbiologist [Matthias Fischer](#), electron microscopist [Ulrike Mersdorf](#), and biologist [Jeffrey Blanchard](#).

Giant viruses that [parasitize algae](#) have been studied for [decades](#). But the field really took off in 2003 when the first giant (400-nm-wide) [virus growing in amoebae](#) was found in a cooling tower in England. It was named 'mimivirus' as it mimicked the appearance of bacteria.

A [world record was set in 2010](#) with the discovery of the whopping 700-nm-wide [Megavirus chilensis](#) off the coast of Chile.

In 2013, a 1,000-nm [pandoravirus](#) was found in a pond in Melbourne. It was named after the mythical Pandora's Box.

The current record-holder is the [1,500-nm-wide Pithovirus sibericum](#), a giant virus buried in the Siberian permafrost for 30,000 years but discovered when the ice thawed in 2014.

●► This paper is available as a pre-print through [bioRxiv](#).

1-minute COVID breathalyzer could revolutionize testing at social events

Source: <https://newatlas.com/health-wellbeing/1-minute-covid-breathalyzer-could-revolutionize-testing-social-events/>



Aug 01 – Researchers have developed a novel device that detects the COVID-19 virus in one minute using just a couple of breaths of exhaled air. The device has the potential to revolutionize the testing process, especially in hospitals and schools and at large-scale social gatherings like concerts or sporting events.

Most people would be familiar with at-home COVID tests, so-called rapid antigen tests or RATs – the pain and sneeze-inducing irritation of swabbing the inside of your nostrils, swishing the mucus-coated swab around in a testing solution, squeezing it onto a test strip and waiting 15 or 20 minutes for a result that may or may not be accurate.

Now, researchers at Washington University in St. Louis have developed a hand-held device that tests for the COVID virus using as little as two exhaled breaths and providing an accurate result in around a minute.



It's an improvement on previously developed breath-analyzing COVID detectors that took [three](#) or [five](#) minutes to provide results.

"With this test, there are no nasal swabs and no waiting 15 minutes for results, as with home test," said Rajan Chakrabarty, co-corresponding author of the study. "A person simply blows into a tube in the device, and an electrochemical biosensor detects whether the virus is there. Results are available in about a minute."

The researchers repurposed a biosensor originally created to test for Alzheimer's-disease-related amyloid beta protein in mouse brains, swapping out the antibody that tests for amyloid beta for a nanobody derived from llama antibodies that recognizes a protein in the SARS-CoV-2 virus, which causes COVID-19.

The process is simple. A 3D-printed collection device is fitted with a straw, which the user blows into. Aerosols from the user's breath collect on the biosensor inside the device, which is plugged into a machine that determines whether the user is COVID-positive or not.

The researchers tested the device in a lab first, using three COVID variants: WA1, Delta, and Omicron. They found that its sensitivity was comparable to other electrochemical detection techniques for SARS-Cov-2. They then tested it on eight human patients, six who were COVID-positive and two COVID-negative. After having the patients blow into the device two, four, and eight times, the researchers found that the device was accurate, gave no false negatives and that two exhaled breaths were sufficient for virus detection.

With a production cost of less than US\$10 per test, the researchers say that their novel device is not only cost-effective, it's non-invasive and its use doesn't require trained personnel. Moreover, it can be adapted to detect a range of respiratory pathogens, including new COVID variants. Currently, the researchers are working on the simultaneous detection of multiple airborne viruses using different specific nanobodies.

This novel device has the potential to revolutionize testing, especially at large gatherings like concerts or sports games that have the risk of becoming 'superspreader' events. Instead of going through the lengthy process of at-home testing, this new breathalyzer could rapidly test for COVID upon entry with little to no inconvenience and a great deal of peace of mind.

"It's a bit like a breathalyzer test that an impaired driver might be given," said John Cirrito, another of the study's corresponding authors. "And, for example, if people are in line to enter a hospital, a sports arena or the White House Situation Room, 15-minute nasal swab tests aren't practical, and PCR tests take even longer. Plus, home tests are about 60% to 70% accurate, and they produce a lot of false negatives. This device will have diagnostic accuracy."

While initial results are promising, the researchers plan to validate them by conducting a longitudinal clinical study.

●► The study was published in the journal [ACS Sensors](#).

The Public Health Role During Mass-Fatality Incidents

By Raphael Barishansky and Audrey Mazurek

Source: <https://www.domesticpreparedness.com/articles/the-public-health-role-during-mass-fatality-incidents>

Many major disasters start without warning, continue for periods ranging from mere seconds to weeks or months, and leave behind a chaotic mass of useless rubble and ruined lives. The work of public health agencies necessarily starts well before the first tremor, continues through the entire response/recovery/resilience process, and ends – well, never.

The term "mass fatality incident" is defined as an incident in which more deaths occur than can be handled by local resources. However, determining what constitutes a mass fatality incident varies from one jurisdiction to another not only because communities differ in both size and resources but also because such incidents can be caused by natural hazards, human-related hazards, or "pro-active" human hazards.

Although different from other types of public health services, and even counter to how most people view public health (i.e., as a sector dedicated to ensuring the health and safety of the public), mass fatality management is actually one of the key responsibilities listed – under the Federal Emergency Management Agency's National Response Framework – as an Emergency Support Function (ESF). Mass fatality management comes under *ESF #8, Public Health and Medical Services*. In most if not quite all jurisdictions, the public health authority is specifically responsible for ESF #8.

The overall responsibilities for public health in a mass fatality incident vary considerably, though, by jurisdiction and state. However, public health still plays an important role during planning, response, and recovery efforts. Today, public health agencies have greater first-responder and overall preparedness roles than ever before. They also have more experience and are members of partnerships that are vital during major disasters – e.g., working with vulnerable populations,



collaborating with community partners and volunteer organizations – and are expanding pre-existing relationships with laboratories and with medical examiners/coroners (ME/Cs).

Rules, Regulations & Responsibilities – With Numerous Exceptions

It is important to remember, though, that public health's responsibilities during a mass fatality incident do not supersede those of the ME/Cs – or of such U.S. government agencies as the Federal Bureau of Investigation (FBI) and/or the National Transportation Safety Board (NTSB). However, jurisdictional and/or state authorities spell out the specific responsibilities of public health and other first responders vs. those of the ME/Cs. One example: In the State of Maryland, the Office of the Chief Medical Examiner (OCME) has jurisdiction over “any death which is the result of a casualty or accident, homicide, poisoning, suicide, rape, therapeutic misadventure, drowning, of suspicious or unusual nature, or of any apparently healthy individual while not under the care of a physician.” In all such cases, local public health departments provide support to OCME and law enforcement agencies – but have jurisdiction over and coordinating authority for all other types of mass fatality incidents that do *not* fall under OCME jurisdiction.

Under normal conditions, approximately 90 percent of the fatalities in Maryland, which result from natural diseases occurring under natural circumstances, are *not* OCME cases. However, approximately 90-95 percent of all of the mass fatality incidents in the state are under the jurisdiction of OCME – because they result from accidents, homicides, and/or other unusual or suspicious circumstances. For most jurisdictions, therefore, only a small percentage of mass fatality events fall outside the care of the ME/Cs (which have and must adhere to their own mass fatality plans). Nonetheless, public health and its partners must still develop detailed plans to ensure that: (a) there is a common understanding of their respective roles, responsibilities, and available resources; and (b) essential functions can and will continue during an incident.

After determining the general parameters of responsibilities – as specified by a state or other jurisdiction's laws – during a mass fatality incident, the next step is to determine what agencies and individuals should be “at the table” at the beginning of the planning process. In that context, what might be and frequently is a very long list obviously should include at least the following: law enforcement agencies and fire departments; emergency medical services (EMS); homeland security/emergency management; hospitals and other healthcare facilities (including mental health providers; ME/Cs; volunteer organizations – the American Red Cross, for example); and representatives of the death care industry (funeral homes, cemeteries, and crematories). A number of state and regional agencies likely to be involved in various ways also should be included.

The Creative Process – Pitfalls and Problem Areas

The mass fatality management plan developed by the aforementioned stakeholders should not supersede but, rather, be complementary to the ME/C mass fatality plan, other responder plans, and/or state and regional plans. If and when possible, the planning process should review, and use as a template, existing plans and best practices/resources from other jurisdictions – e.g., “*Managing Mass Fatalities: A Toolkit for Planning*,” developed by the Santa Clara County [California] Public Health Department. Following are brief descriptions of some but no means all of the principal topics, issues, and potential problem areas that should be included in a truly comprehensive and operationally effective plan:

Introduction: The first component of the plan is introductory in nature and states the rationale (purpose and objectives) behind writing the plan, as well as its scope and a list of emergencies covered – in this example, these are almost always health-specific and would probably include, but not be limited to, terrorist acts or threats, infectious-disease emergencies, the dangers caused by contaminated drugs and/or medical devices, food or waterborne disease outbreaks, and/or contamination of a public water supply. This section also should clearly state which incidents fall under the umbrella of law-enforcement agencies, and which do not.

Authorities and Definitions: The next section of the plan should list the legal authorities under which the plan is being written – e.g., State codes, local Emergency Operations Plans – as well as the relevant definitions. The latter should be as comprehensive as possible because, for legal purposes, the agencies participating may well have to rely on those definitions at a later date.

Situation and Assumptions: This section discusses the jurisdiction's situation and assumptions, including numerous operational realities: the agencies (and/or officials) that have jurisdiction over decedents; various obstacles that have the potential to challenge a response to mass fatality incidents; the roles played by various federal agencies (e.g., NTSB, FBI); and the responsibilities of Disaster Mortuary Operational Response Teams (DMORTs).

Command and Control: This section provides detailed instructions on how an incident or event should be managed (as spelled out in Incident Command System/Unified Command guidelines) as well as how public health and other response agencies should support the ME/C, federal agencies, and the region, etc. This section might also include a detailed breakdown of the roles and responsibilities of health departments and other response agencies.

Concept of Operations: This section, often the longest and most detailed section of the mass fatality management plan, spells out the operational and procedural steps that must be taken to: (a) activate the



plan; (b) communicate with partners, media, and the community at large; and (c) carry out the roles/responsibilities involved in each phase of mass fatality management. (Public health is usually *not* the lead agency designated to carry out the functions/activities under each phase, but it may be the lead coordinating agency and/or play a major supporting role. In addition, it should be remembered that, depending on the responsibilities assigned by local or state authorities, local agencies may be operating under the direction of ME/Cs.)

A Daunting and Detailed List of Duties

After the legal jurisdictional framework and chain of command have been spelled out, the planning process should shift to the specific tasks and responsibilities likely to be faced immediately following, during, and concluding a specific mass fatality incident. Following are a few specific examples of the mass fatality management phases and some probable public health responsibilities in each such phase.

- **Human Remains Recovery/Retrieval:** Public health supports the lead agency (e.g., Fire/Rescue, EMS, and/or law enforcement) in acquiring supplies and resources, providing subject-matter expertise related to decontamination, and maintaining awareness of operations to anticipate challenges.
- **Transportation:** Public health may coordinate transportation, but the lead agencies are usually the local transportation/public works administration and/or death care industry. Transportation needs should be requested through the Emergency Operations Center (EOC), but public health may offer guidelines for suitable transportation assets and the movement of remains, and maintain awareness of the community transportation needs of the death care industry.
- **Storage:** Public health should work with applicable community partners such as hospitals and emergency management agencies to identify appropriate locations for both the short- and long-term storage of decedent remains.
- **Identification and Tracking:** Although identification of decedents is usually led by law enforcement and the ME/C – with law enforcement serving as the lead in notifying the next of kin – all of the response agencies involved, including public health, are responsible for ensuring the careful and respectful tracking of decedents, body parts, and personal effects.
- **Interment:** If remains cannot be stored in a refrigerated facility while awaiting final disposition, temporary interment (i.e., burial) may be considered. Public health assists in selecting appropriate temporary interment sites, ensuring that the appropriate resources are available, and – at the conclusion of the mass fatality incident – assisting with the process of re-interment.
- **Disposition:** A key goal during a mass fatality incident is to ensure that each body reaches the “final disposition” stage in accordance with his or her religious and cultural practices as well as the wishes of the victim’s family. In support of this goal, public health assists the death care industry in developing a viable continuity of operations plan (COOP), providing situational awareness and appropriate public messaging capability, and ensuring that the resources needed are available.
- **Death Certificates:** Although physicians and ME/Cs are responsible for filling out and signing death certificates, public health plays a key role in communities in which the health department processes death certificates. (The health department’s COOP may have to be activated, though, to ensure that the resources needed are readily available to help in the processing of death certificates.)
- **Law Enforcement/Security:** Public health keeps law enforcement informed of security needs, a particularly important responsibility at all mass fatality incident operational areas – storage sites as well as incident sites.
- **Supply and Volunteer Management:** Public health works with community partners, volunteer groups – the Medical Reserve Corps (MRC), for example, and Community Emergency Response Teams (CERTs) – and faith-based organizations to ensure that volunteers are appropriately trained, possess the equipment and other material resources needed, and fully understand their individual and collective roles and responsibilities (and limitations) during the event.
- **Family Assistance:** The family assistance center (FAC) is a particularly important component of the jurisdictional infrastructure both during the planning process and during the event. Depending on the type of incident, the FAC, which can be either a physical or “virtual” location (a designated hotline, for example), usually serves as a primary resource for families that want to exchange information about missing and deceased relatives. The FAC also assists in the re-unification of families with decedents, and provides many of the resources and services needed not only by survivors but also their families (e.g., disaster behavioral health services, final disposition options, grief counseling).
- **Demobilization/Recovery:** Depending on the type of incident, public health may have to provide immediate and/or ongoing support to mass fatality management to work toward a respectful resolution and final resting place for decedent remains. In addition, public health probably will have to manage certain environmental-surety issues such as decontamination, determining a safe return to facilities, and both water and soil sampling.



Laminated Checklists and Other Odds & Ends

Among several essential appendices to the completed plan would be such helpful data as the following: “Key Contacts” information (particularly valuable for agencies and organizations in the death care industry); a list of decedent storage and handling sites; local public and media communications outlets; religious and/or cultural organizations in the local community; a death management process checklist; communications links to ME/Cs; and the steps needed to access state, local, and/or regional mass fatality management plans available to the public.

It should be kept in mind at all times, moreover, that one of the most challenging aspects of the planning process is not writing the plan per se but, rather, ensuring that it is operationally possible, useful, and easy to follow during an actual emergency. Because a mass fatality plan is more technical in nature – and differs in several important ways from most other public health plans – it is particularly important that all of the agencies and individuals involved clearly understand not only their own roles but also the rationale used for the development and organization of the plan.

In addition to training and exercises, each response agency also should develop checklists or tip sheets of the plan – i.e., a relatively short (no more than 4-5 pages) document summarizing the key points and definitions used in the plan. Also included should be a checklist of the planning, response, and recovery responsibilities of each participating agency. These checklists can and should be laminated and should be carried by the units – police, fire, EMS, and health agencies, usually – most likely to be first on the scene for their respective agencies.

Incidents that produce large numbers of fatalities are more common today than ever before, and for that reason alone there is a compelling need to prepare and plan much more effectively than ever before – and earlier – for emergency responses of all types. Weather events such as the deadly tornadoes that devastated several U.S. communities earlier this year, Hurricane Katrina, the Japan tsunami/earthquake – compounded by the 9/11 attacks and other terrorist incidents, as well as aviation accidents and other “manmade” disasters – serve as stern but absolutely essential reminders of how traditional responses have been replaced in recent years by the compelling need for a much broader understanding of the comprehensive planning needed to deal effectively with complex mass fatality events.

Raphael M. Barishansky, DrPH(c), is a consultant providing his unique perspective and multi-faceted public health and emergency medical services (EMS) expertise to various organizations. His most recent position was as the Deputy Secretary for Health Preparedness and Community Protection at the Pennsylvania Department of Health, a role he recently left after several years. He is also currently a doctoral candidate at the Fairbanks School of Public Health at Indiana University.

Audrey Mazurek, MS, has worked at all levels of government for nearly 20 years in public health and healthcare preparedness, emergency management, and homeland security. She was a program manager with the National Association of County and City Health Officials (NACCHO) Project Public Health Ready program. She supported the U.S. Department of Homeland Security in the development of an accreditation and certification program for private sector preparedness. She also served as a public health emergency preparedness planner for two local public health departments in Maryland, where she developed over 30 preparedness and response plans, trainings, and exercises. She is currently a director of public health preparedness with ICF, primarily supporting the U.S. Department of Health and Human Services, Assistant Secretary for Preparedness and Response's (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE) program as the ICF program director.

Health security intelligence capabilities post COVID-19: resisting the passive “new normal” within the Five Eyes

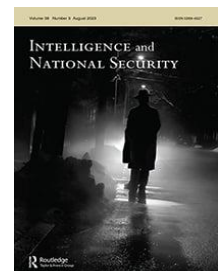
By Patrick F Walsh, James Ramsay and Ausma Bernot

Intelligence and National Security | Published online: 02 Aug 2023

Source: <https://www.tandfonline.com/doi/full/10.1080/02684527.2023.2231196>

Abstract

This paper spotlights lessons for health security intelligence across the ‘Five Eyes’ countries. The COVID-19 pandemic and recent worldwide patterns related to climate change have highlighted the crucial supporting role intelligence analysis may play in comprehending, planning for, and responding to such global health threats. In addition to the human lives lost, the COVID-19 pandemic has revealed serious national security concerns, notably for economic, societal, and in some cases, political stability. In response, a greater emphasis must be placed on intelligence. The paper has three goals. First, it outlines the major thematic areas where key ‘Five Eyes’ intelligence communities’ (ICs) skills were tested in supporting the management of COVID-19: 1) the origins of SARS-CoV-2, 2)

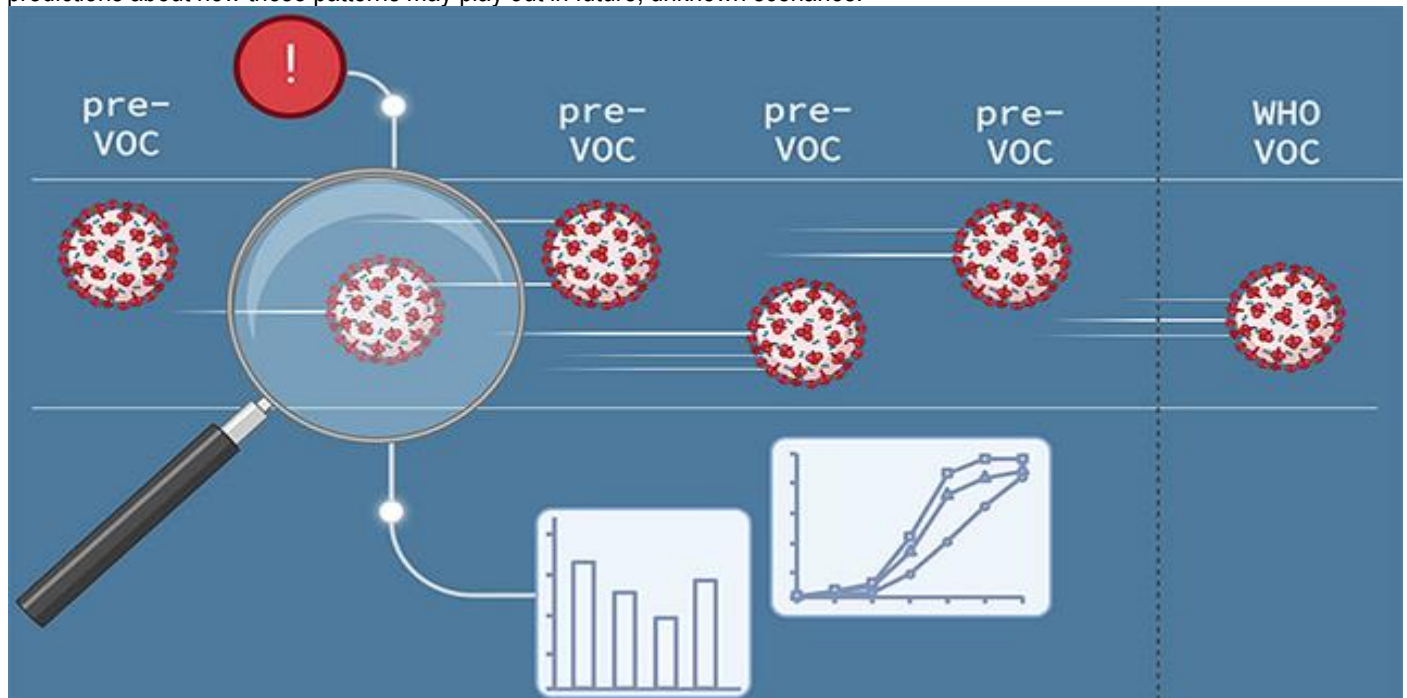


disinformation campaigns, and 3) early warning systems. The article then explores how such factors have impacted ICs' ability to provide decision-making support during COVID-19. Finally, the article discusses how 'Five Eyes' ICs may strengthen capacity in the three crucial areas. The 'Five Eyes' ICs must act swiftly but methodically to assess the security-based analytic lessons learned during the COVID-19 pandemic to maximize preparation for the next inevitable pandemic, whether caused by a natural disaster, climate change, or state or non-state threat actors.

AI May Be Able to Warn Us Before The Next Pandemic Strikes

Source: <https://www.sciencealert.com/ai-may-be-able-to-warn-us-before-the-next-pandemic-strikes>

Aug 05 – The [global COVID-19 pandemic](#) has shown us just how devastating these outbreaks can be – and it could have been much worse. Now, scientists have developed an AI application that promises to warn us about dangerous variants in future pandemics. It's called the early warning anomaly detection (EWAD) system, and when tested against actual data from the spread of [SARS-CoV-2](#), it was accurate in predicting which new variants of concern (VOCs) would emerge as the [virus](#) mutated. Scientists from Scripps Research and Northwestern University in the US used a [machine learning](#) method to produce EWAD. In machine learning, vast amounts of training data are analyzed by computers to spot patterns, develop algorithms, and then make predictions about how those patterns may play out in future, unknown scenarios.



The AI was able to spot variants of concern in advance. (Scripps Research/BioRender.com)

In this case, the AI was fed information about the genetic sequences of [SARS-CoV-2 variants](#) as infections spread, how frequent those variants were, and the reported global mortality rate from [COVID-19](#). The software could then spot genetic shifts as the virus adapted, usually shown in increasing infection rates and falling mortality rates.

"We could see key gene variants appearing and becoming more prevalent, as the mortality rate also changed, and all this was happening weeks before the VOCs containing these variants were officially designated by the WHO," [says](#) William Balch, a microbiologist at Scripps Research.

The specific technique used here by the team is called [Gaussian process-based spatial covariance](#), which essentially crunches the numbers on a set of existing data to predict new data – using not just the averages of the data points but also the relationships between them.

By testing their model on something that's already happened and finding close matches between the real and the predicted data, the scientists could prove EWAD's effectiveness at predicting how measures such as vaccines and [mask-wearing](#) could cause a virus to continue evolving.



"One of the big lessons of this work is that it is important to take into account not just a few prominent variants, but also the tens of thousands of other undesignated variants, which we call the 'variant dark matter,'" [says](#) Balch.

The researchers say their [AI algorithms](#) were able to spot "rules" of virus evolution that would otherwise have gone undetected, and that could prove vital in combating future pandemics as they emerge.

Not only that, but the system developed here could also enable scientists to understand more about the very basics of virus biology. That could then be used to improve treatments and other public health measures.

"This system and its underlying technical methods have many possible future applications," [says](#) mathematician Ben Calverley from Scripps Research.

●► The research has been published in [Cell Patterns](#).

The Potential Efficacy of an Aviation Bioterrorist Attack and Its Psychosocial Consequences

By Olaf Truszczyński

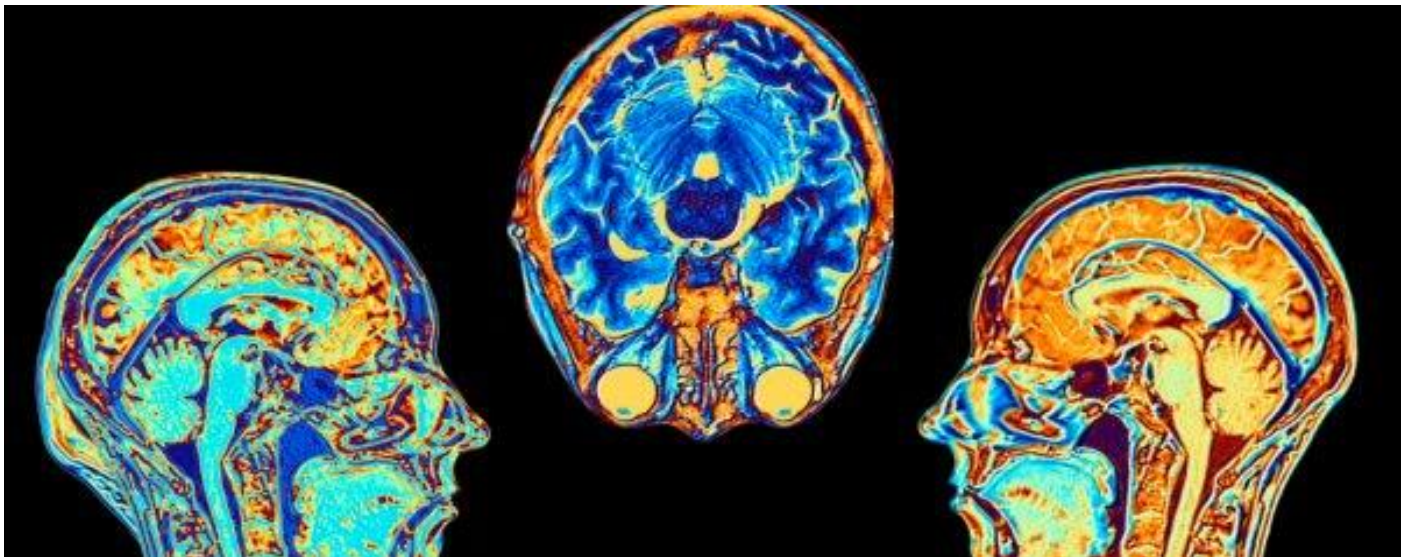
Pol J Aviat Med Bioeng Psychol 2017; 23(2): 19-27

Source: https://www.academia.edu/71445750/The_Potential_Efficacy_of_an_Aviation_Bioterrorist_Attack_and_Its_Psychosocial_Consequences?email_work_card=view-paper

The work concerns the analysis of the possibility of a bioterrorist attack using infected material using modern air transport carriers to infect the human population. It is possible to use passenger and transport planes, but the use of drones and minidrones seems the most dangerous. A bioterrorist attack is very specific and differs from other forms of terrorism, first of all in the possibility of self-replication of the pathogen, as well as the ability to "sleep" its operation even for many years and completely unexpectedly activate it. In such conditions, not only fast medical neutralizing action becomes crucial, but also calming psychosocial reactions and reasonable cooperation of the authorities and the media.

Brain Function Can Still Be Affected by COVID Years After Infection, Study Finds

Source: <https://www.sciencealert.com/brain-function-can-still-be-affected-by-covid-years-after-infection-study-finds>



MRI scans of healthy brains. (Alfred Pasiaka/Science Photo Library/Getty Images)

Aug 05 – [Long COVID](#) can live up to its name. A new study shows that certain symptoms of the condition, such as brain fog, can still be experienced in people with long COVID two years after the original infection. A team from King's College London and Imperial College London in the UK looked at the cognitive test performance of



3,335 people infected by [SARS-CoV-2](#) at some point during the [pandemic](#). The tests measured different capabilities, including memory, attention, reasoning, processing speed, and [motor control](#).

Those who struggled most with the brain tests also reported [COVID-19 symptoms](#) lasting for 12 weeks or more, the researchers found. The impact on cognitive ability was comparable to a 10-year increase in age, on average.

There were two rounds of tests, nine months apart, with the second round carried out nearly two years after the SARS-CoV-2 infection. The data showed no improvement in scores between the two rounds for those experiencing [long COVID](#).

"Our findings suggest that, for people who were living with long-term symptoms after having [COVID-19](#), the effects of the [coronavirus](#) on mental processes such as the ability to recall words and shapes are still detectable at an average of almost two years since their initial infection," [says](#) data scientist Nathan Cheetham from King's College London

There is some more positive news here as well, though. Participants who reported feeling fully recovered from the [virus](#) were posting test scores comparable to those who had never had COVID-19. That shows recovery is possible, even for those experiencing [several months of symptoms](#).

This study adds to the growing body of research on long COVID. Scientists have found that the condition can [cause noticeable changes](#) to the body's immune system and has [an effect on the brain](#) similar to chronic fatigue.

According to the [World Health Organization](#), the number of people living with long COVID is in the tens of millions. It can have a detrimental effect on just about every aspect of daily life and work, and yet there's no cure.

The team behind this latest study wants to see more research looking at the mechanisms behind long COVID, and more support for those who find that [their symptoms persist](#) for months or even years after getting the virus.

"The fact remains that two years on from their first infection, some people don't feel fully recovered, and their lives continue to be impacted by the long-term effects of the coronavirus," [says](#) Claire Steves, a clinical aging and health researcher at King's College London. "We need more work to understand why this is the case and what can be done to help."

●► The research has been published in [eClinicalMedicine](#).

CDC says COVID variant EG.5 is now dominant, including strain some call "Eris"

Source: <https://www.cbsnews.com/news/covid-variant-eg-5-now-eris/>

Aug 07 – The EG.5 variant now makes up the largest proportion of new COVID-19 infections nationwide, the Centers for Disease Control and Prevention estimated, as multiple parts of the country have been reporting their first [upticks of the virus](#) in months.

Overall, as of Friday, 17.3% of COVID-19 cases nationwide were [projected](#) to be caused by EG.5, more than any other group, up from 7.5% through the first week of July.

The next most common variants after EG.5 are now XBB.1.16 at 15.6%, XBB.2.23 at 11.2% and XBB.1.5 at 10.3%. Some other new XBB spinoffs are now being ungrouped from their parents by the CDC, including FL.1.5.1, which now accounts for 8.6% of new cases.

EG.5 includes a strain with a subgroup of variants designated as EG.5.1, which a biology professor, T. Ryan Gregory, [nicknamed](#) "Eris" — an unofficial name that began trending on social media.

Experts say EG.5 is one of the fastest growing lineages [worldwide](#), thanks to what might be a ["slightly beneficial mutation"](#) that is helping it outcompete some of its siblings.

It is one of several closely-related Omicron subvariants that have been competing for dominance in recent months. All of these variants are descendants of the XBB strain, which this fall's COVID-19 vaccines will be [redesigned](#) to guard against.

Officials have said that symptoms and severity from these strains have been largely similar, though they acknowledge that discerning changes in the virus is becoming increasingly difficult as surveillance of the virus has slowed.

"While the emergency of COVID has been lifted and we're no longer in a crisis phase, the threat of COVID is not gone. So, keeping up with surveillance and sequencing remains absolutely critical," Dr. Maria Van Kerkhove, the World Health Organization's technical lead for COVID-19, [said](#) on July 26.

Earlier this year, the CDC disclosed it would slow its variant estimates from weekly to biweekly, in hopes of being able to gather larger sample sizes to produce those projections.

On Friday, the agency said for the first time it was unable to publish its "Nowcast" projections for where EG.5 and other variants are highest in every region.

Only three parts of the country — regions anchored around [California](#), [Georgia](#) and [New York](#) — had enough sequences to produce the updated estimates.



"Because Nowcast is modeled data, we need a certain number of sequences to accurately predict proportions in the present," CDC spokesperson Kathleen Conley said in a statement.

Less than 2,000 sequences from U.S. cases have been published to virus databases in some recent weeks, according to a CDC [tally](#), down from tens of thousands per week earlier during the pandemic.

"For some regions, we have limited numbers of sequences available, and therefore are not displaying nowcast estimates in those regions, though those regions are still being used in the aggregated national nowcast," said Conley.

ChatGPT could make bioterrorism horrifyingly easy

By Jonas Sandbrink

Source: <https://www.vox.com/future-perfect/23820331/chatgpt-bioterrorism-bioweapons-artificial-intelligence-openai-terrorism>



Riot police don gas masks and anti-chemical gloves on March 24, 1995, before raiding a commune of the religious cult the "Aum Supreme Truth" in Kamikuishiki village west of Tokyo. *Yoshikazu Tsuno/AFP via Getty Images*

[Jonas Sandbrink](#) Jonas Sandbrink is a biosecurity researcher at the University of Oxford and a biological security adviser at the UK Cabinet Office.

Aug 07 – In the summer of 1990, three trucks [sprayed](#) a yellow liquid at different sites in and around Tokyo, including two US Naval bases, Narita Airport, and the imperial palace. The attackers belonged to a group called Aum Shinrikyo, a Japanese cult that aimed to cause the collapse of civilization, making space for the rise of a new society ordered according to their religious ideals. Five years later, Aum would gain notoriety by [carrying out](#) sarin gas attacks on the Tokyo subway, killing 13 and injuring thousands.

Aum intended for the yellow liquid dispersed in the summer of 1990 to contain botulinum toxin, one of the [most poisonous biological substances](#) known to human beings. However, no one was killed in the attacks that summer. One [possible factor](#) in their failure is that Aum lacked a crucial bit of knowledge: the difference between disseminating the bacterium *Clostridium botulinum* and disseminating the highly deadly botulinum toxin it produces. It is



unclear whether Aum even managed to acquire a toxin-producing form of the bacterium, and there are also other causes for why Aum's attack failed.

But if it had access to contemporary artificial intelligence tools, Aum Shinrikyo, or a similarly malign group, might not have made this and other mistakes. [ChatGPT](#) is very good at answering questions and providing knowledge, including on the production of botulinum toxin. If Aum had had access to ChatGPT, would the attacks of the summer of 1990 be remembered as possibly the worst bioterrorism event in history?

Advances in artificial intelligence have tremendous potential to have positive impacts on science and health. Tools like ChatGPT are revolutionizing how society works and learns, and artificial intelligence applied to biology has led to solving the decade-old [protein folding problem](#) and is transforming [drug discovery](#). However, as artificial intelligence raises the ceiling of biological engineering and helps distribute these powers to a tremendous number of individuals, there is a serious risk that it will enable ill-intentioned actors like Aum Shinrikyo, to potentially devastating effect. As I have discussed in a recent [preprint](#) paper, large language models (LLMs) like ChatGPT, as well as novel AI-powered biological design tools, may significantly increase the risks from biological weapons and bioterrorism.

How AI language models are a threat multiplier for bioweapons

Large language models — which are very good at answering questions and teaching about dual-use knowledge — may in particular increase the accessibility of biological weapons. In a recent [exercise](#) at MIT, it took just one hour for ChatGPT to instruct non-scientist students about four potential pandemic pathogens, including options for how they could be acquired by anyone lacking the skills to create them in the lab, and how to avoid detection by obtaining genetic material from providers who do not screen orders.

At the same time, the story of Aum Shinrikyo's lack of knowledge about the difference between *Clostridium botulinum* and botulinum toxin is not an isolated example. Past biological weapons programs have frequently been bottlenecked by not having the right staff, with the required knowledge and expertise, to create an effective bioweapon. Al-Qaeda's exploration of bioterrorism was led by Rauf Ahmed, who had originally studied microbes related to food production, and thus tried to [quickly learn](#) about anthrax and other pathogens. Over the course of 2001, Rauf used his scientific credentials to [make headway](#) toward acquiring anthrax. It is not publicly known how far he got; [he was arrested](#) that December.

Despite having access to the relevant equipment, Saddam Hussein's Iraq [never turned](#) its anthrax weapon from a less potent liquid form into a more dangerous powder form, which can be stored and released at much higher and more predictable concentration. That's likely because its scientists lacked the knowledge of the relevant process for drying and milling anthrax. As chatbots become more sophisticated, however, they may inadvertently help individuals with malicious intent to upskill on topics that empower them to do harm.

But how much can you learn from an AI-powered lab assistant alone? After all, to make a pathogen or a bioweapon, you don't just need instructional knowledge of the sort that can be dished out by an LLM, you need hands-on, tacit knowledge. [Tacit knowledge](#) describes all knowledge that cannot be verbalized and can only be acquired through direct experience. Think of how to ride a bike, or for that matter, how to [perform molecular biology](#) procedures, which might require knowing how to hold a pipette, shake a flask, or treat your cells. It is difficult to define the extent of this tacit knowledge barrier and how much impact LLMs like ChatGPT may have on lowering it. However, one fact seems clear: If chatbots and AI-powered lab assistants make the creation and modification of biological agents seem more accessible, then it is likely that more individuals will try their hand. And the more who try, the more who will eventually succeed.

Additionally, ChatGPT is just the beginning of language models and related forms of artificial intelligence. Already now, language models [are revolutionizing](#) the way scientists can instruct lab robots on what work to perform. Soon, artificial intelligence systems will be able to perform ideation and design of experimental strategies. Thus, artificial intelligence will enable and accelerate the increasing automation of science, reducing the number of scientists required to advance large-scale projects. This will make it easier to develop biological weapons covertly.

Biological design tools could simplify bioweapons

While large language models may eventually push the ceiling of biological design capabilities, more specialized AI tools are already doing this now. Such biological design tools (BDTs) include protein folding models like [AlphaFold2](#) and protein design tools like [RFdiffusion](#). These artificial intelligence tools are usually trained on biological data, such as genetic sequences. They are developed by many different companies and academics to help with important biological design challenges, such as developing [therapeutic antibodies](#). As biological design tools become more powerful, they will enable many beneficial advances like the creation of new medications based on novel proteins or designer viruses.



But such powerful design capabilities may also exacerbate biological risks. At the extreme, biological design tools could allow the design of biological agents with unprecedented properties. It has been hypothesized that natural pathogens feature a trade-off between how transmissible and how deadly they are; designed pathogens might not feature such evolutionary constraints. A group like Aum Shinrikyo could potentially create a pandemic virus much worse than anything nature could produce and thus, biological design tools could turn pandemics from the catastrophic risks they are now into true existential threats. Biological design tools could also enable the creation of biological agents targeted at specific geographies or populations.

In the short term, new design capabilities may challenge existing measures to control access to dangerous toxins and pathogens. Existing security measures tend to focus on proscribed lists of dangerous organisms or screening for known threatening genetic sequences. But design tools may simply generate other agents with similar dangerous properties that such measures wouldn't catch. The good news is that — at least initially — new cutting-edge possibilities enabled by biological design tools will likely remain only accessible to a manageable number of existing experts who will use these facilities for legitimate and beneficial purposes. However, this access barrier will fall as biological design tools become so proficient that their outputs require little additional laboratory testing; in particular, as AI language models learn to interface effectively with the tools. Language models are already being [linked up](#) to specialized science tools to help with specific tasks and then automatically apply the right tool for the task at hand. Thus, the heights of biological design could quickly become accessible to a very large number of individuals, including ill-intentioned actors.

Why we need mandatory gene synthesis rules

What can be done to mitigate risks emerging from the intersection of AI and biology? There are two important angles: strengthening general biosecurity measures and advancing risk mitigation approaches specific to new artificial intelligence systems.

In the face of increasingly powerful and accessible biological design capabilities, one crucial biosecurity measure is universal gene synthesis screening. The production of the genetic building blocks for a protein or organism is the crucial step in turning digital designs into physical agents. A range of companies specializes in producing such DNA or RNA building blocks. Since 2010, the US government [has recommended](#) that such gene synthesis companies screen orders and customers to ensure only legitimate researchers are accessing genetic material for controlled agents. Many cutting-edge gene synthesis companies perform such screening voluntarily and have formed the [International Gene Synthesis Consortium](#) to coordinate these activities. However, a significant number of gene synthesis providers still do not screen. Indeed, as the MIT exercise demonstrates, ChatGPT is very adept at pointing out this fact and giving instructions on how to exploit such weaknesses in supply chain security.

What is needed is a mandatory baseline for screening synthetic DNA products. Requiring such baseline screening does not go against the interests of companies: Industry leaders across the US and UK have been screening orders voluntarily and [are actively calling](#) for a regulatory baseline to prevent competitors from skimping on safety. Measures to make gene synthesis screening mandatory should capture increasingly common benchtop gene synthesis devices and need to be future-proof to include screening for functional equivalents of concerning agents. Similar customer screening baselines are also needed for other crucial service providers at the boundary of the digital-to-physical, such as contract research organizations providing services to synthesize organisms.

Advancing governance of artificial intelligence

In addition to general biosecurity measures, we also need artificial intelligence-specific interventions. The first focus should be mitigating risks from large language models because not only are these models likely already lowering barriers to biological misuse, but also because their capabilities may increase quickly and unpredictably. One crucial challenge that applies across the whole range of risks posed by large language models is that new and dangerous capabilities may only become clear after the release of the model.

A particularly crucial role in mitigating risks from LLMs may be played by [pre-release evaluations](#) of model capabilities. Such pre-evaluations are necessary to ensure that new models do not contain dangerous capabilities on public release — and if conducted by a third party, they could ensure that companies have taken appropriate steps during training and fine-tuning to reduce the chance that these models could enable biological misuse. Releasing models through [structured access](#) methods, such as the web ChatGPT interface, can ensure that safeguards can be continuously updated. In contrast, [open-sourcing a powerful LLM](#) has significant risks because fine-tuning and safeguards may be easily removed, and if new dangerous capabilities are discovered, it would be impossible to retract a model or update its safeguards.

Generally, the potential impact of artificial intelligence tools on the risk of biological misuse raises a profound question: Who should be able to access dual-use scientific capabilities? For policymakers trying to answer this question, it will be vital to consider diverse voices from across different disciplines,



demographics, and geographies. This will require difficult trade-offs between the openness of scientific areas relating to pathogens, law enforcement and monitoring of data streams for illicit activities, and increasing risk of misuse.

One sensible position might be that language models like ChatGPT do not need to provide anyone with detailed step-by-step instructions to create a dangerous strain of pandemic flu. Therefore, it might on balance be preferable if public versions of such models do not give detailed answers to questions on this and other dual-use topics. Notably, Anthropic's recently released cutting-edge language model [Claude 2](#) features a notably higher barrier than GPT-4 for handing its users detailed instructions for dangerous experiments.

At the same time, it is important that these tools enable scientists with appropriate training and approval to develop new medications and vaccines. Thus, differentiated access methods are needed for AI-powered lab assistants and biological design tools. This might require advancing ways for legitimate scientists to authenticate themselves online. For instance, to access model capabilities for predicting immune evasion variants of influenza virus to inform vaccine design, a scientist might need to authenticate and provide appropriate documentation of biosafety and dual-use review.

Beyond exacerbating biosecurity risks, advances in artificial intelligence also present an opportunity. As progress in AI spurs more rigorous gene synthesis screening, this will strengthen biosecurity more broadly. And as biological risks drive AI governance measures like pre-release evaluations of large language models, this will mitigate a wider array of artificial intelligence risks. Swift action by policymakers will not only enhance safety but also pave the way for reaping the many benefits of artificial intelligence.

[Jonas Sandbrink](#) is a biosecurity researcher at the University of Oxford and a biological security adviser at the UK Cabinet Office. This article is based on his recently published [preprint](#) titled "Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools."

Navigating considerations of global governance, national strategies, and ethics in biowarfare

By Shravishtha Ajaykumar

Source: <https://www.orfonline.org/research/navigating-considerations-of-global-governance-national-strategies-and-ethics-in-biowarfare/>

Aug 07 – The term 'biotechnology' can refer to any of its various use cases in agriculture, climate management, DNA studies, and many other domains with human life at the core of innovation.^[1] It is a field of technology aimed at domains such as improving human health, environmental protection, preservation of biodiversity, scientific innovation, and improved agriculture.^[2] In 2005, the Organisation For Economic Co-Operation and Development (OECD) Ad Hoc Statistics Group on Biotechnology defined 'biotechnology' as the application of science and technology for parts, products, and models of living organisms for application in goods, services, research and development.^[3] These definitions were expanded to include DNA/RNA, proteins and other molecules, cell and tissue culture and engineering, processing of biotechnologies, gene and RNA vectors, bioinformatics, and nanobiotechnology.

In the field of security, biotechnology research is a vast space, embracing goals such as providing healthy food for soldiers, increasing preparedness in natural disasters and emergencies, and deploying emergency healthcare.^{[4],[5]} Biotechnology has contributed to the enhancement of human life in many ways, but like many innovations, provokes a dual-use dilemma: While biotechnology can assist in improving healthcare and food security, the same technology can be used to perpetuate harm or the threat of harm for geopolitical and strategic purposes—or what is known as biowarfare. 'Biowarfare' refers to the intentional use of biological agents (e.g., bacteria, viruses, fungi, and toxins) as weapons in war scenarios.

This paper focuses on the use of biological agents in warfare and describes historical instances of biological weapon use and emerging technologies with future use potential. It highlights governing structures, outlines India's perspective of biowarfare, and explores how the country can leverage its multilateral alliances to enhance biological weapons deterrence.

Historical Mapping and Contemporary Use of Biological Warfare

Biological weapons can potentially be more dangerous to civilian populations than conventional and kinetic weapon systems, as even minute quantities can cause mass casualties depending on the agent used. The use of biological weapons also adds an element of deniability; if the result is not or cannot be effectively traced back to a source due to its potentially significant area of impact or it is mimicking a natural outbreak, the users of biological weapons could escape accountability.^[6] Dual-use for harm is an externality of biotechnology, as with many technological



innovations. Thus, in biological warfare,^[a] the irremovability from human life augments social and geopolitical concerns around use.^[7] Historically, warfare has included biological weapons.^[8] This use, even when small in scale, has warranted awareness, regulation, and monitoring discussions to aid strategic and deterrence efforts. As Table 1 shows, the intentional use of microorganisms (or their toxins) as weapons is not an uncommon practice and it has had notable impact for decades. The evolution of biowarfare over time can be divided into three periods:^{[9],[10]}

1. Leading up to the 1900s, when biological weapons and toxins were used for political espionage.
2. 1900-1945: This period was characterised by the emergence of small and unsophisticated national biowarfare programmes (e.g., Germany, Japan, the Soviet Union, and the United States) and the use of biological weapons in the First and Second World Wars.
3. After 1945: Broader access to biological agents and the progress made in the field of biotechnology allowed biowarfare programmes to be more accessible even to small groups and individuals. During this period, the lethal potential of biowarfare agents increased due to developments in genetic engineering.

Table 1: Significant, Large-Scale and Recorded Use of Biowarfare

Era	Toxin Carrier	Toxin	Impact
Pre-World War I	Bacteria	Agroterrorism (glanders and Anthrax)	Germany shipped infected livestock to Americanised countries to disrupt the food chain pre-World War I.
World War II	Insect	Flea vector (plague)	The Japanese Army developed the Uji Bomb ^[11] and sprayed allies with infected pathogens, killing approximately 100,000 people.
	Insect	Agroterrorism: potato beetle	France and Germany attempted to use insects such as the potato beetle to destroy crops.
	Insect	Lice vector (typhus)	The Soviets used typhus-infected lice against German troops.
	Insect	Mosquito vector (yellow fever)	The Canadian military used <i>Aedes aegypti</i> ^[b] to transmit yellow fever.
	Bacteria	Anthrax and waterborne organisms	Japanese Army Units 731 and 100 are said to have experimented on humans with aerosolised Anthrax.
	Bacteria	Tularemia	Allegations of Soviet use against Germans
Korean War	Toxin	T2 mycotoxin	Allegation of US use against North Korea in 1952
Cold War	Insect	Vectors	US and Canadian military research and development on using fleas, flies, and mosquitoes to transmit infection.
	Bacteria	Plague and tularemia	US and Russia developed techniques for aerosolising plague and tularemia.
	Bacteria	Anthrax	April 1979: An inhalational anthrax outbreak was reported near the Soviet Institute of Microbiology and Virology at Sverdlovsk, USSR.
	Toxin	T2 mycotoxin	Allegation of Soviet/Vietnamese use in Cambodia and Laos in 1975–1981
	Toxin	Aflatoxin	Iraq 1980: evidence to suggest work to weaponise aflatoxin
Present	Bacteria	Anthrax	Japan 1990–1995: Aum Shunrikyo sect attempts to develop aerosolised anthrax and botulinum toxin



Bacteria	Anthrax / Amerithrax	United States, 2001: After the attacks on the twin towers, many received letters laced with anthrax resulting in the death of 5 Americans, with 17 others falling ill. ^[12]
Toxin	Ricin	United States, 1 November 2011: 3 men arrested by the Federal Bureau of Investigation for planning a ricin attack on US government offices
Toxin	Ricin	United States, April 2013: Letters containing ricin mailed by an unknown perpetrator to the President and a Senator were intercepted before delivery to their recipients

Source: Michael D Christian. "Biowarfare and Bioterrorism."^[13]

The biowarfare capabilities of states have varied across time, ranging from small-scale attacks on stakeholders to larger events that aimed at livestock and agriculture. These attacks, and the uncertainty of scale of impact, contribute to geopolitical tensions; in response, international bodies such as the United Nations Institute for Disarmament Research and the World Health Organization are seeking to supervise biotechnology innovation.^[14] As seen in Table 1, the different uses of biological weapons have expanded the definition of 'biotechnology in warfare' to include various organic carriers, capability objectives,^[4] and the influence of organic weapons.^[15] Spencer (2001) defines the use of biological weapons in war or "bioterrorism" as "the usage of microorganisms as guns of catastrophic impact, which may be defined as the class or approach of use of a weapon gadget that outcomes in a good-sized terrible effect on a nation's bodily, mental or monetary well-being, thereby inflicting a primary amendment of habitual activity."^[16] Therefore, 'biowarfare' is an umbrella term for the state use of biological weapons in war zones, deterrence strategies and research for defence potential. Meanwhile, 'bioterrorism' refers solely to the use of biological weapons by state or non-state actors against civilian populations.^[17] These definitions assist in identifying the use of biological weapons outside of war zones; the susceptibility of non-humans, such as farm animals, and crops, to bioterrorism and agroterrorism^[4] remains consistent. Further, as bioterrorism does not target humans directly, the deniability of accountability is more significant than in biowarfare.

Heightened Threat of Biotechnology Use in Warfare

Genomic Editing and Synthetic Biology

Genetic engineering, first developed in the 1970s, manipulates DNA or RNA, setting the foundation for genomic editing in the present day.^[18] This technology has developed at a rapid pace in the last decade, influencing research and development in biomedicine and technology as well as applications in agriculture in the form of Genetically Modified Organisms or GMOs.^[19]

Genomic editing has three prevalent subtypes: zinc-finger nucleases (ZFNs); transcription activator-like effector nucleases (TALENs); and clustered regularly interspaced short palindromic repeat (CRISPR)–Cas-associated nucleases.^[20] An extension of CRISPR-Cas are two methods for identifying viral vulnerability or presence in genetic samples. These are specific high-sensitivity enzymatic reporter unlocking (SHERLOCK) and the DNA endonuclease-targeted CRISPR trans reporter (DETECTR).^[21] Genomic editing tools like CRISPR-Cas hold promise in applications for immunotherapy, cancer research, and vaccine development.^[22] Its offshoots—SHERLOCK and DETECTR—can identify the presence of viruses or lack thereof in any organism, even if asymptomatic. These two together offer a unique contemporary solution of biodefence^[4] to threats of limited traceability and uncontrolled scope of impact in biowarfare.^[23] However, these innovations in genomic editing also contribute to the dual-use dilemma. Genomic editing has other uses that could heighten the potential threat of future biowarfare tactics in the following ways:

1. Genomic Editing and Gain of Function Research:^[4] Synthetic biology^[4] and genetic editing offer options for repairing genetic defects in living organisms; however, the same can be used to enhance the harmful aspects of viruses and increase the potential of biohacking. An example of this is creating dangerous covert viruses that use harmless bacteria as carriers. This has been demonstrated in experiments conducted by infecting copy DNA (cDNA or DNA reconstructed to imitate an existing strain) with an RNA virus with poliovirus, influenza, and coronavirus.^[24] To counter malicious biohacking and genetic editing, the US Defence Advanced Research Projects Agency (DARPA) is exploring its Insect Allies Program to defend crops against biological threats using Horizontal Environmental Genetic Alteration Agents (HEGAAs).^[25]

Gain of Function Research has, in recent years, referred to a series of experiments attempting to reduce the impact of the H1N1 virus on humans.^[26] This ability to alter the potency and manipulate the effect of a virus on other organisms creates concerns of dual use.^[27] For example, due to the dual use of potency manipulation of a virus, this research was paused in 2012. It was revived in 2017, with the US government lifting the ban and outlining assisting regulations to oversee the Gain of Function and prohibit government funding.^{[28],[29]}



- Antimaterial Weapons: Some types of bacteria and fungi are used to break down plastic and carbon sources. Research is ongoing on enhancing plastic-degrading enzymes to assist in climate change control.^[30] These enzymes, used incorrectly and maliciously, can destroy and degrade infrastructure and harm the ecology and humans as conventional bioweapons do.

Current Global Biowarfare Capabilities

Nation-States with Bioweapon Capabilities

There are a number of countries listed in open-source documents suspected of being non-compliant in the use of biological or chemical weapons.^{[31],[32]} J Tucker and K Vogel (2000) have highlighted countries with programmes and capabilities in biological warfare, including China, Egypt, North Korea, Iran, Israel, Russia, and Syria. This list also includes (by incorporating chemical warfare with biological warfare research) Burma, Cuba, India, South Korea, Laos, Pakistan, and Taiwan.^[33] The James Martin Centre for Non-Proliferation Studies, in its 2008 roster, also listed China, Egypt, North Korea, Iran, Israel, Russia, and Syria as suspected purveyors of biowarfare programmes.^[34] The list also included Canada, Germany, and India, and reiterated other larger countries with past programmes and research in biowarfare, like Russia and China.^[35]

To compare the level of biowarfare capabilities, this paper ranked the countries based on the commonalities in these three studies, factors outside of biowarfare (such as chemical warfare), and the rankings given to them present in all three studies. The categories are Advanced, Intermediate, and Novice.^[1] Biowarfare Capabilities (Table 2).

Table 2: Historical and Contemporary Global Biowarfare Capabilities

Country	Status	Ranking as Given by Mezzour et al. ^[1]
Russia	Advanced	Advanced
China	Advanced	Intermediate
Iran	Advanced	Advanced
Iraq	Advanced	Advanced
Syria	Intermediate	Advanced
Libya	Intermediate	–
North Korea	Intermediate	Advanced
Egypt	Intermediate	Advanced
Israel	Intermediate	Advanced
Burma	Novice	Intermediate
Cuba	Novice	–
India	Novice	Advanced
South Korea	Novice	–
Laos	Novice	–
Pakistan	Novice	Advanced
Taiwan	Novice	Advanced

While the three studies mentioned above list countries with suspected or past biowarfare programmes, that by Mezzour et al. (2014)^[36] showed the capabilities of countries that have also conducted biotechnology-focused research and nuclear research and have nuclear weapons capabilities. Thus, due to the academic pillar of their methodology, the resultant ranking differs from the one presented in the preceding three studies, as shown in Table 2.



Outside of these lists, protections on biowarfare and weapons, and by extension standards for maintenance and monitoring need to be implemented in the countries mentioned above and in others as well. A necessity for this is unreported research, development, and procurement of biological weapons. The lists mentioned above do not mention the most technologically advanced countries globally, such as Finland, the US and Japan.^[37] While they might not have any biowarfare research ongoing, concerns remain.

Non-State Biowarfare Capabilities

Non-state actors are also part of the landscape of biowarfare. The Al-Qaeda, for example, is said to be in possession of biological weapons. Reports from refereed journals have pointed to the alleged involvement of the former Soviet Union in assisting the Al-Qaeda in sourcing these agents.^[38] Other countries and regions like Kazakhstan, the Czech Republic, Afghanistan, and East Asia are also said to have relations with Al-Qaeda in sourcing and purchasing biological weapons, toxins and agents.^[39]

Individuals and small parties have often been seen trying to access biological weapons on the darknet.^[40] The Interpol has created an 'Operational Manual on Investigating Biological and Chemical Terrorism on the Darknet' and formed the National Biosecurity Working Group (NBWG)^[41],^[42] to assist law enforcement officials in identifying and mitigating instances of bioterrorism.

Neuroscience and Technology Application in Warfare

Similar to biological weapons, genetic editing and synthetic biology innovations have also led to developments in neuroscience that could, potentially in the next decade, include manipulating brain functions in warfare.^[43] These can consist of using biological agents that impact neurological ability:^[44]

1. Neuropharmacological and pharmacological agents^[45] that enhance or inhibit an individual's neurological functioning. These can include Amphetamines, MDMA, LSD, and Ketamine.
2. Neuromicrobial agents,^[46] including anthrax or gene-edited bacterium, that can spread viruses.
3. Organic Neurotoxins like Bungarotoxin, Conotoxins, and Najatoxins.
4. Neurotechnological devices^[47] like transcranial neuromodulatory systems, direct-delivery nanosystems, and neuro nanomaterial agents that can help with enhanced delivery and absorption of chemicals.

The use of these features of neurotechnology in warfare is currently unregulated. Moreover, the strategic use of neurobiological data and automation features can enhance the potential use of neuroscience in bioterrorism and biowarfare by altering brain functioning, improving it for allies and inhibiting it for targets.^[48]

Detecting the Use of Biological Weapons

Challenges in Detection

Describing the epidemiology of agents of bioterrorism is a massive challenge for several reasons.

First, there are unknown factors involved, including the scope of bioterrorism, applications and impact of emerging technology, and the effect of automation on the creation of biological and chemical agents. Further, with the speed of developments in emerging technology, it is hard to gauge the future impacts of biological weapons or the forms biological weapons might take.^[46]

Second, as will be discussed in a latter section of this paper—while the Biological Weapons Convention bans the use of biological weapons, there are no verification or investigation mechanisms and the authorities rely on self-reporting.^[47] Furthermore, since military or state organisations have conducted most of the work on bioweapons, only a small proportion of these activities have been publicly reported. There is limited publicly available knowledge on the monitoring of research in the field of biological weapons and biotechnology innovations outside of defence.^[48]

Methods for Detection

The first step in monitoring the use of biological weapons and preventing acts of bioterrorism is to identify them over naturally occurring outbreaks. While both warrant disaster management, identifying both, assists in highlighting levels of deterrence and disaster management.

1. Sanger Sequencing: Unlike traditional forms of warfare, biological warfare and bioterrorism can be covert and untraceable to its source. The impact on living organisms and dependence on living organisms to transfer and carry biological agents and toxins results in a challenging outcome in distinguishing between manufactured events (terrorism) and natural phenomena (epidemics). Some popular methods to determine the origin include the classic Sanger sequencing,^[49] devised by Fred Sanger.^[49] Sanger sequencing, by outlining genome evolution, can predict natural evolution and points of human intervention that would lead to the studied outcome (in these cases, carrying a virus or biological/neurobiological toxin).^[50]

2. Radosavljevic and Belojevic's Method: More recently, a scoring system was developed by Vladan Radosavljevic and Goran Belojevic^[51] that helps differentiate between bioterrorism incidents and epidemics. These investigators use an approach that assesses an incident's qualitative and quantitative



characteristics. These traits fall into three groups that are scored: people (cases), places (spatial distribution), and time. Out of a total of 14, a score of 8 or higher in this system indicates that an event is “more likely” to be artificial (deliberate or accidental) than a naturally occurring epidemic.

For example, in the case of an H1N1 virus outbreak, the three groups would include the number of people affected at first instance and the number of unexpected cases, the non-response to medication, and the clustering of the outbreak. The second category for analysis would include spatial distribution, including limited plausibility for natural occurrence based on ecology, and simultaneous outbreaks in other regions without travel or infection. Finally, the third pillar would be time distribution, requiring such outbreaks to happen in concurrence or immediacy.

This system has helped establish a required level of situational awareness that clinicians cannot achieve in a hospital setting. Therefore, the effective judgment of the origin of an outbreak needs implementation at the public health level rather than that of the individual clinician.

3. Global Adoption of Identifying Outbreak Source: The North Atlantic Treaty Organization (NATO) and the US Centers for Disease Control and Prevention (CDC) developed another method to determine the scope of an act of bioterrorism versus that of an epidemic. This method, similar to Radosavljevic and Belojevic’s, outlines the plausibility of a natural outbreak by measuring certain features of the outbreak:^{[52], [53]}

- Identification of a cluster of cases (large numbers of patients from a similar geographic area with similar symptoms)
- High and rapid fatality among cases
- Many casualties within the first 72 hours may indicate a microorganism attack or within minutes to hours, which may be due to a toxin.
- A lower attack rate in people indoors than outdoors.
- Abnormally high prevalence of respiratory-related disease in diseases commonly cause non-pulmonary syndromes when acquired in nature.
- Casualty distribution aligned with wind direction.
- An illness type highly unusual for the geographic area
- The appearance of a category A, B, or C disease (as defined by the CDC)
- Increased numbers of affected animals, of varying species, in a designated geographic area
- Witness to the attack or discovery of an appropriate delivery system

If the outbreak scores high on these markers in the checklist, there is an increased plausibility of a manufactured act of bioterrorism.

4. High Throughput Sequencing: In the early 2000s, high-throughput sequencing (HTS) [also known as massively parallel sequencing (MPS) technology or next-generation sequencing (NGS)] was introduced. This technology functions as Sanger Sequencing does; however, due to its improved multiplexing capabilities,^[4] this method allows whole-genome sequencing (WGS) of single microorganisms (viruses, bacteria, and fungi) or multiple organisms within an environmental sample. It can simultaneously address multiple DNA/RNA strains for more thorough, cost-effective and time-effective outcomes.^[54]

In 2014, the HTS approach was introduced into routine diagnostics and used to study outbreaks and transmission and to genotype highly resistant organisms. In collaboration with molecular microbiologists and infection control specialists, clinical microbiologists and infectious disease specialists often rely on HTS to identify sources, detect outbreaks, transmit pathways, pathogen evolution, and identify the dynamics of multidrug-resistant pathogens.^[55]

The predominant benefits of HTS over classical Sanger sequencing are:

- i. High-throughput capability: Hundreds of thousands of sequencing reactions may be carried out in parallel, allowing complete sequencing of a whole bacterial genome in a few run-throughs.
- ii. An available protocol for identity and genotyping may be implemented for all microorganisms.
- iii. DNA cloning is eliminated, solely relying on library preparation in a cell-loose system.
- iv. No earlier know-how approximating the collection of a specific gene/genome is required because HTS can examine the DNA templates randomly disbursed at some stage in the complete genome, after which a de novo genome meeting^[6] may be implemented.
- v. No need for isolation, and the lifestyle of the microorganism of interest is incredibly essential. Many traces cannot develop in lifestyle media, permitting the identity of microorganisms and those formerly undetected via more traditional methodologies.
- vi. Cost (generally less than US\$1,000) in keeping with the genome, relying upon the genome length) and the discount in turnaround time (only some hours).^[56]

Widespread use of microbial forensics, including the methods mentioned above, requires educating the forensics community. Implications of such methods need to include reporting by private sector



organisations of research and innovation activities, monitoring of the same and transparency requirements, including applying legal and trustworthy standards for genetic data protection and accuracy of generated data. These include correct use of databases and information tools. End users (crime scene investigators, lawyers, judges, juries) must utilise these innovations to contend with the use of biological weapons and address naturally occurring outbreaks.

Guidelines for Biological Weapon Deterrence

As the potential of biological weapons increase with innovation, national security establishments are being tasked to accord greater attention to deterrence. For example, gene editing has been cited in the US Director of National Intelligence Annual Report 2016, citing suspected development of biological and chemical weapons in states like the Democratic People's Republic of Korea, the People's Republic of China, Russia, and the Islamic Republic of Iran. The same report highlights concerns around biochemical weapons used by Syria and the Islamic State.^[67]

Apart from the speculated use by state and non-state actors, emerging technology in this field has also resulted in academic interest in security and strategy in the field of biological weapon use, i.e., biosecurity.^[68] The US's CDC has identified and classified a list of potential bioterrorism agents.^[69] Agents identified by the CDC are accepted by most authorities worldwide as top priority for preparation and research. Others like Relman expand on this list to include agents that have seen heavy use and research by previously significant military programmes and may hold significance in future research and service.^[60]

Although the danger of large-scale bioterrorism is low, the potential for use at smaller scales and in tandem with other warfare tactics is still prevalent.^{[61],[62]} As shown in Table 1, Anthrax, a lethal agent commonly used in small-scale attacks on high-level stakeholders, has impacted the surrounding populations.^[63]

Certain mechanisms are in place to mitigate the threat.

Biological Weapons Convention

While detection methods for biological weapons are advancing, the ethical guidelines and global regulations have remained constant. As mentioned in earlier sections, the Biological Weapons Convention (BWC) is a legally binding treaty banning the use, development, and trade of biological weapons. After being discussed and negotiated at the United Nations Forum on Disarmament since 1969, the BWC was launched on 10 April 1972 and entered into force on 26 March 1975. It currently has 183 Parties.^[64] BWC prohibits:^[65]

1. Development, inventory, acquisition, storage, and manufacture of weapons, equipment, delivery vectors, biological agents, and toxins.
2. Acquisition or assisting in acquiring agents, toxins, weapons, equipment, and means of transport to be used as weapons.

The Convention further requires States' Parties to destroy or divert "drugs, poisons, weapons, equipment and means of transport" for peaceful purposes within nine months of the Convention's entry into force. These include the weaponisation of biological agents such as Anthrax, Smallpox and Tularemia; and the weaponised use of dual-use toxins such as clostridium botulinum toxin, staphylococcal enterotoxin-B (SEB), conotoxin, clostridium botulinum (BTOX), chimaera pathogens and other derived biotoxins.^[66] The BWC limits the use of pathogens listed above for offensive use. However, it does not ban research on such pathogens for biological weapons deterrence.^[67]

The treaty permits signatory states to consult with one another and cooperate, bilaterally or multilaterally, and address compliance concerns. It also allows States to complain to the UN Security Council (UNSC) if they believe other member states are in violation of the Convention. The UNSC can investigate complaints, though this power has never been invoked. The Council's voting rules give China, France, Russia, the United Kingdom, and the United States veto control over decisions, including those on conducting BWC investigations.^[68]

In June 2023, the BWC established its Biological Weapons Convention National Implementation Measures Database, which allows users to track all national signatories, national programmes and interactions between nations in the field of biological weapon use, research and deterrence.^[69] The BWC also regularly convenes for review conferences and in March 2023 established a Working Group to enhance implementation measures, expanding these to legally binding measures where possible and assisting in expanding and strengthening the Convention.^[70] The Working Group is charged with prioritising scientific and technological research and development and economic growth as a product of international cooperation in the field of biotechnology.^[71] The BWC has seen success in its standards by keeping its fundamentals clear and focusing on the scope of impact of biological weapons rather than altering the need for impact assessment based on the evolution of technology. That is, while biotechnology evolves and innovations in this field emerge, the scope of impact is still measured in human life alteration.



Addressing Limitations

While the BWC has taken steps in limiting the use of biological weapons, some limitations necessitate a rethinking of the treaty.

1. The treaty has been flagrantly violated in the past. For example, the Soviet Union, a party to the treaty and one of its depositaries, maintained an extensive offensive biological weapons programme after ratifying the BWC. While Russia claims that the programme is no longer live, questions about its remnants have not been satisfactorily put to rest.^[72]

In November 2001, the US alleged that Iraq and North Korea had violated the treaty's terms. The US also expressed concern about compliance by signatories Iran, Libya, and Syria.^[73]

With the new working group established in the ninth review conference in March 2023, possible legal guarantees for non-compliance can be discussed and outlined to address this limitation.

2. In 2020, the powers attributed to the UNSC countries to collaborate in the case of disaster management of 'non-traditional' geopolitical issues, especially concerning biological weapons or epidemic outbreaks, were tested. Amid the SARS-Cov-19 outbreak in early 2020, the UNSC could not find a common stance and did not respond effectively until later in July, when they passed Resolution 2532 to cease fire globally and prioritise tackling the pandemic. This delayed response indicated the lack of cooperation at the UNSC level despite BWC and UNSC guidelines creating a foundation for effective and timely responses.^[74]

As this resolution has already been passed, it can act as an example for future disaster management in case of epidemics. However, there needs to be a more substantial representation of global efforts over national interests in the UNSC to encourage this.^[75]

3. The definitions of the BWC have been intentionally inclusive and vague to avoid limited classification. Despite this, they are not inclusive of neuropharmacological agents or neurotechnological innovation to augment delivery systems, gene editing, nanoengineering outcomes for biological weapons, use of biological weapons to impact infrastructure and non-living landscapes, and the possibility of using neurotechnology and humans as biological weapon agents.^{[76], [77]}

Expanding the definition of what consists of biological weapons will target this limitation, as would the newly established working group reviewing this list regularly with upcoming innovations.

The Cartagena Protocol and Nagoya Protocol

The United Nations Conference on Environment and Development (UNCED) established The Convention on Biological Diversity in 1992 to oversee technology and knowledge transfer with relevance to biological diversity and sustainability.^[78] The Convention on Biological Diversity, however, does not limit; rather, it enhances research in biotechnology while prioritising safety and curbing threats to diversity. To achieve these goals, the Cartagena Protocol was established and adopted to ensure "the safe transfer, handling and use of living modified organisms resulting from modern biotechnology that may have adverse effects on the conservation and sustainable use of biological diversity, also taking into account risks to human health, and specifically focusing on transboundary movements."^[79] Currently, the protocol has 173 parties with 103 signatures.^[80]

The Convention on Biological Diversity in 2010 also established the Nagoya Protocol.^[81] The protocol, with 140 signatories, aims to facilitate "fair and equitable sharing of the benefits arising from the utilisation of genetic resources, including by appropriate access to genetic resources and by appropriate transfer of relevant technologies, taking into account all rights over those resources and to technologies, and by appropriate funding, thereby contributing to the conservation of biological diversity and the sustainable use of its components."^{[82], [83]}

Addressing Limitations

While the Cartagena Protocol oversees the sustainable and safe impact of biotechnology on living organisms and includes any transfer of biological agents that may harm ecology and human health, the Nagoya Protocol oversees responsible data sharing and benefit sharing in gene editing. Each protocol, on its own—and the two in combination—are unable to cover the gap.

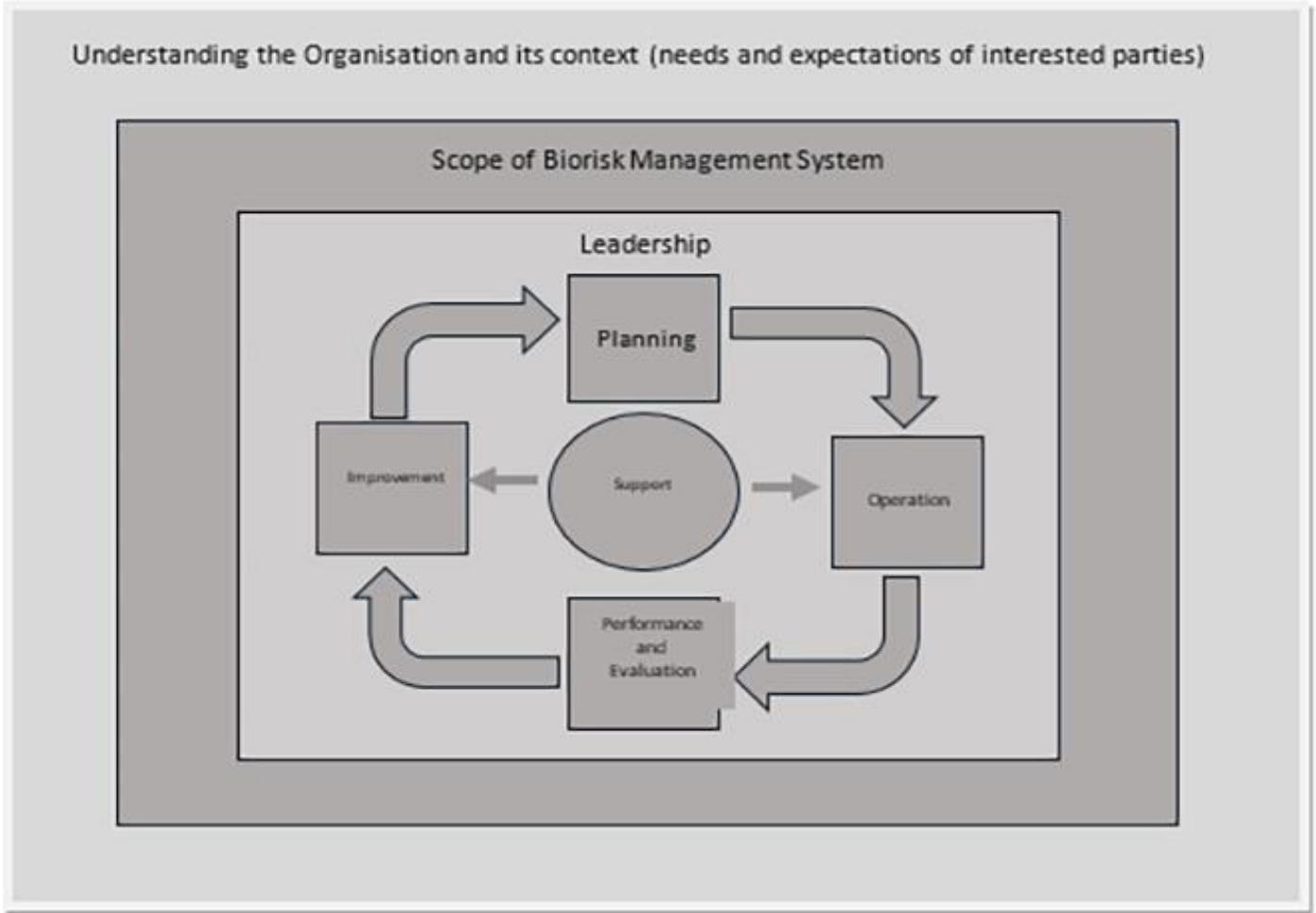
The knowledge transfer of gene editing is encouraged, and biological agents that may come in chemical form, including neurobiological agents, are not covered. This creates a gap in guidelines for the potential knowledge transfer for developing neurobiological agents and using humans as agents of transfer.^[84] Similar to the need to expand on definitions as with the BWC, the Convention of Biological Diversity can either encourage new protocols to include neurobiological agents and human carriers or create addendums to existing protocols with regular review processes.

International Standards Organisation

In November 2019, the ISO released a comprehensive set of standards on biorisk management, i.e., mitigating leakages from laboratories that conduct research and intelligence on biotechnology and its subparts. These standards include maintaining records and establishing biorisk management principles that enable laboratories and related facilities to mitigate biorisk.^[85]



Figure 1. ISO's Biorisk Management System Model (In top-down pyramid view)



Source: ISO 35001:2019: *Biorisk management for laboratories and other related organisations*.^[86] To oversee safety in biolabs and prevent accidental leaks.

As shown in Figure 1, while the ISO standards are comprehensive, the model is presented for management. This framework and model have been adapted from another ISO Standard, ISO 45001 on Occupational Health and Safety management system — Requirements with guidance for use. While its application in most civilian cases of biorisk management may be transferrable for the purposes of biowarfare, the ISO misses on an imperative need for monitoring and international standards on dual-use biotechnology.

Addressing Limitations

The standards presented by the ISO depend on self-governance and implementation, not calling to action any global authorities or national organisations to take charge of implementation and increased accountability. Governments should establish bodies that will ensure that biological labs are certified to follow ISO rules by encouraging funding or subsidies in research to those who are certified and completely compliant.

World Health Organization

The World Health Organization (WHO) too, has an outbreak toolkit that can be used to investigate suspected or natural outbreaks and epidemics.^[87] The toolkit has four overarching stages.

Stage 1: To detect, alert and report any possible cases of bioattacks/epidemics.

Stage 2: To begin information gathering and evaluation.

Stage 3: To increase and supplement the base data collected by adding environmental data, clinical information, technological assistance and statistical plausibility.



Stage 4: To conduct field investigations which, unlike most other standards, include the psychogenic impacts beyond toxicological and environmental impacts.

Stage 5: The final results of the study and investigation which may be released in form of a public report, or can be used for internal determination.

This framework is often used to investigate alleged bioattacks. Further, the UN Secretary-General has the authority to investigate the possible use of bioweapons.^[88]

Addressing Limitations

Bureaucratic delays between WHO and the UN Secretary General's office slows the process of detection and there is a need for a third-party or subsidiary organisation that can expedite.^[89] Establishing a coordinating authority that removes these delays will reduce the time allocated to monitoring, assessment and reporting of bioterrorism or epidemic instances.^[90]

The Regulatory Landscape in India

India has strong biotechnology capabilities but has focused its efforts outside of biowarfare and biological weapon deterrence.^{[91],[92]} The country's priority has been on research and development, as seen in the National Biotechnology Development Strategy 2021 – 2025.^[93] Research in recent years has engaged public health as its main outcome, including diseases like cancer, tuberculosis, and malaria, as can be noted with the scope of biological data collection for biotechnology research by biobanks in India.^{[94],[95]}

India's current regulations around biotechnology development are inclusive, with guidelines on data and benefit sharing in biotechnology, guidelines for gene editing, and Biosafety Programme.^{[96],[97],[98]} There are significant gaps in the guidelines, however. For one, while they address the need for funding and innovation in the field of biotechnology, the Biosafety Programme has not been updated to include human carriers or neurobiological agents as weapons.^[99] This results from isolated expertise and knowledge mismatch between scientists and policymakers.

To lead the strategy and deterrence in the biowarfare landscape, India must be equipped to detect or respond to biological threats from both natural and artificial sources. India must raise awareness, bridge science and policy, and mobilise resources. An essential part of biological weapons is the risk of impact on human life and ecology, and thus necessary to consider in deterrence. India is also vulnerable to these risks due to its high population density, weak public health infrastructure, low public health spending, and lack of training and awareness on biosecurity and measures.^[100]

When naturally occurring infectious agents such as disease-causing viruses accidentally escape storage facilities, naturally evolve, or are manipulated to be used as biological weapons—all life is compromised. Therefore, despite India's growing biotechnology capacity in academic and industrial settings, it must be equipped to detect or respond to threats from either source.

India has signed a 10-year defence framework agreement with the US, which includes provisions for "a lightweight, protective suit effective in chemical and biological hazard environments."^[101] However, this move does not explicitly discuss a need for deterrence strategies. India needs to further strategic realignment of the Department of Biotechnology, National Disaster Management Agency, and Defence Research and Development Organisation to address the gap in biotechnology applications in strategy and security. This realignment will create a resurgence in focus on biotechnology research in disaster management and security applications.

The most significant gaps can be seen from a political and governance perspective. Having a single agency that looks after the process of biotechnology innovation, including in the field of defence, does not need to replace existing authorities, like the Department of Biotechnology. An organisation (akin to the Indian Space Research Organisation, or ISRO, for the space industry) can act as a coordinating authority to ensure all agencies have strategic alignment. This agency will also assist in staff capacity building and regular training in detecting and reporting biological threats. It could remove the issue of siloing, as it will not be concerned with only scientific innovation, as the Department of Biotechnology is, nor only strategic use of biotechnology, as any defence-led organisation might be.

India has also been a significant member of multilateral alliances with similar interests in technological advancement and utility for human life enhancement. One such multilateral alliance is the Quad Security Dialogue or Quad.

Leveraging the Quad

The Quad of the US, Australia, India, and Japan began their maritime cooperation after the 2004 Indian Ocean tsunami. Today, the four countries have a much broader range of interests, including security, economic and health issues.^[102] So far, the four have focused their biotechnology efforts on biopharmaceuticals, genomes, agricultural biotechnology, and industrial biotechnology.^[103]

India and the US have both been listed as countries with biowarfare capabilities and awareness, as shown in previous sections, determined by including academic research and historic participation in biowarfare.



However, these two countries have not been listed under any suspected lists of contemporary biowarfare activities. Australia and Japan, too, have aligned themselves with the BWC.^{[104], [105]}

The Quad can be a powerful platform in influencing the landscape of biological warfare in the following ways:

1. Collaboration and a united front: All four countries have a vested interest in biotechnology innovation and the landscape of biological weapons deterrence, as characterised by their participation in the Cartagena Protocol, Nagoya Protocol, and the USA-India defence framework bilateral agreement.

Australia, too, through its Defence Science and Technology Organisation (DSTO) under the Department of Defence operates the Biological Defence Research. This office seeks to ensure biodefence in areas where biological weapons may be used and enhance Australia's participation in biological weapons deterrence.^[106] For its part, Japan is also a member of the Australia Group^[6] under the BWC and maintains strong controls and reports over the trade and transfer of biological agents.^[107] India, the US, and Australia are also members of the Australia Group.^[108]

In this area, there can be collaborations to represent common interests and increase focus on biosecurity. The 'One Health' initiative already provides a framework for international collaborations focusing on human health and that of other living organisms.^[109] While this is for naturally occurring outbreaks, a similar mechanism can be adapted to highlight disaster management in the case of bioattacks. Furthermore, with the Quad, WHO can highlight this initiative, which can in turn further the interests of the Quad countries concerning bioweapons disarmament and biorisk management and monitoring.

3. Setting an example to enhance standards: The Quad can further align itself on the current controls and standards on laboratories and present any further standards that should be implemented as discussed in the section on the ISO biorisk management standards, self-reporting leakages and identification of any "lab-specific issues".

The Quad countries also have biobanks monitored and overseen by national regulations or guidelines.^{[110], [111], [112], [113]} By creating monitoring standards for other forms of biotechnology research and data sharing standards within this platform, the Quad can encourage monitoring and data sharing of non-strategic biological and biotechnological laboratories and setting standards, thus, for the rest of the world.

3. Reviewing assessment methods: Angela Kane, a disarmament advocate and diplomat, has advocated for the Joint Assessment Mechanism (JAM) under the Nuclear Threat Initiative (NTI). The JAM is proposed to be housed under the UN Secretary General's Office and expedite the assessment of suspect biological events.^[114] The NTI would act as a subsidiary office reporting directly to the UN Secretary-General on any exploitation or non-compliance of the BWC. A collaboration like the Quad can also align itself with newer assessment methods like JAM, and advocate for its adoption by the UN and WHO to ensure future epidemics and bioattacks are detected and contained faster.

4. Prevent non-state actors from accessing weapons: The Quad countries can align their border control and cybersecurity authorities with Interpol for collaboration and cooperation to curb the traceable purchase and trade of biological agents and weapons. This can be done using mechanisms established by Interpol, like the Operational Manual on Investigating Biological and Chemical Terrorism on the darknet to trace purchases online and a National Biosecurity Working Group (NBWG) to align trade between the Quad countries. These measures will assist in curtailing individual and non-state actor access to bioweapons and can be a step in the right direction to make the Quad a change-maker in the field of disarmament.

Future Challenges

Biowarfare is no longer a naturally occurring agent that impacts all life. With innovations, there is scope for newer bioweapons and biowarfare.

- Genome editing and synthetic biology have made it possible to identify and impact only certain groups of people with a bioweapon and manipulate the potency of existing viruses or diseases in carriers.^[115] Concerns around this include the potential grave impacts on local ecosystems and people. Guidelines and guarantees around the use of genome editing, synthetic biology and biometric informatics for weapons need to be highlighted.
- With the advent of Artificial Intelligence and growth in data sets, the scope of bioactive components and toxins being expanded upon by AI is possible.^[116] Policies around this area need to ensure that AI in warfare is not permitted to help develop chemical compounds that can be used to create toxins.
- Biolabs are the basis of research and innovation in biological and chemical agents. However, such research and innovation can be conducted outside traditional biolabs. What comprises a biolab and the basic requirements to be certified as a biolab must be redefined. With technologies overlapping and innovating, leakages are also possible from non-traditional and non-biological labs, and thus contemporary definitions are required. Such redefining will help monitor efforts and government intervention in case of leaks and track sales and purchases of biological and chemical agents, even in small amounts.



- Dual-use dilemmas need to be expanded. As seen in the brief section on neurobiological weapons, some are used as recreational drugs. Specifically, how drugs allowed in free trade can be misused by malicious parties need to be considered. Thus, expanding definitions in dual-use concerns will help monitor and mitigate the trade and transfer of neurobiological agents.
- War gaming, [AI](#) running simulations or controlled experimentation of biological weapons need to be introduced to ensure the applicability of biodefence measures, the scope of impact of bioattacks, and mitigation tactics.

Conclusion

Biodefence may seem a distant possibility to the average citizen, and yet biological weapons have been used for centuries. In recent years, the focus on potential biolab leakages, possible bioattacks, and biotechnology solutions has increased discussions on biowarfare and deterrence. Other than nation-states, criminals and terrorists often see biological weapons as a plausible alternative to conventional weapons. This is because biological weapons are relatively cheap to produce, microbes are relatively available, are quickly produced and supplied without being detected.

Biowarfare standards by the Biological Weapons Convention guide signatory nations; those by the International Standards Organisation outline best practices for biolabs and other organisations; and rules set by the Interpol govern non-state actors. However, due to the lack of global and social accountability, none of these standards is infallible. There is a need to incorporate rapid forms of assessment at a global level; this can include incorporating updated detection methods like High Throughput Sequencing at national and international levels, associated with a body that focuses on monitoring and detection like the Joint Assessment Mechanism under the Nuclear Threat Initiative. It is also essential to highlight the power of microbiological forensics while meeting the expectations of law enforcement, the public, policymakers, and the scientific community.

At the global, multilateral, and national levels, the solution to future biological weapons deterrence consists of the same four steps: presenting a united front against bioweapons; enhancing present-day standards to be future-proof by holding regular review cycles to include updating technology and ensuring reduced timelines between such review processes; enhancing assessment methods and monitoring agencies; and reassessing the focus on non-state actors in the landscape of biowarfare.

►► References are available at the source's URL.

[Shravishta Ajaykumar](#) is Associate Fellow at ORF's Centre for Security, Strategy and Technology.

This plant may be a surprise hero in our fight against fungal pathogens

Source: <https://newatlas.com/biology/plant-persephacin-fungal-pathogens/>

Aug 03 – While water lilies are perhaps most famous for starring in French impressionist artist Claude Monet's work, they may also have a molecular secret weapon that could help in our ongoing fight against fungal infections.

After viruses and bacteria, fungus is the most deadly pathogen and, much like bacteria, is adapting fast to be resistant to current medical interventions. While the official numbers show that around 8,000 Americans die from fungal infections each year, it's [likely to be much higher](#), since many cases go undiagnosed and, as an 'opportunistic pathogen,' the microorganism can attack weakened immune systems for complex comorbidities.

The [World Health Organization](#) last year called for urgent attention to be paid to fungal pathogens, which are becoming increasingly prevalent and threatening, spurred on by climate change.

However, there's some good news. Scientists out of the University of Oklahoma (OU) may have found a molecule in a species of water lily or lotus that can fight off fungal infection.

"The molecule we're excited about is called persephacin," said Robert Cichewicz, professor in the Department of Chemistry and Biochemistry, Dodge Family College of Arts and Sciences at OU. "This antifungal discovery appears to work on a broad spectrum of infectious fungi, and it is reasonably non-toxic to human cells, which is a huge deal because many current treatments are toxic to the human body."

Cichewicz, who has been researching fungi for two decades, points out that the strategies plants have developed to withstand attacks might be our best bet at fighting off pathogen threats.

Much like bacteria, pathogenic fungi are fast to adapt and circumvent existing treatment; it's an impressive feat in terms of the evolutionary biology 'arms race,' and the science world is forced to play catchup.





"Fungi are found throughout the botanical world, and plants and fungi often work together," said Cichewicz. "Some of these fungi kill competitors or deter insects from eating the plant."

"We hypothesized that if these plant-dwelling fungi, known as endophytes, could help the plants fight off infections by killing the invading fungi, then these molecules might also be able to protect humans and animals from fungal pathogens," he added. "As it turns out, we were right."

While it may not be a silver bullet, the ability of persephacin to fight off fungal infections is a promising development in a field that's proved frustrating for scientists.

"Antifungal resistance keeps evolving, and this could provide a new alternative," said Cichewicz. "That's why this molecule is so exciting."

●► The research was published in the [Journal of Natural Products](#).

Catapulting corpses?

By Matt Field

Source: <https://thebulletin.org/2023/08/catapulting-corpses-a-famous-case-of-medieval-biological-warfare-probably-never-happened/>

Aug 10 – Poke through the history of biological weapons long enough and you will likely come across a particularly macabre claim. In 1346, the story goes, an army of the Golden Horde—an offshoot of Genghis Khan's Mongol empire—was laying siege to Caffa, a Genoese trading center on the Crimean Peninsula. But as Janibeg, the ruler of the Golden Horde, waited for Caffa to surrender, his fighters began to succumb to a mysterious ailment. "It was as though arrows were raining down from heaven to strike and crush" the Mongols, a notary from the city of Piacenza in present-day Italy wrote. According to the 14th century account, the beleaguered Mongol commanders had one final move: to hurl their plague dead over the fortress walls. In Gabriele de Mussi's narrative, the Genoese inside the fort soon fell ill. They clambered aboard their ships and fled toward Italy—to Genoa, Venice, and other ports, carrying with them the very



plague they sought to escape. “It was as if they had brought evil spirits with them: every city, every settlement, every place was poisoned by the contagious pestilence,” the notary wrote. Known as the Black Death, the bubonic plague crippled Europe when it arrived in 1347, killing [perhaps 50 million people](#). If de Mussi’s tale were true, the Mongol siege had been a devastating biological attack.

The story has certainly stuck.

Since de Mussi’s [work](#) was re-discovered in a university library in Poland in 1842, researchers of weaponry, the plague, and biological warfare have picked up parts of its narrative. Look up “The Black Death” in the Encyclopedia Britannica and [it’s right there](#): “With his forces disintegrating, Janibeg used [trebuchets](#) to catapult plague-infested corpses into the town in an effort to infect his enemies. From [Caffa], Genoese ships carried the epidemic westward...” The medieval allegations are in YouTube and TikTok videos by the History Channel and others, some with millions of views. In the academic literature the anecdote can be found in reputable publications ranging from the *Journal of the American Medical Association* to the CDC’s *Emerging Infectious Diseases*.

The problem is, there’s strong reason to doubt de Mussi.

Jean Pascal Zanders, a veteran scholar of weapons of mass destruction, has been looking into de Mussi’s Caffa claims as part of [a project](#) on [the history](#) of biological and chemical warfare. He argues that the story doesn’t comport with how medieval artillery worked, the geography of Caffa, or medieval warfare practices. “A picture that seems to be plausible on a very basic level actually doesn’t stand up to scrutiny,” Zanders said.

Interpreting de Mussi

By the mid-1800s, Zanders said, scholars had converged on the idea that the plague had originated in the East, somewhere in Asia, and travelled westward toward Europe. The re-discovery of de Mussi’s tale provided them with a back-dated confirmation of the by-then popular theory. The corpse-flinging part was an afterthought.

For decades, some scholars who referenced de Mussi even seemed to miss a critical fact: The notary wasn’t in Caffa during the siege. That didn’t matter much if the point was to cite evidence that the plague originated in Asia, but if the Mongols really catapulted plague-dead into Caffa, de Mussi didn’t see it. Records from his home in Piacenza attest to him being there the whole time, Zanders said.

It wasn’t until the 20th century that scholars started giving the catapulting claim more serious consideration. This, Zanders said, grew out of an interest in military history. One turning point occurred after a British sports and weapons enthusiast, Ralph Payne-Gallwey, wrote about ancient and medieval artillery and devoted a chapter of his 1907 *The Projectile Throwing Engines of the Ancients* to the trebuchet, a catapult-like siege engine used to launch heavy stones at fortresses. In his book, Payne-Gallwey cited numerous medieval references “to the practice of throwing dead horses into a besieged town with a view to causing a pestilence therein.” The work helped establish the idea of trebuchets as powerful weapons commonly used by medieval armies to spread disease.

Subsequently, de Mussi’s assertions about the corpses were included in prestigious publications. Writing in 1966 in the *Journal of the American Medical Association*, Vincent J. Derbes, a medical doctor, [noted](#) Payne-Gallwey’s assessments of trebuchets as well as another anecdote of body launching to conclude that “there is every reason to accept the feasibility of hurling plague-ridden cadavers over the city walls.” In 2002, University of California, Davis professor Mark Wheelis likewise [wrote](#) in *Emerging Infectious Diseases* that the Mongols would have camped one kilometer from Caffa’s walls in order to be safe from the city’s defenders and that the front lines would have been 250 to 300 meters from the walls. He argued that trebuchets could have launched diseased cadavers across that distance and thereby spread the plague. Rats harboring fleas carrying the plague bacterium, *Yersinia Pestis*, conversely, according to Wheelis, could not have travelled that far. The evidence, Wheelis wrote, suggested that “the hurling of plague cadavers might well have occurred as [de Mussi] claimed, and if so, that this biological attack was probably responsible for the transmission of the disease from the besiegers to the besieged.”

The Stockholm International Peace Research Institute (SIPRI) amplified both scholars, first in 1971 and then in [1999](#), when Wheelis wrote a chapter on early biological warfare, which covered, [in part](#), the Caffa siege. “And SIPRI books are like the Bible,” Zanders said, noting their credibility in the field. As the leader of SIPRI’s chemical and biological weapons program at the time, Zanders had a hand in reviewing Wheelis’s chapter, but because of limited data available to him, he said he wasn’t able to challenge the narrative. A handful of publications helped de Mussi’s story become “historical fact,” Zanders said.

A landscape from the 1790s depicting Caffa, now called Feodosia. The old Genoese city and its walls are visible in the distance. Gottfried Heinrich Geißler via Wikimedia Commons.

Trebuchets and the geography of Caffa

Trebuchets were the culmination of medieval siege engine design, reigning as the most powerful artillery for centuries until cannons began to replace them in the late Middle Ages. Derbes wrote that from



experiments and other sources, Payne-Gallwey had determined the largest trebuchets could throw an object weighing 300 pounds a distance of 300 yards. According to de Mussi's account, catapults were used to fling bodies over the walls at Caffa, but both Derbes and Wheelis implied that these would have been trebuchets, the best of which could theoretically launch a human payload.

But there are several problems with accepting that the Mongols launched cadavers with trebuchets.

For one, no trebuchet has ever been found, Zanders said. What's left to history are historical references or drawings that lack perspective. Following in the footsteps of Payne-Gallwey and his experiments, researchers and trebuchet fans on YouTube have re-imagined what the weapons must have looked like, constructing their own. But these are modern re-creations that may not accurately reflect medieval capabilities.

Even if trebuchets had a range of 300 yards, as Payne-Gallwey concluded, Caffa would have been suboptimal terrain for them, Zanders argues. The hilly topography would have made it challenging to launch non-aerodynamic bodies up hills and over walls. The Mongols would have had to place their trebuchets close to the fortress, where they would have been vulnerable to defensive fire. And Zanders said people were living outside of the city walls, meaning there would have been opportunities for the plague to spread between the besiegers and the besieged.

The most powerful trebuchets weighed tens of tons. Dismantling and moving them would have been a massive logistical operation. Across most terrains, Zanders said, the weapons were "too huge to transport" and would have been built on site using local wood. Zanders couldn't find reference in his research to there being suitable trees around Caffa with which to build trebuchets. "One thing that stood out was the absence of trees in descriptions," he said. "Many shrubs and other things and low trees, but definitely nothing like oak trees—solid wood to build these types of machines."

Not that the Mongols even used the type of trebuchet that could launch bodies, those operated by dropping a heavy counterweight, such as container full of sand or rocks, to swing a launching arm. According to Zanders's research, the Mongols instead used mangonel trebuchets that operated by human labor. "The Mongols at the time, the Golden Horde, used Chinese trebuchet technology, which were mangonels," Zanders said. "So the wrong type of engines." These smaller trebuchets could fire a 33-pound projectile close to 400 feet, according to Zanders.

[A video with 2.3 million views on the Smithsonian Institution's YouTube channel shows a reconstructed trebuchet in action. Smithsonian Channel/YouTube – click on photo](#)



Medieval warfare

The Middle Ages have a gruesome and violent reputation; think Vlad the Impaler, Ivan the Terrible, or William the Conqueror. And Zanders believes part of what makes de Mussi's tale of the Siege of Caffa believable are arguments about how common it was to catapult dead bodies or large animals. Indeed, the historical record includes several instances of this sort of attack. But through analyzing a variety of sources, Zanders undercuts many of the claims.

"We see that the chronicler was never a contemporary of the described events," Zanders said during one recent presentation on his research. "The narrative emerged decades, if not longer, after the reported incidents. Different narratives can exist of the same event. However, the most intriguing aspect is that in all of those narratives, we only will see or read about a single incident of catapulting cadavers during a war or a whole campaign. There is never a suggestion of a wider practice."

For example, according to one history of the Hundred Years' War—a multi-generational conflict between England and France between 1337 to 1453—as French forces laid siege to a castle in Thun l'Eveque, France, they launched horses at their enemies, causing a stench that allegedly drove the castle's defenders to consider surrender. Jean Froissart, a medieval writer, recounted the story in his book *Les Chroniques*, lending credibility to the idea that trebuchets could launch dead animals (or even humans) at a besieged fortress. But Zanders looked into the claim and found several reasons to doubt its veracity. Froissart, born in the 1330s, would have been a young child at the time of the siege in 1340. Parts of his narrative appear to be copied from another chronicler, Jean le Bel, who witnessed the conflagration but didn't mention siege engines or animal projectiles. Also, one version of Froissart's tale that Zanders analyzed doesn't contain a description of launching horses. Likewise, Zanders was not able to corroborate the tale of a 1422 siege at Karlštejn Castle in the present-day Czech Republic. Again, the chronicler, Antoine de Varillas, seemed to be the only person to describe the hurling of war dead.



How de Mussi's claim took hold

The plague is believed to have originated in Central Asia and trade in Crimea may have played a role in spreading it to Europe. But that doesn't mean that the Mongol siege of Caffa, whether it involved cadaver launching or not, was responsible. Wheelis, who found de Mussi's story to be plausible, nevertheless wrote that the "[p]lague appears to have been spread in a stepwise fashion, on many ships rather than on a few."

The way de Mussi crafted his tale may have been akin to a game of medieval telephone. The notary wasn't in Caffa, but Piacenza, near Genoa, where he likely would have come in contact with returning traders. He might then have worked the details he heard from them into a second-hand narrative comports with his religious convictions about righteous Christians and the contemporary theory of disease transmission, namely that foul air or miasma caused sickness. Zanders theorizes that de Mussi at that point may have settled on a reasonable synthesis: God struck down the Mongols and miasma, brought on by the catapulted bodies, spread the plague among the Genoese. "He is a firsthand chronicler of what other people were telling him, but the construction had to fit with his conception of the world. And he got confused," Zanders said. "And that's probably what has happened."

And the game of telephone appears to be going on still, with one researcher or writer citing a previous one, without first figuring out if de Mussi's claim is true. "Anybody writing something on biological weapons," Zanders said, "particularly people starting out in the field or writing an essay for school or university, they will always mention it. And it's always like one or two sentences they're going to use; nobody develops the issue further."

Seth Carus, a scholar of biological and chemical warfare who was a professor at the National Defense University, supports Zanders's analysis. "As Zanders has illustrated, there is reason to doubt the claim that biological warfare was waged at Caffa, yet the story is repeated as though it has been proven beyond a shadow of a doubt," he told the *Bulletin*. Many biosecurity experts, he said, probably believe the oft-told tale, despite a lack of evidence. That can have an impact beyond the community of plague or military history buffs. "My fear," Carus said, "is that repeating false claims of past biological warfare normalizes the idea of intentional use of disease, making the actual use of biological weapons more likely."

[Matt Field](#) is editor, biosecurity at the *Bulletin of the Atomic Scientists*. Before joining the *Bulletin*, he covered the White House, Congress, and presidential campaigns as a news producer for Japanese public television. He has also reported for print outlets in the Midwest and on the East Coast. He holds a master's degree in journalism from Northwestern University.

Poxvirus Therapy: Existing Drugs May Offer New, More Durable Approach

Source: <https://www.genengnews.com/topics/infectious-diseases/existing-drugs-may-offer-new-more-durable-approach-to-poxvirus-therapy/>

Aug 09 – Scientists in the U.K. have discovered how poxviruses such as the monkeypox virus (MPXV) and variola viruses evade host cell defenses by exploiting a protein, cyclophilin A (CypA), that puts the brakes on a natural cellular antiviral protein called human tripartite motif protein 5α (TRIM5α), which then allows the pathogens to replicate and spread. Results from the study, headed by a team at the University of Oxford, the University of Cambridge, and the Pirbright Institute, point to a new therapeutic approach that may be more durable than current treatments, and which could feasibly use existing immunosuppressants such as cyclosporin A (CsA) and other antiviral drugs that target cyclophilin A.

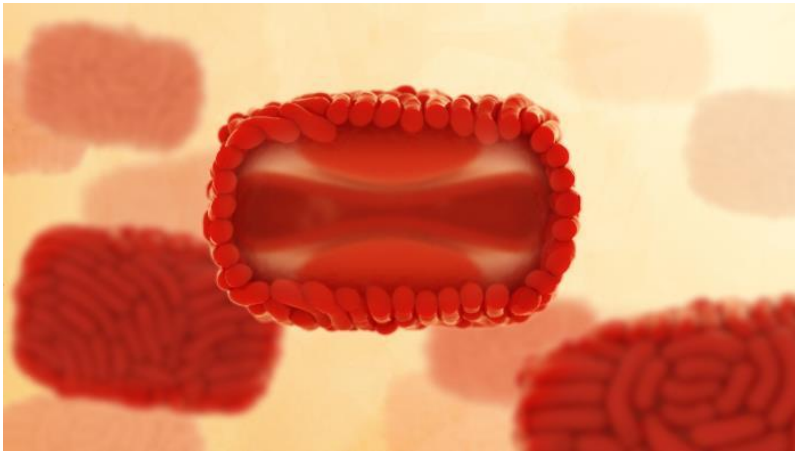
Initial experiments reported by the researchers suggested that these drugs can restrict replication and spread of poxviruses. They suggest that this approach to treatment, whereby the drug does not directly target the virus, could make it more difficult for poxviruses to evolve drug resistance. And because the protein-hijacking mechanism is the same across many poxviruses, cyclophilin A-targeting drugs could be effective in treating a range of diseases.

"The drugs we identified may be more durable than the current treatment for monkeypox—and we expect will also be effective against a range of other poxviruses including the one that causes smallpox," said research lead Geoffrey L. Smith, FRS FMedSci FRSB, who conducted the work in the department of pathology at the University of Cambridge, the Dunn School of Pathology, University of Oxford, and the Pirbright Institute. Smith and colleagues reported on their findings in *Nature*, in a paper titled, "[TRIM5α restricts poxviruses and is antagonized by CypA and the viral protein C6](#)," in which they concluded that their results "warrant testing of CsA derivatives against orthopoxviruses, including monkeypox and variola."

Smallpox has been eradicated as a disease since 1979, but the virus that causes it, variola, is still being held in two high-security labs—one in the United States and one in Russia. The threat of variola virus being used in bioterrorism has led to a drug, tecovirimat, being licensed to treat smallpox. Vaccinia virus (VACV), the live vaccine used to eradicate smallpox, is also currently being used to immunize at-risk populations against monkeypox virus, the cause of monkeypox (mpox), the team explained. "VACV, cowpox virus (CPXV), MPXV, camelpox virus (CMLV),



and variola virus (VARV), the cause of smallpox, are all orthopoxviruses and are immunologically cross-protective.” Tecovirimat has been used to treat severe cases of mpox over the last year, but this has resulted in the emergence of multiple drug-resistant strains of the monkeypox virus.



This illustration depicts a number of mpox virions. The foreground particle is shown in a cut-away view, revealing its interior dumbbell-shaped core, containing the DNA of the virus, and lateral bodies, which are surrounded by an exterior coat of surface filaments. [CDC/ Cynthia Goldsmith. Illustrator: Stephanie Rossow (CTR)]

Once a poxvirus infects a host cell it has to defend itself from attack by cellular proteins that would restrict virus replication and spread. The newly reported research started with the simple observation that vaccinia virus infection causes a reduction in the level of TRIM5 α in human cells. To find out why, the team engineered human cells to lack TRIM5 α and found that in these

cells the virus replicated and spread better, indicating that TRIM5 α has anti-viral activity. The team next identified the vaccinia virus protein that TRIM5 α targets. They also discovered that the virus has two defenses against attack by TRIM5 α . First, it exploits another cellular protein, cyclophilin A, to block the antiviral activity of TRIM5 α , and second, it makes a protein, C6, that induces destruction of TRIM5 α . “... the antiviral activity of TRIM5 α is countered by the proviral activity of CypA, which in turn is antagonized by CsA and derivatives that prevent the binding of CypA to its viral target, the poxvirus capsid protein L3,” the team stated. L3 is highly conserved in orthopoxviruses, and the team showed that L3 from VACV, MPXV, and VARV binds to human CypA and human TRIM5 α , and the former interaction is prevented by CsA and derivatives. Moreover, they wrote, “Like L3, C6 is highly conserved in orthopoxviruses, and C6 orthologues from VACV, CPXV, CMLV, MPXV, and VARV all bind to human TRIM5 α and induce its degradation, despite most of these proteins deriving from viruses that are not endemic in humans.” Existing drugs target cyclophilin A, and when the team tested a series of these drugs against a range of poxviruses, including monkeypox, they found that the drugs exhibited antiviral effects, effectively by making the virus more sensitive to TRIM5 α . “The role of CypA in antagonizing the antiviral activity of TRIM5 α provides a route to antiviral drug development for orthopoxviruses such as MPXV and VARV,” the team noted. “CsA and the non-immunosuppressive derivatives alisporivir and NIM811, interrupt the interaction of CypA and L3, and thereby reverse the proviral activity of CypA and enhance TRIM5 α -mediated restriction. These compounds are therefore antiviral in the presence of CypA and TRIM5 α and can restrict the replication and spread of orthopoxviruses.” “There are various drugs that target cyclophilin A, and because many of them have gone through clinical trials we wouldn’t be starting from scratch but repurposing existing drugs, which is much quicker,” said Smith. “Our results were completely unexpected. We started the research because we’re interested in understanding the basic science of how poxviruses evade host defenses and we had absolutely no idea this might lead to drugs to treat monkeypox virus and other poxviruses. The authors further noted that in contrast with tecovirimat, which does not block replication and needs a functional immune system to remove virus-infected cells alongside drug treatment, CsA, alisporivir, and NIM811 hinder virus replication by targeting a cellular protein, “making the emergence of drug resistance difficult.” Both of the non-immunosuppressive derivatives have also progressed in development to Phase II clinical trials, and so there is also an indication of their safety. “Therefore, clinical testing of these drugs against MPXV is warranted,” the team stated.

Long COVID may be caused by damage to cells' energy generators

Source: <https://newatlas.com/medical/long-covid-caused-by-damage-to-mitochondria-genes/>

Aug 11 – A new study has found that SARS-CoV-2, the virus that causes COVID-19, damages the genes of the mitochondria, the cell’s energy generators, causing dysfunction in organs other than the lungs that continues after the lungs have recovered. The finding may explain why some people suffer from long COVID.

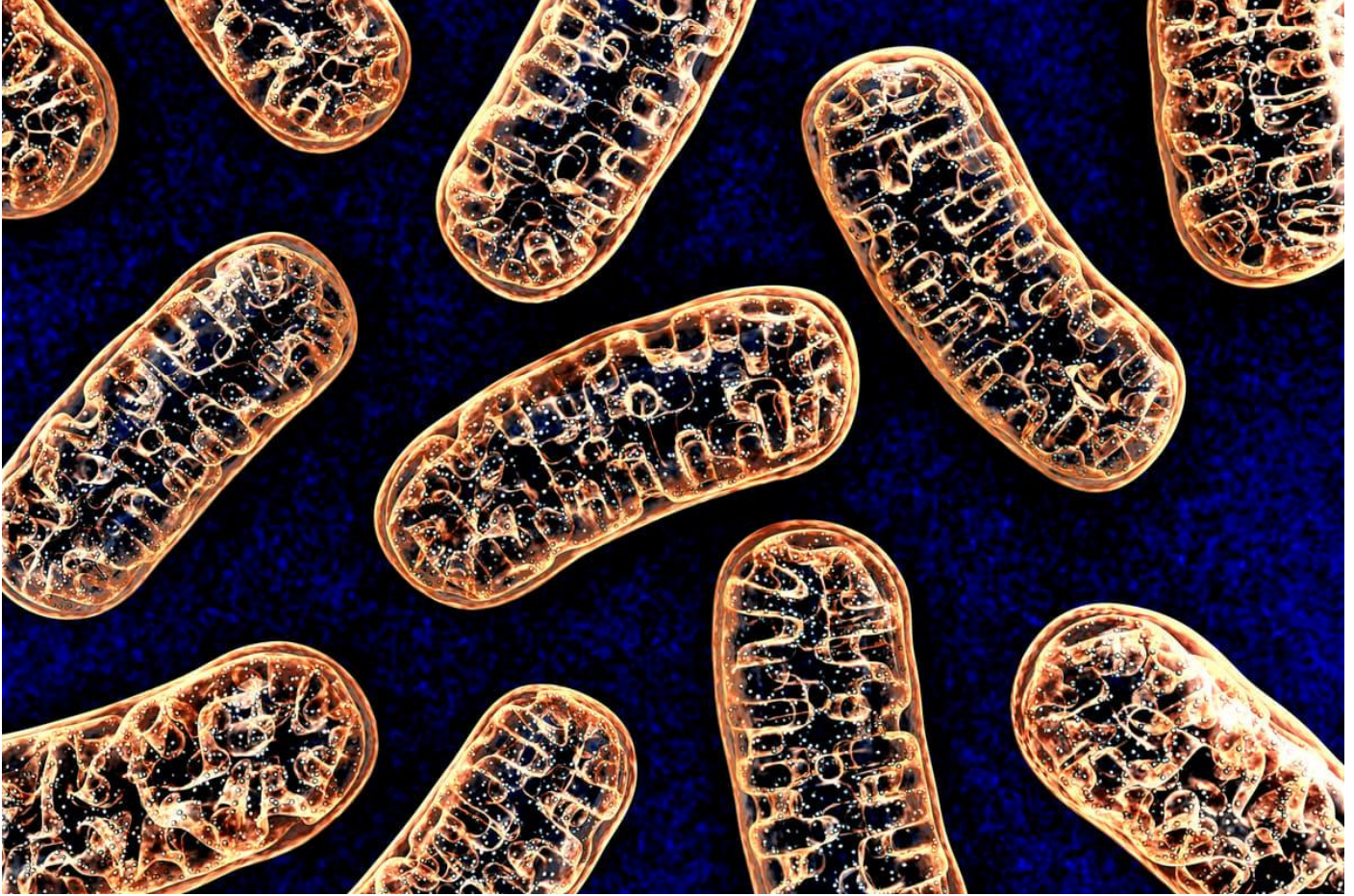
Since the COVID-19 pandemic first hit, researchers have been trying to figure out why, compared to other coronaviruses, SARS-CoV-2 produces such negative long-term effects.

Long COVID is the condition where symptoms persist for weeks, months, and even years after infection with SARS-Cov-2. Chronic pain, brain fog, shortness of breath, chest pain and intense fatigue – all of



which can be debilitating – are common long COVID symptoms. Now, a study led by researchers at the Children’s Hospital of Philadelphia (CHOP) and the COVID-19 International Research Team (COV-IRT) may have provided some answers. And it has to do with mitochondria, the powerhouses of cells.

Every cell has mitochondria, and each mitochondrion contains its own DNA (mitochondrial DNA or mtDNA). mtDNA contains 37



genes, 13 related to making enzymes for energy production, with the remaining genes providing instructions for making molecules called transfer RNA (tRNA) and ribosomal RNA (rRNA), the chemical cousins of DNA that help assemble amino acids into functioning proteins.

To analyze how SARS-CoV-2 impacts mitochondria, the researchers studied their gene expression using a combination of nasopharyngeal (nose and throat) and autopsy tissues from affected patients and animal models.

“The tissue samples from human patients allowed us to look at how mitochondrial gene expression was affected at the onset and end of disease progression, while animal models allowed us to fill in the blanks and look at the progression of gene expression differences over time,” said Joseph Guarnieri, the study’s lead author.

They found that, in autopsy tissue, mitochondrial gene expression in the lungs had recovered, but mitochondrial function in the heart, kidneys and liver remained suppressed. In animal models where the virus had peaked in the lungs, the researchers found that mitochondrial gene expression was suppressed in the cerebellum even though SARS-CoV-2 was not seen in the brain. Additionally, animal models revealed that during the mid-phase of the infection, lung mitochondrial function was beginning to recover.

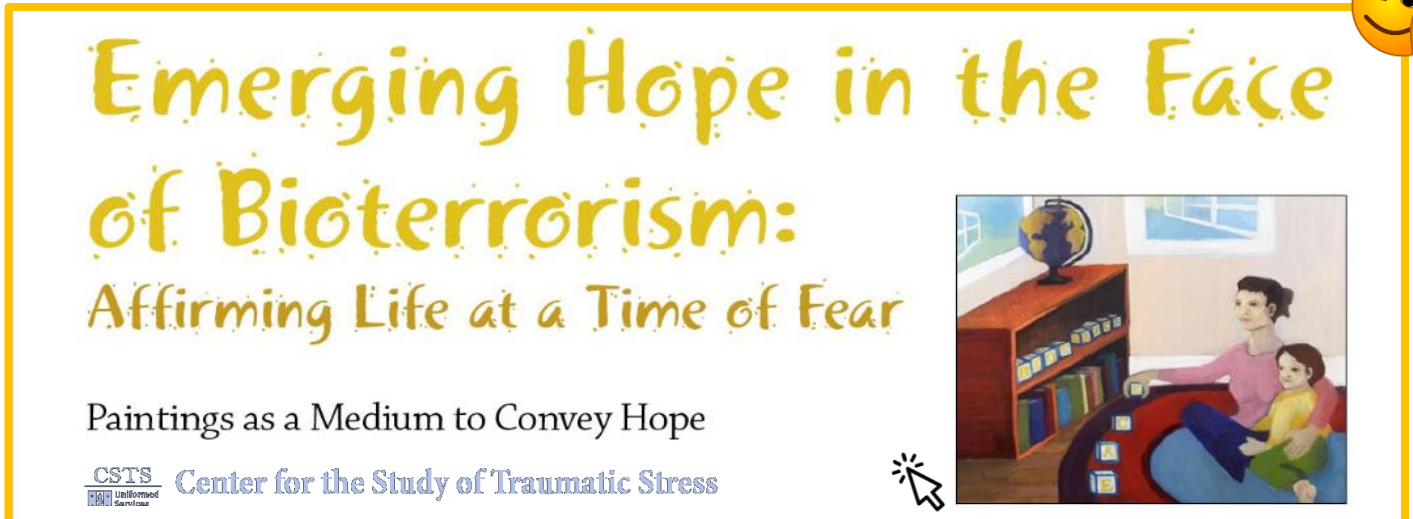
The findings suggest that while SARS-CoV-2 infection initially involves the lungs, over time, mitochondrial gene expression is restored there but remains impaired in other organs, the researchers say. They also say that the findings support the hypothesis that individual differences in mitochondrial function may explain why the severity of COVID-19 infections differs between people.

“This study provides us with strong evidence that we need to stop looking at COVID-19 as strictly an upper respiratory disease and start viewing it as a systematic disorder that impacts multiple organs,” said co-author Douglas Wallace. “The continued dysfunction we observed in organs other than the lungs suggests that mitochondrial dysfunction could be causing long-term damage to the internal organs of these patients.” The study did identify a potential therapeutic target, microRNA 2392 (miR-2392), which was shown to regulate mitochondrial function in human tissue




samples analyzed by the researchers. “The microRNA was upregulated in the blood of patients infected by SARS-CoV-2, which is not something we normally would expect to see,” said Afshin Beheshti, another of the study’s co-authors. “Neutralizing this microRNA might be able to impede the replication of the virus, providing an additional therapeutic option for patients who are at risk for more serious complications related to the disease.”

●► The study was published in the journal [Science Translational Medicine](#).



Emerging Hope in the Face of Bioterrorism:
Affirming Life at a Time of Fear

Paintings as a Medium to Convey Hope

 **Center for the Study of Traumatic Stress**

Risk analysis in suicide bioterrorism

By Jason D Söderblom

Source: <https://rusi.org/publication/risk-analysis-suicide-bioterrorism>

Governmental responses to bioterrorism seem limited to searching for biological agents at airports and shipping container entry points, and promoting bio-hazard awareness at mail handling facilities. In the wake of successful suicide terrorist attacks in Israel and Iraq, and given the success of suicide terrorist hijacking, a logical extension of the suicide attack phenomenon is to expect self-contaminated suicide terrorists to present a bioterrorist threat.

Defining the bioterror threat

Biological terrorism can be loosely categorised based on the agent used. First are biological toxins — sometimes referred to as ‘bio-toxins’ — poisons which are produced by living organisms. Examples include botulinum, staphylococcus enterotoxin, aflatoxin, and shigella toxin. A bio-toxin consists of an amino-acid chain of several hundred peptides to several thousand proteins. Some organic compounds, which are not peptides, can also be classed as toxins, however.

Gorka and Sullivan make the point that, in nature, bacteria, fungi, algae, plants, and animals produce a substantial range of toxins with a potential to be more lethal than the greater magnitude of nerve agents.¹ Moreover, type-A botulinum toxin (BTX), with a mean lethal dose estimated to be as low as a few tenths of a microgram, has been described as “the most lethal substance known”.² BTX could surpass the lethality of a nuclear explosion in terms of the potential number of casualties.³

The second category is the ‘virus threat’. Examples include smallpox, influenza, dengue fever, yellow fever, Rift Valley fever, and haemorrhagic fevers like Lassa, Ebola, and Marburg. Smallpox spreads directly from person to person, primarily by droplet nuclei expelled from the oropharynx (the space beneath the mouth cavity) of the infected person, or could be disseminated by aerosol spray. Natural infection occurs following implantation of the virus on the oropharyngeal or respiratory mucosa. Exposure to smallpox could therefore occur through inhalation of an aerosol or exposure to a ‘suicide carrier’. Smallpox symptoms include fever, vomiting, headache, and backache; and after two to four days, skin lesions appear.⁴ Smallpox is thought to be fatal in approximately 30% of people who have never been vaccinated. This risk is further exacerbated by the fact that medical practitioners can easily mistake smallpox for chicken pox.⁵ Persons with smallpox are not infectious during the incubation period; they are most infectious during the first week of severe illness, for this is when the



largest amount of virus is present in saliva. This non-contagious period explains the effectiveness of the containment of cases during the global eradication programme. Importantly, post-exposure vaccination can prevent smallpox even after exposure to the virus. In the 20th century, naturally occurring smallpox killed approximately 300 million people. 6

The third category of bio-threat is 'bacteria', which includes anthrax, plague, cholera, brucellosis, typhoid fever and rickettsial agents such as typhus, Rocky Mountain spotted fever and Q-fever. Brucellosis (of which Crimean fever is a form) is delivered through inhalation of aerosols or by ingestion via sabotage of the food supply. 7 Cholera is delivered by ingesting contaminated food or water. Brucellosis is delivered by ingestion, inhalation of aerosols, or sabotage of the food supply. Glanders and melioidosis are delivered by inhalation of aerosols. Tularaemia is delivered through inhalation or ingestion of aerosols or contact with a tick or other tularemia-infected arthropod or animal. Q-Fever is delivered by inhalation of aerosol or ingestion.

The effectiveness of the bioterror threat

Problems with delivering a bio-attack are the acknowledged Achilles' heel in biological warfare. 8 Wind-patterns, air temperature, rain, and the presence of ultraviolet light can affect both the mortality rate from a bioterror attack and the life span of the bio-organism. 9 Unlike conventional warfare, a reliance on the 'luck and favour of the natural elements' is a logistical problem for both the terrorist in ensuring maximum casualties, and the victim state in guarding against a bioterror attack. Whilst a victim state can generally regulate and monitor the use of crop-dusters over open-roofed stadiums, it remains impossible to regulate the wind blowing across the top of the stadium. Wind carrying a bio-agent released two kilometers away is exceptionally difficult to take counter-measures against, yet this uncertainty cuts both ways, for if the wind-speed dies down, the attack could be a non-event, and the potential for containment of the bio-weapon is greatly improved. Thus bioterrorism may appear fraught with a complex problem surrounding the question of how to effectively deliver the attack. Yet this uncertainty would be greatly reduced through using suicide terrorists to deliver the biological agent.

It's all in the delivery: suicide bioterrorism

It remains effectively impossible in a democracy to prevent a suicide bioterrorist from entering a public space, such as an airport, stadium, school, grocery store, or shopping mall and spreading a bio-agent before the symptoms become apparent. A scenario to demonstrate my case is illustrated below. It will comprise a bacteria threat (pneumonic plague) as an initiator piggybacked with a virus threat (smallpox), and will also entail the targeting of a democracy, and the use of suicide terrorists to deliver the agents.

Scenario: plague (bubonic, pneumonic, septicemic)

Currently there is no widely available 'rapid' confirmation diagnosis test to identify plague. 10 Confirmatory tests can be done through blood and sputum (if pneumonic), bubo aspirates (if bubonic), and central spinal fluid (if meningitis occurs). Antibiotics are an effective treatment, but waiting for lab results before starting the treatment is, according to Pamela Weintraub, effectively a "death sentence". 11 Bubonic plague is contracted through the bite of a flea or through handling infected animals. Thus the bubonic plague is not very practical for suicide bioterrorism, whereas pneumonic plague is widely considered to be a more practical option. Yet for suicide bioterrorism, this remains somewhat impractical as those suffering from pneumonic plague are visibly sick within one to six days and thus can be quickly identified and removed from the community. This is not to suggest that forms of the plague would not cause havoc and a considerable number of deaths. A suicide pneumonic plague terrorist would not look out of place in a hospital ward or a local GP's surgery. The suicide pneumonic plague carrier will not be seeking to be positively diagnosed with the plague, but will be relying on the 'flu-like symptoms' to remain undiagnosed as pneumonic plague. It is often assumed that the 'visible sickness' of the plague-infected terrorist would make plague-based bioterrorism easily detected, but pneumonic plague would be an effective tool in a two-tier (piggyback) terrorist attack.

Terrorists' ability to acquire plague

Pamela Weintraub states: "Experts in bioterrorism consider the plague a serious threat. Not only is it highly fatal and contagious, it is also stored in microbe banks around the world." 12 In the 1950s and 1960s there were many institutions and thousands of scientists working with plague. It thus remains probable that this expertise could be purchased at any time, given the level of poverty in countries of the former Soviet Bloc. 13 It is feasible that terrorist networks could acquire plague with minimal effort, and if the suicide terrorist remains undetected around the target he would succeed in causing havoc even if aerosolising equipment could not be acquired.

In May 1995, Larry Wayne Harris, a member of the anti-government 'Christian Patriots' and a former member of Aryan Nation, a neo-Nazi organisation, ordered samples of yersinia pestis, the causative agent of the plague, from the American Type Culture Collection. 14 Harris, a microbiologist, said he feared an "imminent invasion of Iraqi super-germ-carrying mice", and purported to be researching a "plague



antidote". The US Centers for Disease Control and Prevention has since tightened up requirements for shipping special disease agents and toxins, such as bubonic plague, tularemia and brucellosis. Yet this lax security in the U.S before 1995, and the lax security that continues today in the former USSR, show that the possibility of terrorists acquiring the plague is real. 15

Terrorists' ability to acquire smallpox

Intelligence agencies and international relations scholars are concerned that Russian researchers of the former Soviet Biopreparat, of whom many have been unemployed since the 1990s, could be tempted to smuggle and sell smallpox to those terrorist groups with the financial resources and microbiological expertise to use it, or further weaponise it. Marvin Cetron, president of Forecasting International Ltd, a risk assessment company working with both the US Department of Defense and the FBI, has stated, "I think the chance is about 80% of terrorists obtaining smallpox." 16

States' ability to counter and contain

To use Australia as an example, routine vaccination against smallpox was introduced in Australia in 1917 because of an epidemic in New South Wales. However, by the 1950s in most parts of Australia vaccination was only mandatory people for travelling overseas or for medical students, nurses, and others at potentially greater risk of exposure. And vaccination was no longer required for any Australian, following global eradication of smallpox in the 1970s. The World Health Organization (WHO) reported that the last smallpox death occurred in 1977 and announced its worldwide eradication in 1979. As a result, most countries ceased vaccination against smallpox decades ago.

Testing the scenario

Two 'suicide pneumonic plague infected terrorists' strategically target numerous doctors' offices (in winter) to obtain a medical certificate to explain their absence from work — they could even leave before seeing the physician. They blend in with people suffering flu symptoms in the waiting room, but they are already effectively spreading the pneumonic plague amongst staff and patients.

A terrorist organisation claims responsibility for the plague outbreak. Citizens are too terrified to seek medical attention, as they are now aware that medical facilities have been targeted. This is when the second stage of the bioterror attack occurs. Smallpox is delivered to the target city through either aerosolised delivery or by means of another infected set of suicide terrorists passing on smallpox through exhaled droplets.

Mass terror is created by the paradox that smallpox needs to be contained and treated, yet the mass plague (and smallpox) infection of patients and staff at hospitals causes citizens to stay away from medical facilities. A radio talk show host ponders aloud whether by attending the doctor to get checked for the flu, or vaccinated for smallpox, you may acquire both the pneumonic plague and smallpox before the vaccination takes effect.

Large segments of the community avoid medical treatment. The strain placed on the infrastructure of the city brings it to a halt, aircraft do not arrive or leave, police at roadblocks turn back fleeing residents, and the 'terror' caused by the bioterror attack is unmatched by any previously experienced health catastrophe. The economy is brought to a standstill, and the bioterrorists now have political influence as they have demonstrated their capacity to inflict terror.

Worse still, a rumour circulates that the smallpox is a weaponised variant from the former USSR for which there is no vaccine. Thus the containment of infected people proves to be impossible, even though WHO vaccines arrive quickly. People are too frightened to leave their homes and there are simply not enough respirator masks to go around.

Risk analysts are fully aware that policymakers respond quickly to visible crises, even if the baseline rate of danger has not altered. 17 In the event of a bioterror attack, schools, hospitals, police, government agencies and the public will need to engage in unprecedented levels of trust and co-operation. Strict policies will be needed to mitigate and contain the crisis. Once a serious bioterror attack has occurred, the existing infrastructure of society would not easily cope with the scenario detailed in this article, and containment would most probably fail.

This proposed scenario is logically feasible, and has a potential to inflict greater death and terror than the 'Dark Winter' bioterrorism smallpox exercise conducted in 2003, given the piggyback strategy employed. 18 Worse still, the scenario introduces smallpox of a weaponised variant; this variant may render the existing WHO smallpox vaccine ineffective, no matter how quickly it is administered.

Jason D Söderblom is an intelligence analyst for the Terrorism Intelligence Centre, in Canberra, Australia, and is also a staff member at the Faculty of Law at the Australian National University (ANU) where he researches and writes on international law, public law and public policy.



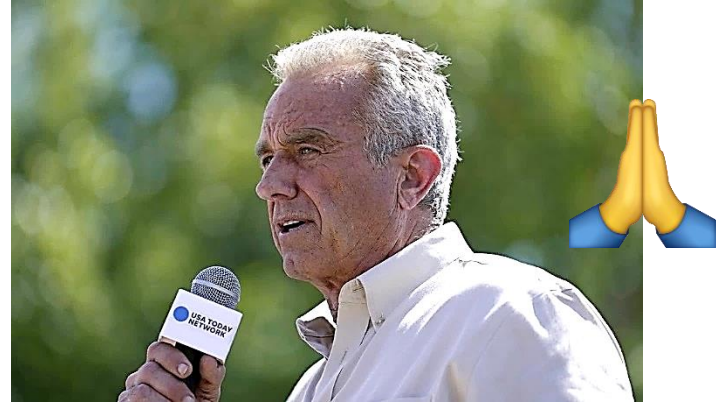
US biolabs in Ukraine created as part of bioweapons programs — Kennedy Jr.

Source: <https://tass.com/defense/1660431>

Aug 15 – The US has created biological laboratories in Ukraine within the framework of Pentagon programs on developing biological weapons, US presidential candidate Robert Kennedy Jr. told political commentator Tucker Carlson.

"We have biolabs in Ukraine because we are developing bioweapons," Kennedy Jr. said. "Those bioweapons are using all kinds of new synthetic biology and CRISPR technology and genetic engineering techniques that were not available to a previous generation," he said in an interview with Carlson posted on the X social network (formerly known as Twitter).

"When the Patriot Act reopened the biolabs arms race in 2001, the Pentagon began putting a lot of money into bioweapons," Kennedy Jr. added. "But they were nervous at that time because if you violate the Geneva Convention, it's a hanging offense," he explained. "So they were nervous about actually going full force into bioweapons development. So they transferred the authority for biosecurity to one agency in the HHS [the US Department of Health and Human Services]," the politician added. "But now, when you do bioweapons development, every bioweapon, it needs vaccine, so you develop them side by side because in a 100% of the cases when you deploy a bioweapon, there's blowback. Your side also gets sick," he concluded.



In mid-April, a Russian parliamentary commission presented its final report on the investigation into the activities of US-run biolabs in Ukraine. According to the document, the Pentagon's military biological program had grown large in scale, being implemented under the guise of anti-terrorist projects and activities permitted by the Biological Weapons Convention.

The commission also pointed out that the activities of all the US-controlled laboratories involved Pentagon experts. However, their work is secret and government agencies in the host countries only have access to secondary research.

Natural or Not? Identifying Genetically Engineered Organisms

By Aliyah Kovner

Source: <https://www.homelandsecuritynewswire.com/dr20230815-natural-or-not-identifying-genetically-engineered-organisms>

Aug 15 – Ever since gene editing became feasible, researchers and health officials have sought tools that can quickly and reliably distinguish genetically modified organisms from those that are naturally occurring. Though scientists can make these determinations after careful genetic analysis, the research and national security communities have shared a longstanding unmet need for a streamlined screening tool. Following the emergence of SARS-CoV-2, the world at large became aware of this need.

Now, such tools are being built.

A suite of techniques – one lab-based platform and four computational DNA sequence analysis models – was developed and refined over the course of a six-year program funded by the United States Intelligence Advanced Research Projects Activity (IARPA). These approaches have the potential to dramatically shift current screening capabilities for detecting engineered organisms.

Susan Celniker's team at Lawrence Berkeley National Laboratory (Berkeley Lab) was chosen to lead the testing and evaluation phase of the program, called Finding Engineering-Linked Indicators, or FELIX. She and her colleagues designed and produced increasingly challenging biological samples and assessed how well the tools made by participating academic and industry groups performed.

"What the FELIX program revealed in its initial months was that the capability to efficiently identify modified organisms in the environment does not exist. And so, the program really started at the foundations to developing first-in-class capabilities to identify modified organisms," said Ben Brown, a staff scientist computational biologist in Berkeley Lab's Biosciences Area, who co-led the project design with Celniker. "It's a very important program in that it created the tools to fill an important segment of our national security space."

Testing the Testers

To evaluate the work accomplished by its research teams, IARPA leveraged national laboratories to perform Test and Evaluation. This process ensures capabilities and tools that are developed under



programs like FELIX can achieve the same results as reported by the researchers and are meeting program metrics, enabling evaluation of progress within the program. To ensure the tests would be as useful as possible for national security applications, the teams evaluated their performance with samples based on current and potential real-world scenarios.

In total, the scientists at Berkeley Lab, Pacific Northwest National Laboratory, and the United States Department of Agriculture produced nearly 200 unique sample organisms with innocuous modifications ranging from large DNA sequence deletions or insertions all the way down to very subtle single nucleotide alterations made using CRISPR. Each testing group was given samples containing altered organisms as well as unmodified control samples containing non-modified organisms – known as “wild type” – that had never been fully sequenced before, so the genomes were not available in any database for comparison. The samples included virus particles and cells from bacteria, mammals, and fungi. These blinded samples represented potential human pathogens, such as HIV and *E. coli*, plant-infecting pathogens, and engineered complex species. To ensure health and security for participants, all of the microbial or viral samples created for testing were noninfectious and all were controlled under strict biosafety procedures.

The Testing and Evaluation portion of FELIX was divided into four phases, where each subsequent phase had more difficult samples. Groups with candidate tests were eliminated along the way if their technique did not perform well enough.

In the beginning, testing groups received purified samples with only one organism each, and they got multiples of every sample to determine whether the testing technique generated reproducible results. At the end, the testers received mixed samples designed to approximate real-world testing conditions. “For the final round, we gave them mixtures of up to 10 wild type and engineered organisms with different mutations in them to mimic what a soil sample might look like. And we actually did give them two soil samples as well as actual microbiome samples from a cow digestive tract and a mouse digestive tract,” said Celniker. “So they got very complex samples that were really challenging.”

Celniker and Brown further challenged the testing groups by designing samples that incorporated naturally occurring genetic oddities. For example, they presented samples containing bacteria that had acquired new genes by swapping plasmids – circular pieces of DNA that are separate from the cell’s main genome – with other species of microbes. Gene acquisition from plasmids is very common in single-celled organisms, and it is through this mechanism that strains of bacteria can very quickly gain new traits such as antibiotic resistance.

They also threw in some hybridized influenza samples that could not have formed naturally (despite the virus’s penchant for genetic cross-over) because the strains never circulated at the same time or on the same continents. Real-world gene scrambling events like these make it difficult to differentiate between natural and synthetic gene additions, but being able to do so is an essential capability of a modified organism detection tool.

To that end, the IARPA program leaders set an ambitious goal for the testing technologies of 99% specificity (no more than 1% of wild types misidentified as modified) and 90% sensitivity (no more than 10% of tests could misidentify a modified organism as wild type). The four techniques that passed through to the end of phase four testing and will be useful for identifying biological threats were a lab-based test from the company Draper and computational models from Raytheon, Ginkgo Bioworks, and Noblis. These techniques were shown to be excellent at identifying wild type organisms, and a Berkeley Lab-developed ensemble of the computational models achieved 99% specificity.

The sensitivity in identifying engineered organisms of individual models was between 55%-70%. But the ensemble was able to achieve approximately 72% sensitivity under cross validation, which occurred when it was tested on new sequence datasets. Overall performance of individual models and the ensemble demonstrated considerable improvement over existing state-of-the-art capabilities.

A New Resource

One reason why it’s so hard to tell natural and engineered organisms apart is that scientists around the world use many different databases and programs to review and store genome sequence data. And on top of that, people use different names and terms to describe genes and predict their functions based on the sequences – a process called annotation. So, despite the fact that more and more species have had their genomes sequenced, the data isn’t necessarily easy to use.

To remedy this issue, Celniker recruited her Biosciences Area colleague Chris Mungall, a computer staff scientist, to lead the development of an open-access software program and database. The result was Synbio Schema, which catalogs the annotated genomes of national security-relevant engineered and wild type organisms using standardized language. Each sample that Celniker’s team created for the testers was also added to the new database and annotated with the standardized language, providing an easy-to-use resource for future researchers.

“This is the first curated database and common language for engineered vs non-engineered organisms, and they really had to build the airplane in flight because nothing like it existed previously, and the program would have been crippled without it,” Brown said.



“The real problem arises when multiple research groups are trying to share and compare results,” explained Mark Miller, a software developer in Mungall’s group. “If there are any internal inconsistencies or other issues within a team’s database, or if there are structural or nomenclature differences between the teams’ databases, then nobody can tell whether one team’s data agrees with the other teams.” This forces scientists to tediously review annotations manually for accurate comparisons.

Growing the Biodefense Industry

Building on the success of the FELIX program, the Berkeley Lab scientists plan to expand the database by adding new organisms that could be exploited as bioweapons, and call on other groups to add new sequences as well. Meanwhile, Brown is looking forward to using the neatly organized database to train machine learning models, which will lead to even better modified organism detection tools in the future.

Looking to next steps, the team hopes to use the knowledge and techniques gained from the FELIX program to develop detection tools capable of ecosystem-scale monitoring to detect threats in the environment in real time – a capability that Brown describes as “NORAD for biology.”

[Aliyah Kovner](#) is a science writer and editor, and multimedia producer, at Berkeley Lab.

The nose knows: 8 diseases that dogs are good at sniffing out

Source: <https://newatlas.com/health-wellbeing/diseases-that-dogs-are-good-at-detecting-volatile-organic-compounds/>



Aug 15 – It’s been estimated that dogs smell up to 10,000 times better than us. That’s in part because they have about 220 million scent receptors, whereas humans have a mere 5 million. But dogs also inhale in short breaths up to 300 times a minute, meaning that their olfactory cells are constantly picking up new scents. It’s these factors that make them effective – and adorable – real-time disease detectors.

When we’re sick, we produce compounds that waft around us. In infectious or disease states, volatile organic compounds (VOCs) are emitted in breath, blood, sweat and urine, creating a volatilome or ‘aura’



ICI C²BRNE DIARY – August 2023

of molecules around the human body. These VOCs often result in changes in body odor, which, studies have found, are detectable by dogs. But what conditions are dogs able to detect?

Here are eight diseases that our furry friends are particularly good at sniffing out.

Cancer

Research has shown that trained dogs can detect different types of cancer, including melanoma, [colorectal](#) (bowel), lung, [ovarian](#), [prostate](#) and breast cancers. A [2021 study](#) found that a trained dog could sniff out breast cancer from the urine samples of 200 people with 100% accuracy. Of these people, 40 had breast cancer, 182 had other cancers, and 18 were found not to have cancer. But dogs don't necessarily have to be trained to detect cancer. In a [2013 case study](#), an Alsatian, who happened to be a rescue dog, persistently licked at an asymptomatic lesion behind her 75-year-old owner's ear. After seeing his doctor, the man was diagnosed with malignant melanoma.

Diabetes

Diabetic alert dogs (DADs) are service dogs that are specially trained to alert their owners to high and low blood sugar levels; both potentially life-threatening conditions. A [2016 study](#) out of the UK suggested that a dropping blood sugar produces a VOC called isoprene, which is not detectable by humans but that dogs can smell. A [study](#) published in 2019 looking at the reliability of dogs at detecting blood sugars found that, while there was variability between individual dogs, on average 81% of alerts occurred when sugar levels were 'out of range,' that is, too high or too low.

Narcolepsy

Narcolepsy is a lifelong neurological disorder that affects the brain's ability to regulate sleep-wake cycles, leaving people prone to sudden attacks of sleep that, depending on when they hit, can be dangerous. In a [2013 study](#), trained dogs detected 11 out of 12 narcoleptics, leading researchers to conclude that narcolepsy patients produce a distinct dog-detectable odor.

Epilepsy

Like narcoleptics, [studies](#) have found that people with epilepsy produce a specific odor, discernible by trained dogs, that warns of an impending seizure. Even in patients with different types of epilepsy, which produce different types of seizures, dogs were able to detect 'seizure odor' with a sensitivity between 67% and 100%.

Untrained dogs are also capable of detecting seizures. In a [2019 study](#), 19 untrained dogs of various breeds all displayed a significant increase in attention-seeking behaviors – such as making eye contact with a person – when they detected odors from sweat samples taken from epileptics, compared with samples from non-epileptics. It's also been suggested that dogs detect seizures by picking up on behavioral, rather than biological, cues. Regardless, the end result is the same.

Migraines

There are many phases to a migraine, with the first being the premonitory phase, which can present with warning signs like mood changes, food cravings, nausea and brain fog. A lot of the evidence around migraine-detecting dogs is anecdotal, but [53.7%](#) of 1,029 adult migraine sufferers self-reported that their (untrained) dog's behavior changed prior to or during the initial phase of migraine, with changes usually noticed within two hours before the onset of symptoms. Dog alerting behavior included staring, refusing to leave their owner's side, sitting or lying on their owner, or herding them to bed or the couch.

Parkinson's disease

A recent [Chinese study](#) evaluated the accuracy of sniffer dogs to distinguish between patients with Parkinson's disease (PD) who were medicated, those with PD who weren't medicated, and a control group. In people who were medicated, the dogs showed a sensitivity of 91%, for unmedicated PD patients, sensitivity was 89%.

There's a [clinical trial](#) currently running to assess the ability of dogs to discern PD patients from non-PD patients, with a view to using them to ensure early diagnosis of the disease.

Malaria

[Research](#) has found that people infected by malaria produce an odor that makes them more attractive to mosquitoes. In a [2019 study](#), Gambian children with and without asymptomatic malaria were given socks to wear overnight. After sniffing the socks, two trained dogs were able to correctly identify 70% of children with malaria and 90% of healthy children, even detecting children with low parasite loads.



COVID-19

A [just-released review](#) of existing peer-reviewed studies concluded that trained scent dogs are as effective and often more effective at detecting COVID-19 than the tests we currently use, both PCR testing and rapid antigen tests (RATs). And a dog's ability to detect the SARS-CoV-2 virus is not impeded by the presence of other viruses, such as the common cold or flu.

These studies demonstrate the ability of human's best friend to be a cheap but quick and accurate means of detecting disease. But despite this, dogs are not widely used for this purpose.

While there has been, of late, a concerted effort to develop technologically advanced (and relatively expensive) biosensors to diagnose disease, perhaps we should instead focus on the dog's advanced sense of smell. We already use dogs as therapy animals in some hospitals and aged care facilities. Why not put their innate super sniffers to use as disease detectors in these places as well?



Hollywood Predictive Programming: White Supremacy and Bioterrorism

Source: <https://www.zerohedge.com/news/2023-08-15/hollywood-predictive-programming-white-supremacy-and-bioterrorism>

Aug 16 – Having recently watched two new films released in 2023 ([The Wrath of Becky](#) and [Resident Evil: Death Island](#)), it was striking how propagandized the storylines were, filled with subtle and outright nods to the narrative du jour of the week. Storylines are crafted to capture the imaginations of viewers, preying upon their fears, suspicions, and concerns about the invisible present-day boogeyman dangers. (Un)naturally, such

worried and suspecting minds have been manipulated to think this way by repeatedly reinforcing narratives at the behest of state-sponsored media outlets churning out “here's what you need to know” (here's how you should interpret what we are telling you) content. Relentlessly and unapologetically.

► Read the full article at the source's URL.

Wisconsin Sen. Ron Johnson unleashes bizarre rant about Covid pandemic and claims it was 'pre-planned' by unnamed elites with the goal of taking away human rights



Source: <https://www.dailymail.co.uk/news/article-12400175/Wisconsin-Sen-Ron-Johnson-goes-bizarre-rant-Fox-News-claims-Covid-pandemic-pre-planned-unnamed-elites-goal-taking-away-human-rights.html>

Aug 12 – [Wisconsin](#) Senator Ron Johnson has went on a bizarre rant while appearing on [Fox News](#) and claimed the Covid pandemic was 'pre-planned' by unnamed elites.

The [Republican](#) appeared on the news channel alongside presenter Maria Bartiromo and was speaking about the pandemic and vaccines.

During the interview, Johnson wildly claimed that the pandemic was planned as part of an ongoing scheme to take away the freedom of Americans.

The 68-year-old said: 'We are going down a very dangerous path, that has been laid out and planned by an elite group of people that want to take total control over our lives.

'That's what they are doing bit by bit. They really risk taking away all of our sovereignty. But people have to wake up to the dangers of the moment.'

He said: 'The doctors I have been dealing with, they believe hundreds of thousands of Americans lost their lives because they were denied early treatment.

'They were denied it because the FDA sabotaged Ivermectin saying 'c'mon y'all you're not a cow, you're not a horse'.

'This was a noble prize winning medicine that could have saved hundreds of thousands of lives.



ICI C²BRNE DIARY – August 2023

Johnson continued: 'This is all pre planned by an elite group of people. This is very concerning in terms of what has happened, what is happening, what continues to be planned for our loss of freedom.'

'It needs to be exposed but unfortunately there are very few people in Congress who are willing to take a look at this, they all pushed a vaccine. 'So many people just simply don't want to admit they were wrong and they are going to do everything they can to assure they are not proving wrong. 'We are up against a very powerful group of people here Maria.'

Following his interview on Fox, Johnson claimed on his Twitter page that the FDA had 'quietly' approved the use of Ivermectin.

Johnson had been referring to an ongoing legal battle between the FDA and three doctors who accuse the agency of impeding their right to prescribe Ivermectin as treatment for Covid.

The FDA has not approved the drug for fighting Covid-19, but conceded that doctors have the authority to prescribe if they wish.

During the pandemic, the senator had made multiple podcast and radio appearances pushing Ivermectin as a treatment for Covid.

At the time, Johnson had argued for the use of Hydroxychloroquine and Ivermectin as treatments.

Ivermectin is commonly used to deworm livestock, and it is approved for use in humans to treat parasitic infection.

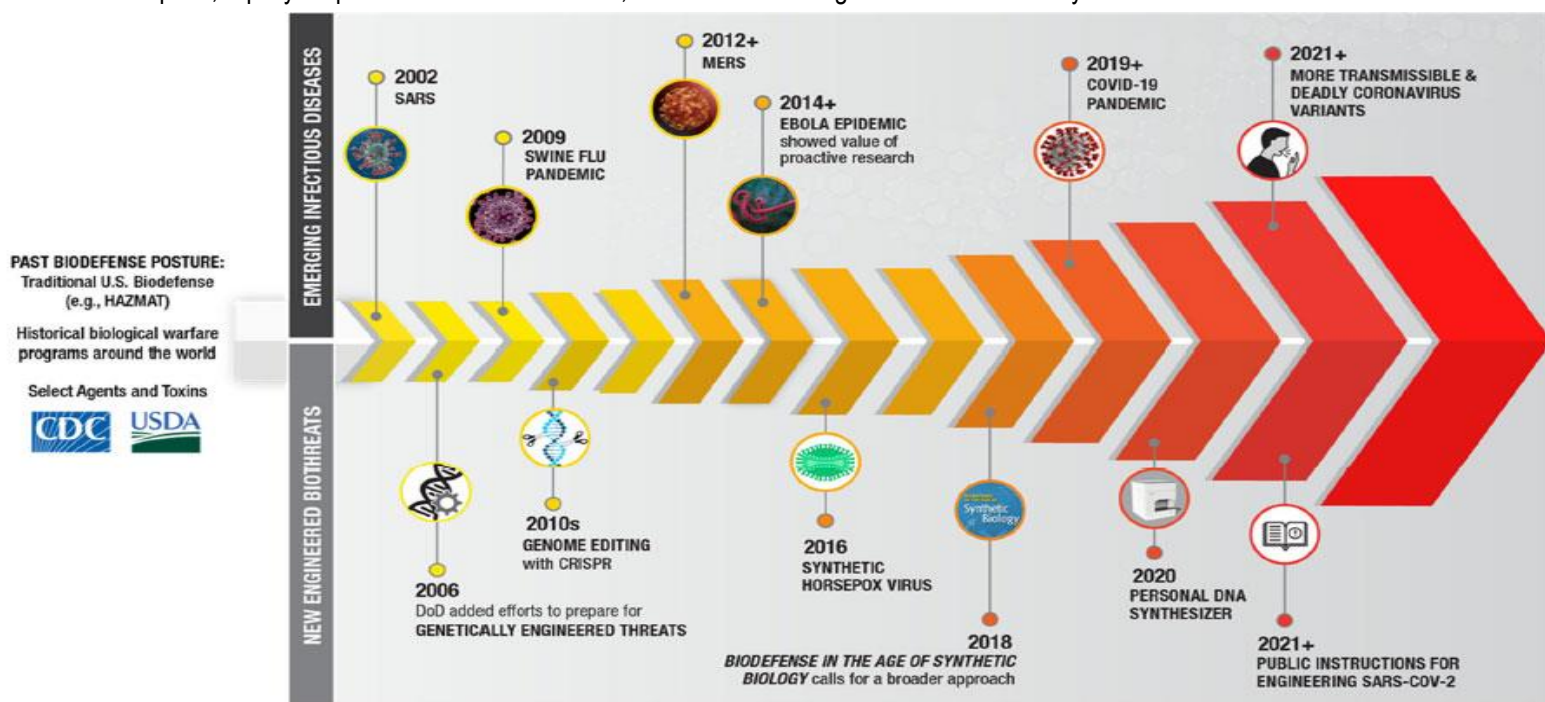
The drug became popular among conservatives after commentators and held up the anti parasitic drug as a miracle cure for the coronavirus and other illnesses. The Food and Drug Administration has not approved it for use in treating COVID-19 and warns that misusing ivermectin can be harmful, even fatal.

DOD Biodefense Posture Review Released

Source: <https://globalbiodefense.com/2023/08/17/dod-biodefense-posture-review-considers-biological-risks-from-climate-ai/>

Aug 17 – The U.S. Department of Defense today released the [Biodefense Posture Review](#), outlining reforms aimed to posture the DOD in the face of future biothreats.

"We face an unprecedented number of complex biological threats," said Deborah Rosenblum, Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs. "The Biodefense Posture Review fully assesses the biological threat landscape through 2035. This review outlines significant reforms and lays the foundation for a resilient total force that deters the use of bioweapons, rapidly responds to natural outbreaks, and minimizes the global risk of laboratory accidents."



Evolving Biothreat Landscape

In November 2021, the Secretary of Defense issued a memorandum, [Biodefense Vision](#), providing direction for the Department to ensure DoD's preparedness to operate in a biothreat environment and to support the national biodefense enterprise at home and abroad. In that memorandum, the Secretary of



Defense directed a comprehensive review of DoD's biodefense posture to bolster the Department's overall defense posture and maintain readiness and resilience against burgeoning threats, whether they are naturally occurring, accidental, or deliberate in origin. "We're increasing collaboration and synchronizing efforts across the DOD enterprise—everything from policies and authorities, to research, acquisition, and investments—to meet the department's biodefense requirements," said William LaPlante, Under Secretary of Defense for Acquisition and Sustainment. "One of the most important reforms in the Biodefense Posture Review that we have already institutionalized is the Biodefense Council."

The Biodefense Council will build on the intense collaboration of the DoD biodefense enterprise over the past several years and will synchronize and integrate authorities and responsibilities to provide a more empowered and collaborative approach to biodefense. "The Biodefense Posture Review and the Biodefense Council will further enable the Department to deter biological weapons threats and, if needed, to operate in contaminated environments," said John Plumb, Assistant Secretary of Defense for Space Policy. He adds, "As biological threats become more common and more consequential, the BPR's reforms will advance our efforts not only to support the Joint Force, but also to strengthen collaboration with allies and partners."

Naturally Occurring Biological Threats

Biological threats can affect humans, animals, plants, and the environment, resulting in significant health, economic, social, and national security impacts. Infectious disease threats do not respect borders. Novel infectious diseases, the resurgence and spread of once geographically limited infectious diseases, zoonotic diseases, and antimicrobial resistance can overwhelm response capacities and make outbreaks harder to control. As seen with the COVID-19 pandemic, an infectious disease outbreak could spread rapidly across oceans and continents, directly affecting the U.S. population and its health, security, and prosperity.

Respiratory diseases (e.g., tuberculosis, seasonal influenza), food and waterborne diseases (e.g., typhoid, cholera), and vector-borne diseases (e.g., malaria, dengue fever) may cause local or regional epidemics. While force health protection (FHP) measures are usually effective in countering these threats, some emerging infectious disease threats (e.g., multiple-drug resistant bacteria, malaria organisms resistant to anti-malarial medications) risk rendering medical countermeasures ineffective. And COVID-19 demonstrated that some of the most challenging infectious diseases are pandemic-capable novel respiratory pathogens that are either unsuspectingly introduced or arise in areas with limited surveillance and laboratory capabilities. Delays in detection and warning, coupled with global travel, now allow such organisms to rapidly spread around the globe.

Accidental Biological Threats

The risk of laboratory accidents may be increasing with the rise in the number of laboratories around the world conducting high-risk life sciences research and research with potential pandemic pathogens without appropriate oversight. Although this research is important for developing countermeasures and understanding and predicting future outbreaks, laboratories with insufficient biocontainment or biosafety protocols and practices exacerbate the risk of an outbreak through laboratory-acquired infections or accidental release of a pathogen into the environment. Even with state-of-the-art equipment and standard biosafety and biosecurity protocols, laboratory accidents are possible due to human error or mechanical failures.

As the biothreat landscape evolves, there is an increased potential for a biological safety (biosafety) event resulting in the unintentional release of pathogens. Growing research in infectious diseases enables the development of testing, pharmaceutical treatments, and vaccines to support public health and the global community. As research in the field of biology and biotechnology expands, so does the increased potential of accidental bioincidents. The increase in accidental biothreats challenge biosafety, biological security (biosecurity), physical security, and other biological containment (biocontainment) considerations, and creates the concern of unintended and dangerous consequences resulting from inconsistent or incomplete review and oversight mechanisms.

Deliberate Biological Threats

The use of biological weapons or their proliferation by state or nonstate actors presents a significant challenge to national security, people, agriculture, and the environment. Multiple nations have pursued clandestine biological weapons programs, and a number of terrorist groups have sought to acquire biological weapons. In addition, advances in biotechnology, including synthetic biology, could make it easier to develop and use biological agents as weapons. In many countries around the world, pathogens are stored in laboratories that lack appropriate biosecurity measures and could be diverted by actors who wish to do harm. Further, thousands of clinical samples generated during an epidemic can pose a biosecurity vulnerability if handled without appropriate security considerations, potentially facilitating access to materials and information that could be used in the development of a biological weapon.

The PRC, Russia, North Korea, and Iran, probably maintain the knowledge and capability to produce and employ traditional pathogens and toxins. These countries historically pursued, and at least one country

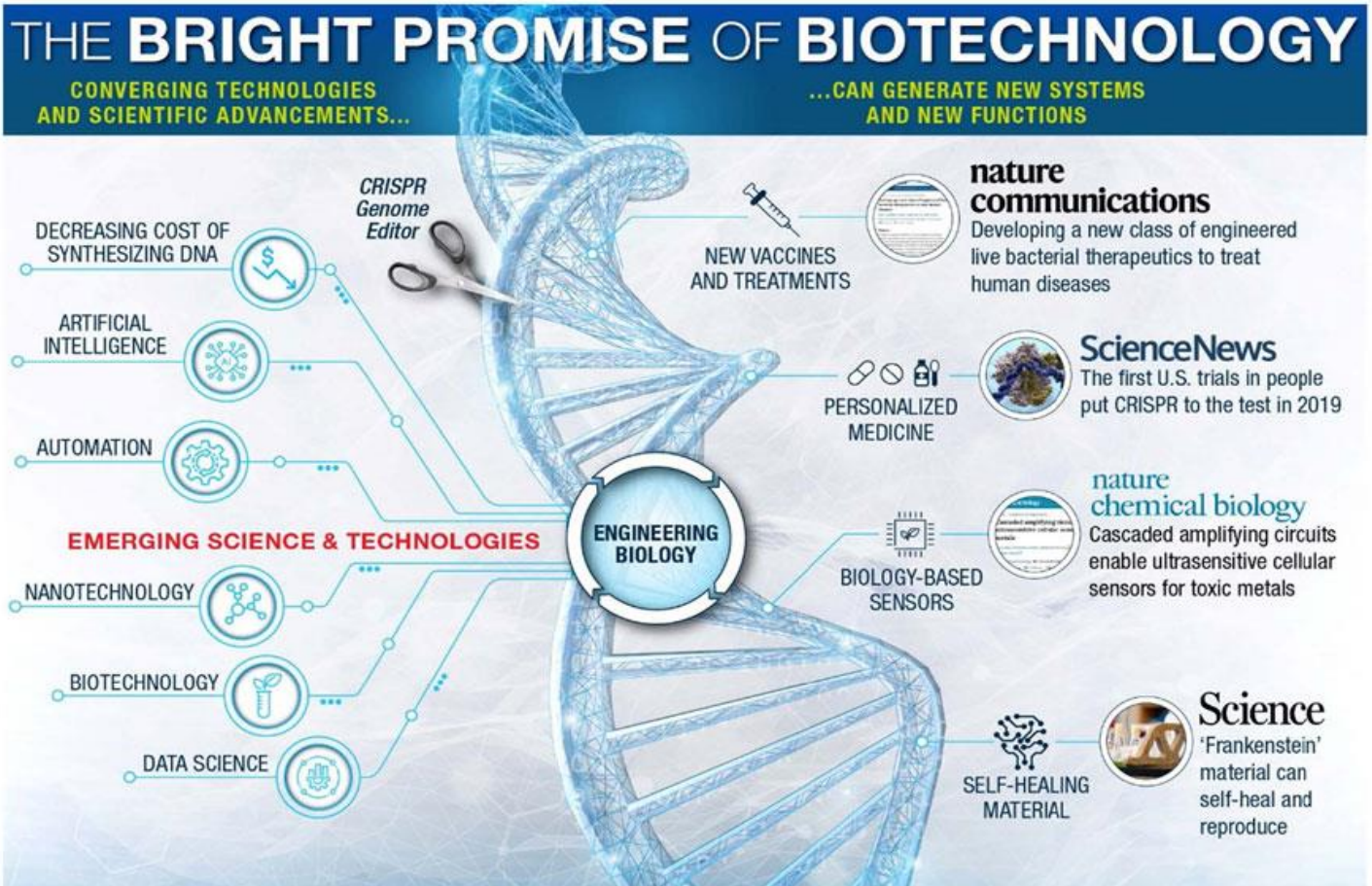


(North Korea) continues to pursue, pathogens that cause highly infectious or contagious diseases, such as anthrax, plague, and toxins, including botulinum toxin. These nations probably also retain the knowledge and ability to employ these agents if necessary. Adversaries could also use advances in peptide synthesis technology and metabolic engineering to develop and produce toxins in quantities suitable for a range of employment options. Advances in both synthetic biology and peptide synthesis could enable states to develop a wide range of novel toxins with both incapacitating and lethal effects that are not on a select agent list. These toxins could include animal toxins, marine toxins, or plant toxins. Peptide synthesis technologies developed in the last decade could allow toxins, including engineered variants, to be synthesized in quantities that are more militarily relevant, raising the concern that they are no longer just suitable for targeted killings.

The United States assesses that North Korea and Russia maintain offensive biological weapons programs in violation of Biological Weapons and Toxins Convention (BWC) obligations and identifies concerns with Iran's activities and its compliance with the BWC. Russia has provided an incomplete acknowledgement of the former Soviet program, has not furnished evidence of the dismantlement or cessation of key activities, and continues secrecy efforts to protect Russia's potentially dual-use biological research and development efforts.

Additionally, the most recent Compliance and Adherence Report with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments raises concerns with PRC compliance with the BWC, based on research and activities with potential dual-use applications. The United States has compliance concerns with respect to PRC military medical institutions' toxin research and development given their potential as a biothreat. The PRC has also released plans to make China the global leader in technologies like genetic engineering, precision medicine, and brain sciences. These Chinese publications have called biology a new domain of war.

The PRC and Russia have also proven adept at manipulating the information space to inhibit attribution, to reduce trust and confidence in countermeasure effectiveness, and potentially to slow decision-making following deliberate use. The U.S. military has been involved in conflict operations during every declared pandemic of the 20th and 21st centuries. None of these events were a result of bioweapon use, but they all challenged the military's operational capabilities. The most likely infectious disease threats to deployed U.S. forces come from endemic diseases (i.e., diseases that regularly occur in a particular population or area).



Emerging and Disruptive Technologies

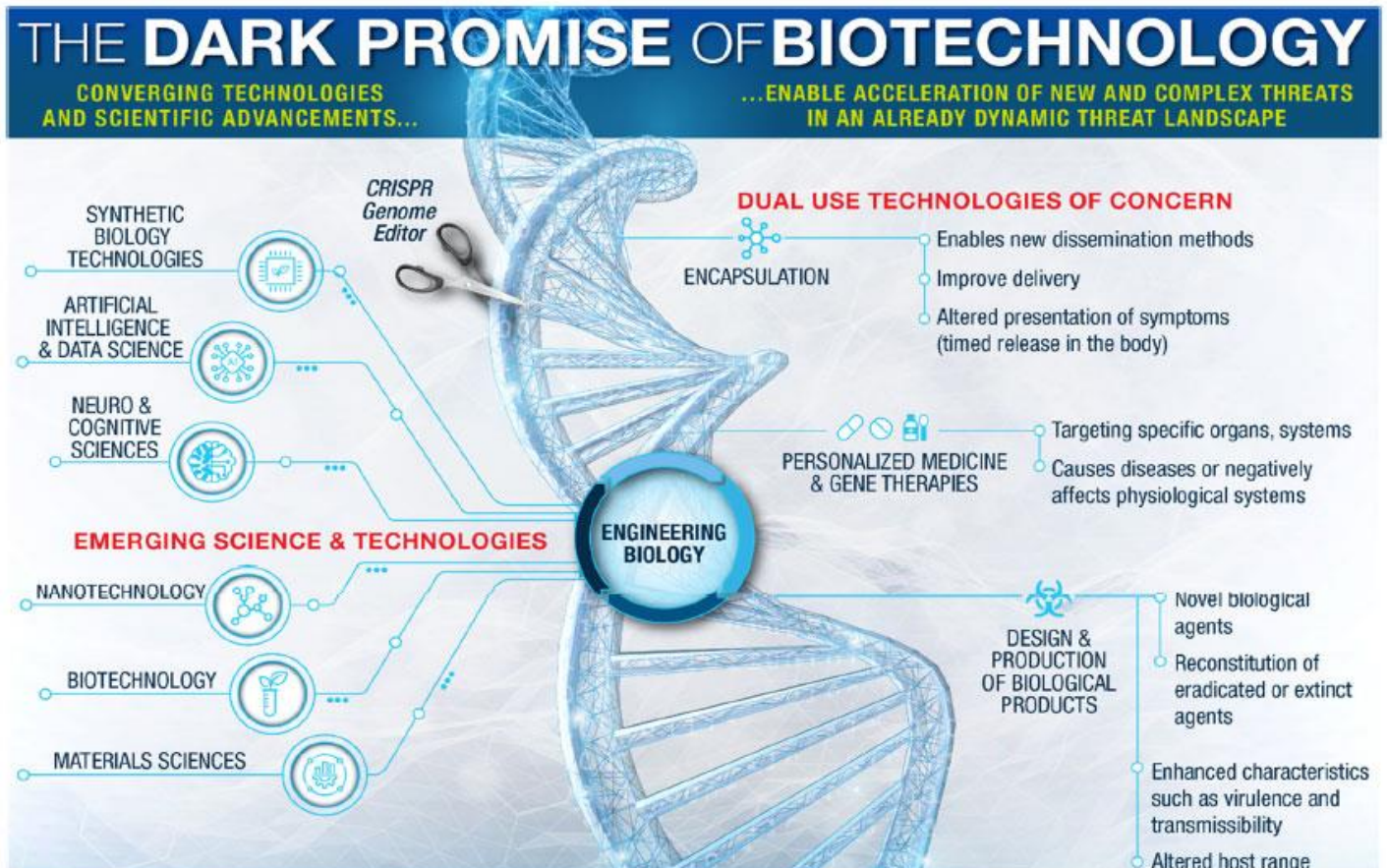
New technologies, such as big data, artificial intelligence, and genomic modification, have the potential to significantly influence the chemical, biological, radiological, and nuclear (CBRN) environment. Such technologies simultaneously offer the prospect for more effective, resilient, and cost-efficient military and civilian solutions while also representing potential new threats from state and non-state actors. The same biological and chemical science advancements created to develop life-saving medical countermeasures could also be used by potential adversaries to develop new or enhanced agents.

Technologies intended to reduce testing and production inefficiencies, such as biofoundries and additive manufacturing, create opportunities to reduce the development footprint and increase the number of proliferation pathways available to malign actors. In this way, emerging and disruptive technologies present both risks and opportunities to the United States, its allies, and partners.

Risks from Bioincidents

The ability to determine a deliberate biological weapons attack is complicated by the potential for an accidental laboratory release and the growing risks from naturally occurring diseases due to climate change. Additionally, reservoirs of naturally occurring pathogens of high consequence are potential avenues for biological weapons research.

Adversaries can also leverage this more complex operating environment to constrain U.S. strategic choices by masking an attack, augmenting other activities, or conducting an opportunistic disinformation campaign. Furthermore, outbreaks are likely to lead to an increase in requests for Defense Support of Civil Authorities, which adds a competing activity to the Joint Force mission of fighting and winning the nation's wars.



As the biological threat landscape continues to evolve, so must our biodefense capabilities. It is critically important that the Total Force can fight and win in a CBRN-contaminated environment. This importance stretches across the costs and risks of future biological threats, whether natural or human-made, for the Department and the Joint Force.

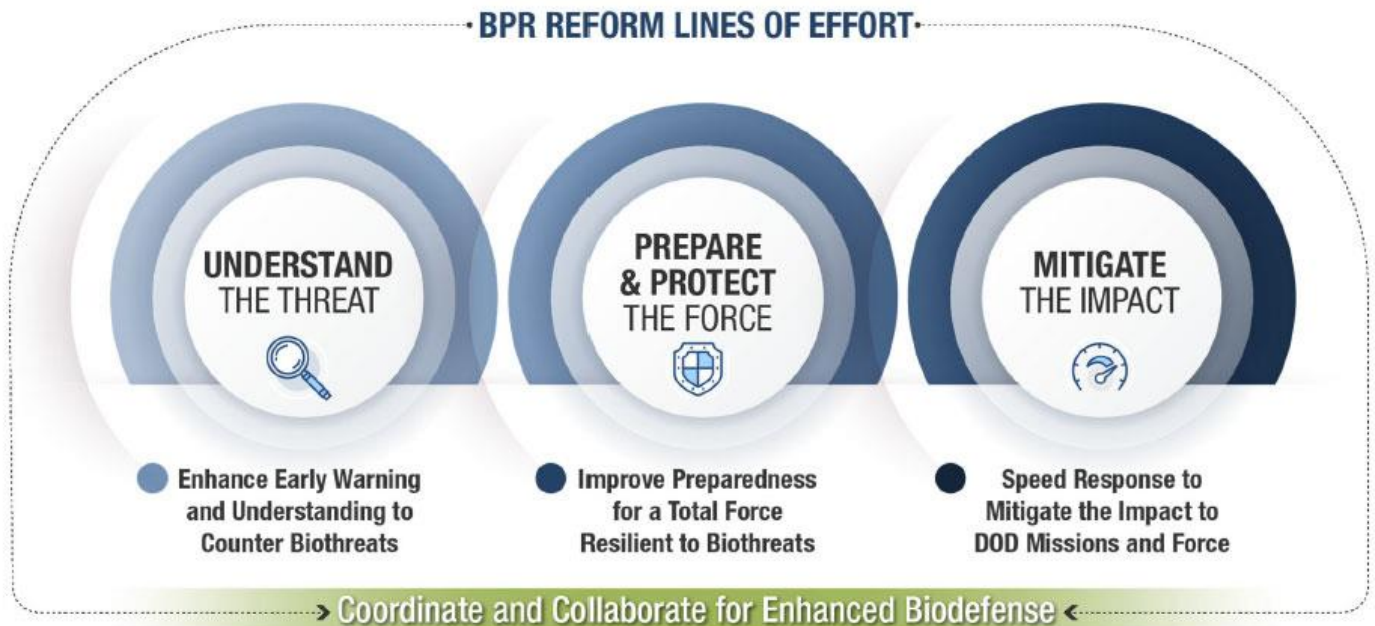
Lines of Effort to Drive Biodefense Actions

A Total Force resilient to biotreats and biological hazards (biohazards) provides the first step to deter the use of bioweapons and deliberate attack. Such resilience, properly messaged and demonstrated, bolsters



integrated deterrence. DoD's extensive biodefense capabilities can be leveraged to deny or greatly minimize the benefit of using bioweapons and further deter the development or proliferation of bioweapons. Should deterrence fail, this resilience will enable the Total Force to operate through contaminated environments and further diminish adversary benefits of deliberate biological attacks. In concert with improved Total Force resilience, collaborative biodefense engagement with our allies and partners improves our mutual biodefense, strengthens our alliances, improves interoperability, and promotes burden-sharing. These partnerships maximize effectiveness and minimize risk to the Total Force. Reinforcement of international norms, the Committee on Foreign Investment in the United States (CFIUS) process, export controls, information security, and cybersecurity (protection against loss of critical data, capabilities, or intellectual property) will all work to slow and obstruct adversary bioweapon programs. A similarly wide range of response actions could help hold perpetrators accountable for the use of bioweapons and support identification and attribution of naturally occurring diseases or sources of accidental bioincidents.

Given that naturally occurring disease cannot be deterred, DoD requires a resilient force enabled by capabilities that also address emerging disease threats. The ability and capabilities to deter deliberate biological attacks also improve the Total Force's overall resilience to emerging, naturally occurring, infectious diseases of operational significance.



Four BPR reform lines of effort drive biodefense actions and address the potential costs and risks posed by future biothreats, regardless of origin, to DoD missions and the Total Force.

- Coordinate and Collaborate for Enhanced Biodefense
- Enhance Early Warning and Understanding to Counter Biothreats
- Improve Preparedness for a Total Force Resilient to Biothreats
- Speed Response to Mitigate the Impact to DoD Missions and Forces

Biodefense Council

The Biodefense Council will serve as the principal forum to advise the Secretary of Defense, the DepSecDef and other DoD leadership on biodefense issues and address the challenges identified in the BPR and beyond. The Biodefense Council will not supplant individual missions in biodefense but will facilitate integration and information flow; enable collective decisions; convene the biodefense enterprise to review topics on a recurring basis; and empower the heads of DoD Components to address tough or acute challenges, when necessary.

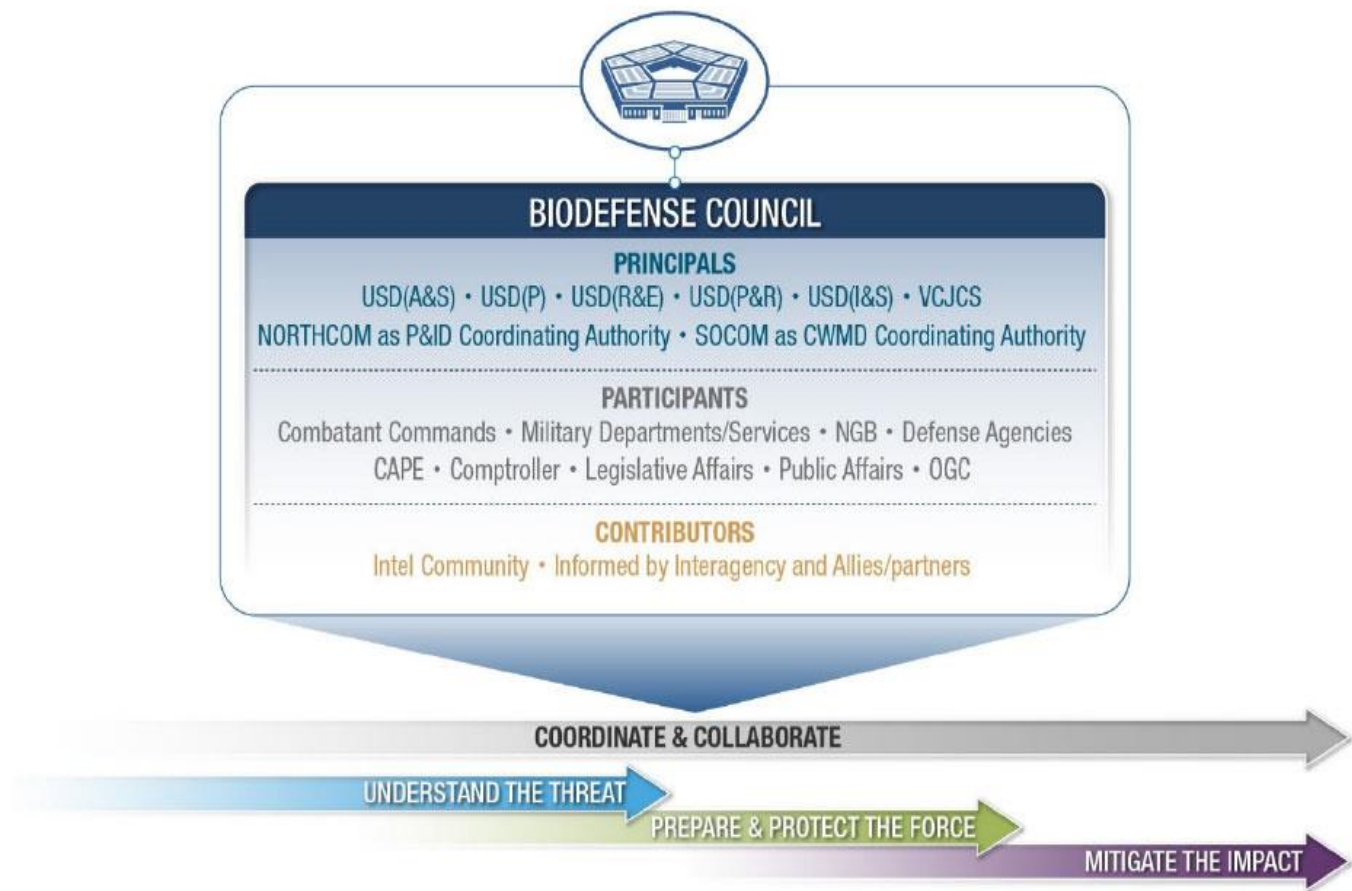
The Biodefense Council will convene to delineate primary functions to enhance collaboration, prioritize threats, and create an efficient approach to address the prioritized threats. Additionally, the Biodefense Council will advance the execution of responses to significant bioincidents and enhance the ability of DoD to mitigate biothreats and biohazards.

The Biodefense Council is chaired by the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)). The Biodefense Council has a single chair to better organize DoD-wide biodefense



ICI C²BRNE DIARY – August 2023

responsibilities. The Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)) will serve as the Council's Executive Secretary.



Biodefense Council Governance Structure

The Biodefense Council's activities include: providing guidance and oversight for the biodefense posture; synthesizing intelligence products, biosurveillance, early warning, and attribution information in order to warn DoD leadership of potential impacts on posture and missions; reviewing biodefense integrated portfolio priorities and coordinating investment strategy to address readiness shortfalls and modernization needs; and serving as a standing body to facilitate DoD-wide collaboration on biodefense response activities, as needed, to address bioincidents of national or international significance.

Improve Biothreat Intelligence Collection, Analysis, and Sharing.

The rapidly evolving threat landscape warrants bolstering the Department's intelligence collection and analytic capabilities to better detect emerging threats of potential operational significance or pandemic potential that may impact our ability to achieve the defense strategy. These improvements will enhance capabilities to collect, analyze, and make reporting readily available to more quickly identify emerging biothreats, increase early warning, and speed threat characterization to understand the potential impact of biothreats on DoD missions, capabilities, and people. Robust intelligence collection, in concert with the work of other departments and agencies, will seek to provide early indication and warning to help manage risk.

Increase Biothreat Situational Awareness Through Biosurveillance

Biosurveillance is a key enabler to gather, integrate, interpret, and communicate essential information and indications of biohazards or disease activity affecting DoD missions or forces.

The Biosurveillance Program covers all CBRN health surveillance and seeks to inform decision makers with early warning of health concerns to enhance protection of the force. Current program efforts include



development of a concept of operations for a Hub- and Portal-based approach and conduct of a capability based assessment to address burgeoning threats and prioritize early warning.

The BPR identified opportunities to improve and refine the programmatic strategy for biosurveillance to build DoD's capabilities for early warning, risk awareness, and monitoring for bioincidents. The Biodefense Council will oversee the Biosurveillance Program Strategy to ensure a forward-leaning program with the necessary, clearly defined, ambitious milestones to transform biosurveillance data into actionable, decision-focused information at the tactical, operational, and strategic levels.

Expedite Characterization of Emerging Threats

DoD must be prepared to rapidly develop and deliver capabilities against any potential threat, including currently unknown or novel ones. To be prepared, DoD requires enabling capabilities and analytical capacity to quickly characterize the potential risks posed by emerging or reemerging biothreats, and an assessment of existing and developing capabilities against those threats. This threat characterization must be closely linked to intelligence and biosurveillance improvements that drive early warning.

DoD will pivot away from viewing the threat landscape as a defined list of known biological and chemical agents towards removing or reducing the impact of agents' effects. DoD's enhanced biodefense and pandemic preparedness will enable the Chemical and Biological Defense Program (CBDP) to expand efforts to characterize biothreat agents and support more rapid development and delivery of biodefense products and capabilities.

Recommendations in this area include speeding validation of existing capabilities against emerging threats or rapidly delivering new physical countermeasures (e.g. improved mask filtration, updated detector modalities); more adaptable processes to drive development of novel medical countermeasures and label expansion against novel pathogens; and additional investments in multiplex and threat-agnostic detection systems.

Reinforce Biorisk Management to Ensure Safe and Secure Research

As DoD pursues R&D to address emerging threats, it must minimize the chances of laboratory incidents, reduce the likelihood of deliberate or accidental misuse of biological agents, ensure effective biorisk (biosafety and biosecurity) practices and oversight, and promote responsible research and innovation.

The BPR recognizes that, since the 2015 biosafety lapses at Dugway Proving Ground, Utah, DoD has made significant changes to improve biorisk programs at DoD laboratories conducting RDT&E with BSAT. The creation of the DoD BSAT Biorisk Program, with the USD(A&S) as the PSA and the Secretary of the Army designated as the DoD Executive Agent, has made progress in improving the oversight, technical review, inspection, and synchronization of biorisk programs across DoD BSAT laboratories. To oversee the possession, use, and transfer of BSAT—which have the potential to pose a severe threat to public, animal, or plant health—all DoD BSAT laboratories must comply with Federal Select Agent Program regulations, which are jointly managed by the CDC and the U.S. Department of Agriculture.

The DoD BSAT Biorisk Program oversees compliance with Federal regulations, coordinates necessary inspections and reviews, and is responsible for ensuring that DoD reports any BSAT releases to the congressional defense committees. The BSAT Biorisk Program includes a scientific review panel that conducts technical and periodic assessment of biorisk protocols and funds projects to promote responsible research, to close scientific knowledge gaps, and to base DoD protocols on sound scientific data to mitigate risk.

The BPR recommends further review for opportunities to strengthen biorisk management within DoD to ensure a coordinated and integrated effort, better posturing DoD's laboratories and performer partners to safely and securely conduct research into prioritized, emerging threats.

The BPR identified opportunities to decrease the risk of accident and improve biorisk management through increased coordination, clarification of responsibilities, and the potential to leverage the oversight activities. To develop DoD's biorisk workforce and reduce the potential for conflicts of interest between lab safety and research outputs, the Chemical and Biological Defense Program (CBDP) is centrally funding the Biosafety Officers supporting DoD biological select agents and toxins (BSAT) laboratories, beginning in FY 2023.

To minimize the risk of overseas accidents, DoD should improve coordination with allies and partners to identify and capitalize on critical defense-specific capabilities. These partnership activities present opportunities to strengthen DoD transparency and compliance with international standards and norms and serve to counter disinformation asserting DoD biodefense activities support an offensive weapons program.

BPR recommendations also include more proactively countering adversary mis/dis-information campaigns and rhetoric around biodefense activities and that attempt to undermine peaceful efforts.

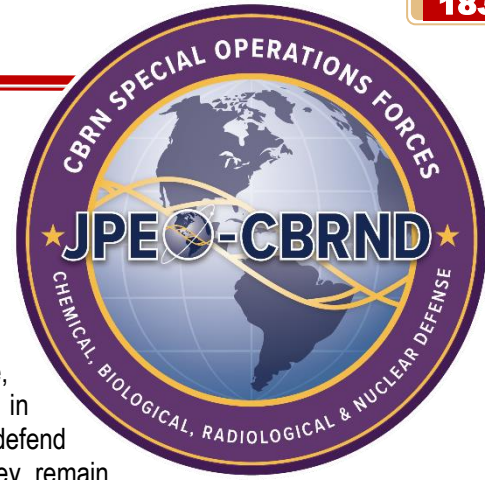
●► Read the full report: [U.S. Department of Defense 2023 Biodefense Posture Review](#)



The Need for Speed in Biodefense: How JPEO-CBRND is Shaping its Biological Defense and Medical Strategies

By Kelly Burkhalter and Daniel Critchfield

Source: <https://www.homelandsecuritynewswire.com/dr20230819-the-need-for-speed-in-biodefense-how-jpeocbrnd-is-shaping-its-biological-defense-and-medical-strategies>



Aug 19 – Biological incidents possess an alarming ability to wreak havoc on a massive scale, capable of rapidly escalating beyond the scale seen during COVID-19. The need lies in developing solutions that surpass the speed of these threats. Our warfighters need to swiftly defend themselves against a biological threat, or better yet, prevent it entirely, to ensure they remain operationally ready to carry out their mission. The COVID-19 pandemic is the perfect example of how a biological incident can start off small and swiftly snowball into unprecedented crisis levels.

The Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND), on behalf of the Defense Department (DOD), partnered with the Department of Health and Human Services (HHS) to support the national response to the COVID-19 public health emergency. Though its role in the pandemic response will fully transition to HHS this fall, JPEO-CBRND implemented lessons learned to update its approach to tackling emerging threats. This dynamic strategy underscores the principles of rapid response, integrated layered defense and partnerships to protect military personnel from CBRN threats.

In the 2022 National Biodefense Strategy, the White House outlined the importance of staying ready for any biological incident through investing in capabilities such as manufacturing, developing prototypes, analyzing existing data that could be useful in developing future countermeasures and standardizing clinical trials. Collectively, these goals will enable future response efforts to move faster at lower cost.

The future of biodefense depends on the ability to rapidly respond to an event by quickly developing and distributing medical countermeasures (MCMs), such as vaccines and therapeutics. This includes optimizing manufacturing techniques and establishing robust partnerships to ensure these MCMs can be quickly and effectively deployed in the event of a threat.

JPEO-CBRND's Joint Project Lead for CBRN Defense Enabling Biotechnologies (JPL CBRND EB) has led a significant investment in platform technologies and programs to improve preparedness for future threats. Platform technology refers to the use of standardized processes and tools to rapidly develop and manufacture MCMs in response to a threat. This approach is like setting up an assembly line that can be turned on when needed, rather than building the line from scratch each time a product is required. The goal is to have the ability to quickly develop and manufacture MCMs in response to a threat.

In addition to the use of platform technologies, another practice to ensure rapid development of MCMs is to quickly pivot from a prototype to a product that can be distributed in compliance with U.S. Food and Drug Administration (FDA) regulations for emergency use. This puts safe and effective medicines and drugs into the hands of warfighters faster, leveraging processes such as emergency use authorization (EUA) on the path to full FDA licensure, since the licensure process can take nearly decades for countermeasures to be available.

"This dynamic approach allowed us to get vaccines out the door quickly, because we have already completed a lot of the upfront work," said Bruce Goodwin, Joint Project Lead for JPL CBRND EB. "We are deliberately looking for stepping stones along the FDA licensure path, positioning safe and effective products so they are safe enough for our warfighters and the medical community to respond quickly to a demand signal."

Partnerships are another key to a strong biodefense approach. Collaborating across disciplines and with industry was critical to the COVID-19 response and will continue to be important to push other biological threat solutions forward. In addition to HHS, JPEO-CBRND worked with organizations such as the Defense Contract Management Agency, Army Contracting Command, U.S. Agency for International Development and Army Corps of Engineers, and supported Operation Warp Speed during the COVID-19 response. These diverse partnerships helped the organization understand the options available to move solutions forward, brought different minds to the table and helped the program find a way to say, "yes," quickly.

"One of our leaders during the response would tell us repeatedly that 'every day counts.' At the time, we thought he was trying to inspire. In retrospect, he was absolutely and literally correct. Not only every day, but every hour counts in a response. Issues like 'wrong type of funding' and 'delayed contract modifications' are antithetical to rapid response," said Dr. Chris Earnhart, Chief Technology Officer for JPL CBRND EB.

Platforms and strong partnerships are two key enablers to a rapid response. JPEO-CBRND has several programs underway to support speed and agility in medical countermeasure development. These programs take a proactive approach through constantly examining possible solutions for potential



incidents, rather than simply waiting for something to happen first. Moreover, these programs leverage readily available data and materials, maximizing their efficiency and effectiveness.

“Our medical strategy is a direct output of our COVID-19 response,” said Nicole Kilgore, Deputy Joint Program Executive Officer for CBRND. “One of our biggest lessons learned is we can’t wait for perfect to act. We need to approach these efforts by working activities in parallel and accepting risk as we work our way through testing potential courses of action. This is why our Medical Strategy relies on flexible contracting, innovative approaches, and proven platforms to get our Joint Force safe solutions quickly.”

“Programs that allow us to actively modernize biodefense such as Rapid Acquisition and Investigation of Drugs for Repurposing (RAIDR) is already underway within our Joint Project Manager for CBRN Medical. RAIDR finds additional uses for approved and safe drugs that are currently not being used. So, we take a second look at those proven-safe medical countermeasures and see whether they can help us respond quickly to the ever-changing threat landscape,” said Kilgore.

Another program managed by the Joint Project Manager for CBRN Medical is the Vaccine Acceleration by Modular Progression (VAMP) Enhanced Biodefense program, which brings together interagency, industry and academia to design and construct vaccine prototypes and evaluate them in clinical and non-clinical studies.

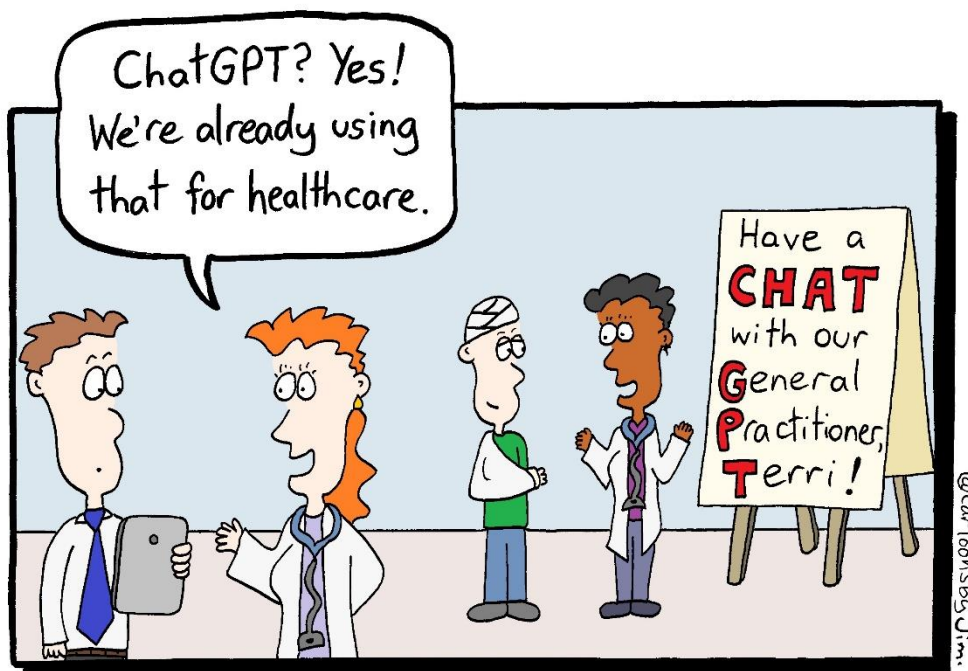
Within JPL CBRND EB’s program portfolio are two additional biodefense efforts. The Generative Unconstrained Intelligent Drug Engineering (GUIDE) program is a robust suite of computational tools that enable rapid countermeasure development using information gleaned from subject matter expert knowledge, databases, artificial intelligence/machine learning tools, and infrastructure for efficient development of potential MCMs. Rapid Access to Products in Development (RAPID) is another new program, which provides a broad library of MCMs ready for emergency fielding in a potential CBRN incident.

“As we face an uncertain future, the lessons learned from COVID-19 will undoubtedly shape our approach to biodefense. With a strong and coordinated response, we can be prepared for any biological threat that may come our way. The importance of speed cannot be overstated, and we must continue to work together to protect the men and women of the Joint Force and the public,” said Kilgore.

The DOD is currently underway with a review of the Nation’s current and future bio-preparedness posture and working to create tools and capabilities to mitigate emerging threats. The work the JPEO-CBRND has done to respond to and mitigate COVID-19 has ensured a more stable supply chain and a ready industrial base, laying the foundation for future readiness.

[Kelly Burkhalter](#) is a Lead Associate, at Booz Allen Hamilton.

[Daniel Critchfield](#) is a Strategic Communications Specialist, at Booz Allen Hamilton.



ICI
International
CBRNE
INSTITUTE

A common roof for international
CBRNE First Responders



Join us!



Rue des Vignes, 2
B5060 SAMBREVILLE (Tamines)
BELGIUM

info@ici-belgium.be
www.ici-belgium.be