2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

January 2019

New year

New challenges

New threats

Preserve peace

www.cbrne-terrorism-newsletter.com

C²BRNE DIARY– 2019©

January 2019

Website: www.cbrne-terrorism-newsletter.com

Editor-in-Chief

BrigGEN (ret) Ioannis Galatas MD, MA, MC (Army)
PhD 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

PUBLISHER

Mendor Editions S.A.

3 Selinountos Street
14231 Nea Ionia
Athens, Greece
Tel: +30 210 2723094/-5
Fax: +30 210 2723698

Contact e-mail: Valia Kalantzi info@mendor.gr

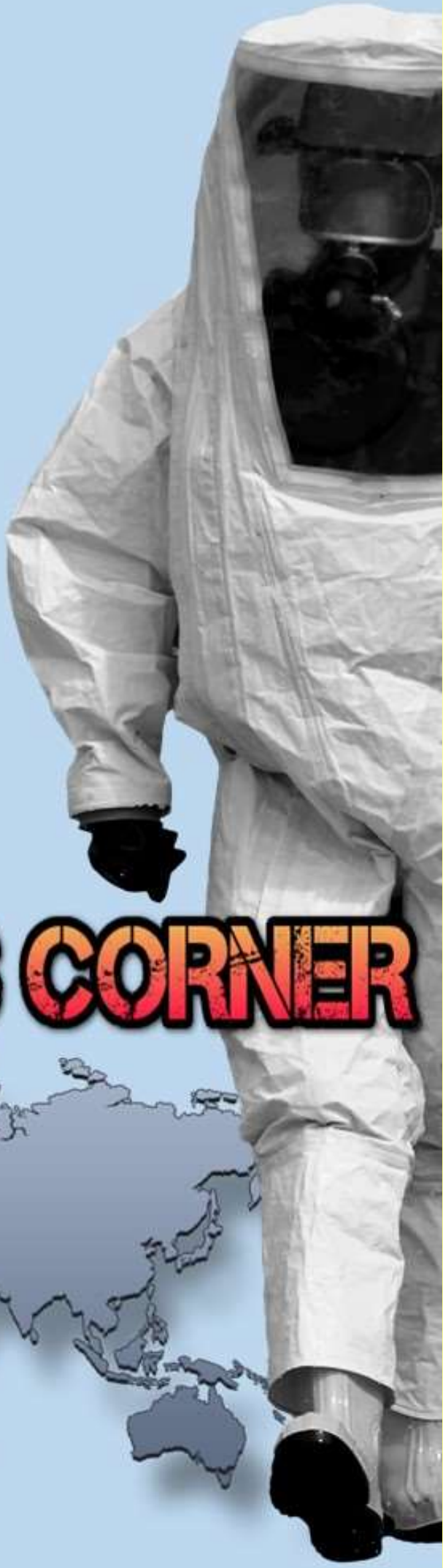
C²BRNE DIARY is:

1. Read by First Responders in more than 80 countries around the globe;
2. Distributed free to more than 700 institutions, organizations, state agencies, think tanks, defense companies, institutions and universities.

International CBRNE Institute

CBRNE-Terrorism Newsletter

C²BRNE DIARY



EDITOR'S CORNER

Editorial

Brig Gen (ret'd) Ioannis Galatas, MD, MA, MC

Editor-in-Chief
C²BRNE Diary

Dear Colleagues,

A very Happy New Year 2019 to all CBRNe First Responders around the globe! Tons of health, joy, stamina, dedication, hard work, a touch of luck, infinitive doses of patience, moderate tolerance to stupidity especially when it comes from people in high places, healing humor and success in both personal and professional life!

The C²BRNE Diary will continue to provide information related to the field of our expertise mainly because knowledge is power and the best vehicle to overcome obstacles, identiy gaps and solve problems. A new chapter – "Drone News" – has been added in Part II of the newsletter. Not because of the latest December 2018 Gatwick insidence but because drones and UAVs are not future pictures but a yesterday's reality. New applications and tasks are added almost on daily basis both in the miitary and civilian environments. They used to say for CBRN threats that it is not a matter of how but a matter of when. And there is nothing more true than a UAV attack that will cause havoc and bloodshed. Conventional or assymmetric? Who cares!

We always welcome articles you think they would be of interest to others or your own writings on CBRNe related issues. We have a wide network of sources searching the world for new products, new ideas and new solutions but an additional pair of eyes is always welcomed. May I remind to new readers that the Editor's Corner chapter contains info and articles on a spectrum of topics of various security and geoplitical issues that caught our attention. Some articles are accompanied by a short comment – not always a polite/civilized one. Through life I prefered to say things by their name and if something is good to say "bravo" and if it is wrong to say "are you serious?" or "it is wrong"! From a diplomatic point of few there is nothing more stupid than this! I know; you know! But if I had the charisma I would be one of them, not a CBRNe first responder and an officer (and a gentleman)!

There are some new collaboration is place and some new projects abroad that are very interesting and might boost our defenses against CBRN threats. New Year will also be devoted to the effort to introduce the module of "CBRNe Medicine" into the curriculum of university medical and nurse schools in an effort to enhance the differential capabilities of new front-line health professionals that one day might look the enemy in the eyes during their shift at the emergency department of their hospital. Basically it is an effort to transfuse a CBRN security culture in the hospital sector that stubornly prefer to think that it will not happen to them! Well, we all know that bad things happen out of nowhere whether it is a tsunami during a concert in Indonesia, an earthquake, a nuclear power plant accident in a neighboring country, a meteor fall in Russia, an indistrial accident in France or a sarin release in Tokyo metro system. And we do want to see the same surprised faces in our TVs stating that it was too big, too sudden or too exotic!

It will be a very interesting year and it is in our hands to make it peaceful and fruitfull! Remember that you all belong to the "very few and the brave"!

The Editor-in-Chief

Migration and Terrorism: A New Approach to Consider the Threat

By Orlando Cenciarelli[1], Sandro Mancinelli[2], Gian Marco Ludovici[3] and Leonardo Palombi[2]

[1] Department of Industrial EngineeringUniversity of Rome Tor VergataRomeItaly

[2] Department of Biomedicine and Prevention, School of Medicine and SurgeryUniversity of Rome Tor VergataRomeItaly

[3] International Master Courses in Protection Against CBRNe EventsUniversity of Rome Tor VergataRomeItaly

Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges pp 277-287 [First Online: 01 November 2017]

Source: https://link.springer.com/chapter/10.1007/978-3-319-62108-1_13

Abstract

Migration is part of human history since ancient times; this phenomenon can result from several reasons, through which are delivered, as well as individuals, the main characteristics of the societies of origin. Currently, several theories relate the spread of international terrorism with migration, particularly by supporting the close relationship between migration, religious extremism and terrorist events. Other literature considers terrorism as a phenomenon with characteristics similar to a disease, for many common aspects with specific illness, such as cancer or psychiatric pathologies. In this review, the correlations between migration and terrorism are analyzed and the different theories that consider terrorism similar to a disease are considered.

The Terrorist Threat After ISIS is Here

By Dr. Erroll G. Southers

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/terrorist-threat-after-isis-is-here/

Members of the KKK march down Pennsylvania Avenue in Washington, D.C., in 1927. (FBI photo)

February 2018 – Many Americans, including those in leadership positions, believe the dominant terrorist threat to the United States originates abroad and is motivated by an extremist interpretation of Islam. They're wrong. The narrative that posits terrorism is primarily a tactic of foreign-born extremist Muslims is woefully and dangerously incomplete. It's time to get our facts straight.

White supremacist groups are growing in size, lethality and capability

While the United States spent more than a decade disrupting terrorist organizations abroad, a different threat was growing here at home. Its ambitions were different, but its tactics increasingly mirrored those being used by our adversaries in al-Qaeda, ISIS and other groups. This should not come as a surprise.

In 2009, a Department of Homeland Security (DHS) Intelligence and Analysis (I&A) Directorate report, "Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment," held up a mirror to America that didn't fit the common narrative (i.e., terrorism is purely a tactic of extremist Muslims). The report found that economic hardship, the election of the first African-American president, and the volume of veterans returning from foreign wars (who could be targeted for radicalization and recruitment) were coalescing into a troubling picture of right-wing extremism in America.

The assessment determined that right-wing extremists were leveraging what I refer to as "the Obama effect." The election of the first African-American president with a Muslim father fueled right-wing recruiting and mobilizing efforts. The white supremacist website Stormfront, for example, received such an onslaught of Internet traffic on the night of Barack Obama's election that the website crashed. Further proof of what was to come: on that same historic night, one in every 100 Google searches that including the word "Obama" also included search terms for "KKK" or the N-word.

Nevertheless, when the I&A report was released, the backlash was overwhelming, driven primarily by the report's finding that veterans would be attractive for right-wing recruiting and radicalization efforts. The notion that an American military member could become an extremist was unthinkable, even offensive to their service. But the subtext to this negative public reaction revealed a deeper national challenge. We wanted our adversary to be foreign and Muslim. Clear demographic and religious lines bring a sense of comfort, reinforcing the "otherism" narrative that tomorrow's attacker inevitably hails from another country, another nationality, and another religion.

The facts were clear as day, delivered by dedicated professionals working at the one federal department purely focused on guarding against threats manmade and natural. These were *the* experts delivering definitive analysis. But America wasn't ready to accept the truth.

Designating an attack as a hate crime obscures a clear view of the threat environment

One reason the public overall (including federal, state and local leaders) struggles to appreciate the scope of the right-wing extremist violence is that it is inconsistently prosecuted as a hate crime and almost never prosecuted as an act or attempted act of terrorism, a situation enabled by the legislative fact that terrorist prosecution often requires the attacker's motivation to be in furtherance of a *foreign* terrorist organization or ideology.

For decades, the security community has wrestled over how to define terrorism. There is still no agreement. The government agencies responsible for counterterrorism or terrorism investigations all use slightly different definitions of the acts they seek to prevent. There are, however, three elements to terrorism on which American agencies agree: the essence of the activity is violence; the targets are civilians (which in the U.S. context arguably includes law enforcement officers); and the objective is political (broadly) or ideological in nature.

These three qualities are apparent in scores of attacks perpetrated by non-Muslim, American-born extremists. Yet most acts of right-wing extremist violence escape public knowledge or mention when they are designated hate crimes or, worse, are quickly dismissed under the banner of mental illness, typically diagnosed *despite* any immediately available medical history.

By this, there are numerous attackers who have escaped the terrorist label, even as it perfectly aligns with their violence and extremist ideologies. Making matters more complicated is that hate crime statistics are typically flawed: bias and criminal motivation are not always easy to determine. What is more, victims and law enforcement underreport

such crimes. (Note: We are beginning to see some movement toward prosecuting domestic terrorists as terrorists, such as the case of white supremacist Taylor Wilson who was charged with terrorism in federal court in Nebraska after attempting to derail a cross-country Amtrak train.)

The data on right-wing extremist violence are sobering. A recent study of domestic terrorism incidents from 2008 to 2016 identified 194 cases of executed and/or foiled terrorist acts. These included:

- **63 cases of extremist Muslim terrorism, defined as incidents motivated by the political ideology espoused by groups such as ISIS and al Qaeda; 76 percent of those plots were foiled.**
- **115 cases of right-wing terrorism, involving deaths, injuries or property damage; only a little more than one-third of those plots were foiled.**
- **Left-wing incidents totaled 19, causing seven fatalities.**

Total deaths associated with extremist Muslim incidents were higher, mostly attributed to the attack at Fort Hood in Texas. While more people were murdered in Muslim Identity attacks, right-wing terrorist attacks were independently more lethal. Almost one-third of right-wing incidents resulted in fatalities, while 13 percent of the extremist Muslim incidents resulted in deaths. It is important to note that 48 percent of the foiled extremist Muslim incidents were the target of sting operations, this compared to right-wing attacks (12 percent) or far-left attacks (10.5 percent).

The lesson in these figures is that right-wing extremist attacks are more likely to kill people, they are less likely to be foiled, and if they are foiled, only about one in 10 is due to a purposeful sting operation. The rest, presumably, were due more to luck or an aware, engaged public ready to report dangerous behavior. This is not an adequate approach to a growing homeland security threat.

White-supremacist groups use recruiting strategies employed by foreign extremist groups (e.g., ISIS)

Right-wing groups are excellent students of ISIS and groups like it. There are currently highly organized efforts to draw new members into the right-wing extremist fold. A 2016 George Washington University Program on Extremism study, "Nazis vs. ISIS on Twitter," offers a startling insight: since 2012, American white nationalist movement Twitter accounts have seen followers grow more than 600 percent. The report states: "Today, they outperform ISIS in nearly every social metric, from follower counts to tweets per day."

The right-wing objective is to leverage online capability to facilitate greater outreach and eliminate the need for physical meetings, thereby increasing operational security. The proof of this is the August 2017 "Unite the Right" rally in Charlottesville, Va. ProPublica reported that white supremacists planning the rally joked about using vehicles to run over their adversaries—which is precisely what a white supremacist did as the protest and counter-protest were dispersing.

That message and thousands more shared among white supremacists were leaked from a chat room app (Discord) and posted to the website of a left-wing media collective identified as Unicorn Riot. It revealed that white supremacist groups devoted months to tracking potential Charlottesville counter-protesters online, infiltrated counter-protest meetings, and posted and shared their identities with law enforcement as likely troublemakers. This is the level of organization and dedication driving the white supremacist movement toward increasing instances of terrorism.

Charlottesville was a seminal event, galvanizing white supremacist and other extreme right-wing groups, which is a rare occurrence. White supremacist groups typically despise groups of similar ideology. Not so in Charlottesville. It should be a clear wake-up call to public safety professionals, lawmakers and leaders across the country. Intelligence reveals these traditionally fractured groups are mirroring al-Qaeda-to-ISIS organizational evolutionary designs. They are becoming highly adaptable and cohesive.

What does the future look like? Not good. This is an increasing threat that is insufficiently addressed, and particularly in the current political and rhetorical environment (whatever one's leanings), groups that once stuck

to the shadows are increasingly present in the public eye.

Case in point, the Southern California-based "Rise Above Movement" (RAM). This group is composed of a number of convicted felons and offers no illusion about their intentions—they train to fight, post their assaults online, travel to events in other states, and are fearless in the face of authority.

Troublingly, and for reasons yet-to-be determined, some violent incidents are reportedly being ignored by law enforcement. Four violent attacks documented by ProPublica resulted in one arrest, and charges were never filed in that case. They reported that law enforcement officials in Charlottesville, Huntington Beach, San Bernardino and Berkeley (jurisdictions with video evidence of RAM's violent activities) either refused to discuss the group or lamented they had insufficient resources to conduct an investigation. This is not to cast conspiracy on Southern California law enforcement. Rather, it is plain evidence that the right-wing threat is continuing to metastasize and, at least in some jurisdictions, it is not even receiving investigation, much less a focused public safety response to what is clearly a terrorist threat.

As security professionals, we are continually thinking of the next threat, the one over the horizon we have failed to imagine. In our current environment, imagination is unnecessary. The next terrorist threat is marching in the streets, waving flags and proclaiming an ideology that posits the moral superiority of one group over another. We have seen this in cities in Syria, Iraq and elsewhere; we know where it leads. It is far past time to orient our security apparatus to address this obvious threat within our borders.

Dr. Erroll G. Southers *is an internationally recognized expert on counterterrorism, public safety, infrastructure protection, and homeland security. He is the Director of the Safe Communities Institute at the University of Southern California, where he is also a Professor of the Practice of Governance. Dr. Southers is also the Managing Director for Counter-Terrorism & Infrastructure Protection at TAL Global, an international security consulting firm. Previously, Dr. Southers served as the Associate Director of the National Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE). He has also served as: California Governor Arnold Schwarzenegger's Deputy Director in the California Office of Homeland Security; Chief of Homeland Security and Intelligence for the Los Angeles World Airports Police Department (the nation's largest airport police department); and President Barack Obama's first nominee for Assistant Secretary of the Transportation Security Administration.*

Qatar's Cabinet gives the nod to a draft law to check money laundering, terror funding

Source: https://www.qatarliving.com/forum/news/posts/qatar%E2%80%99s-cabinet-gives-nod-draft-law-check-money-laundering%C2%A0terror-funding

Dec 27 – Qatar has been doing a lot to ensure that money from the country is not laundered and used for the funding of terror.

A few months back, it signed a **Memorandum of Understanding with the USA** to ensure this does not happen. And now, Qatar's cabinet has given its formal approval to a draft law on Anti-Money Laundering and Countering the Financing of Terrorism, reported *Gulf Times*.

The draft law will replace Law No 4 of 2010, in light of modernization of international standards on the same. It will enable financial institutions and competent authorities to deal effectively with financial crimes, thus protecting the economic system from exploitation by criminal elements.

Qatar's Prime Minister and Interior Minister HE Sheikh Abdullah bin Nasser bin Khalifa Al Thani chaired the Cabinet's regular meeting at the Amiri Diwan yesterday.

The Cabinet also approved a draft law on preventive measures against animal-originated infectious and epidemiological diseases in the GCC countries. The Cabinet considered several other issues took appropriate decisions.

Greece: Massive increase of attacks on Christian symbols and Orthodox churches

Source: https://voiceofeurope.com/2018/12/greece-massive-increase-of-attacks-on-christian-symbols-and-orthodox-churches/

Dec 22 – Each year there are more attacks on churches, chapels, atypical places of religious worship, religious monuments, synagogues and even cemeteries, Greek newspaper Eleftheros Typos reports.
Specifically, according to the Greek Secretariat of Religions, **last year the attacks on religious buildings (includes vandalism, burglaries, thefts, sacrifices, fires, etc.) rose by 159 per cent, while the primary target appears to be the Orthodox Church.**
A significant increase is also seen in the number of attacks to several religious communities, with four of them registered in 2016, whilst last year that number was eight.
The numbers speak for themselves. In 2017 a total of 556 incidents were recorded against place of religious worship, 536 of those attacks made in Christian places.
In particular, according to the relevant report of the General Secretariat of Religions, 525 cases against the Orthodox Church (94 per cent of the total incidents), many of which bear religious intolerance causing intense reflection within the Greek Church.
"Evidence shows that the primary target of the attacks in our homeland is the Orthodox Church. This fact cannot be overlooked. We owe the State and the Church to seek ways of cooperation so that this profane reality that affects our history and identity is eliminated," says Secretary General of Religions, Giorgos Kalantzis.

Greece has experienced an unprecedented wave of migrants from the Middle East, of which several are ISIS members and completely intolerable against people or symbols of other beliefs. At the same time the leftish government seems unable (or unwilling) to deal effectively with the Anarchist criminality in Greece, which is responsible for most of the attacks on Orthodox churches.

EDITOR'S COMMENT: I was wondering what would be the response of both governments and citizens in S Arabia, Pakistan, UAE, Qatar, Indonesia, Turkey or Iran in case similar actions against mosques and other holly/worship places were recorded in their countries. OK, you got me! I was joking! I do know what they would do! And I applause them! I will always remember a sign on the wall just after passing passport control at Abu Dhabi International Airport saying "*You are now in the Emirates; behave like an Emirati*!"

Hannover Airport incident: Drug driver smashes through fence 'to chase plane which had just landed'

Source: https://www.standard.co.uk/news/world/hannover-airport-incident-flights-suspended-as-man-tries-to-drive-onto-tarmac-near-runway-a4026976.html

Dec 29 – A man sparked a major security alert at Germany's Hannover Airport on Saturday after he drove through a fence and reportedly tried to chase a plane which had just landed.
The Hannoversche Allgemeine newspaper reported the man smashed through a perimeter fence and tried to pursue an Aegean Airlines plane which had just landed from Athens.
Hannover Police said it managed to stop the car after it drove onto the airport's apron area, where planes are parked. The force said officers then "overpowered" the driver.
The man, in his mid-20s, was driving a silver BMW with Polish licence plates. Police said he tested positive for amphetamines and cocaine.
Officers said the man's motive was unclear. There was no indication he had an extremist history, or that the incident was terror-related. It's thought he acted alone.

The security scare forced flights to be suspended for four hours as bomb disposal experts examined the car, which police described as a routine measure.
It was found not to have any "dangerous items", with flights eventually resuming just after 8pm local time. Take-offs as well as landings had been suspended while the incident was investigated, though the airport's terminals remained open.
No one was hurt in the drama. Police were seeking more information about the driver, who wasn't carrying an ID card.

EDITOR'S COMMENT: I am commenting not because the airplane was a Greek Aegean Airlines carrier but because the gap in Hannover's airport security is huge. Imagine some alternatives: the car crash on the landing gear of the plane; the car is a VBIED that is exploding when near the plane; the car explodes outside or under the departure gates during busy hours; the car approaches the moving corridor leading to a plane and the crew hijacks the plane on the ground and a few more. One more time, those responsible for the security of the airport and traveling people failed to think as terrorists. They thought that a fence can always keep the evil out. But again, their inability proved wrong – no victims this time, but with a potential for an hetacombe!

Nine injured by car ramming in Tokyo's trendy Harajuku district on New Year's Eve

Source: https://www.news.com.au/world/pacific/nine-injured-by-car-ramming-in-tokyos-trendy-harajuku-district-on-new-years-eve/news-story/6550afa1986b396692e599763e0b4e80

Jan 01 – Nine people were hurt, one seriously, when a man deliberately ploughed his car into crowds celebrating New Year's Eve along a famous Tokyo street, police and media said Tuesday.
With an "intent to murder", 21-year-old Kazuhiro Kusakabe drove a small vehicle into Takeshita Street in Tokyo's fashion district of Harajuku at 10 minutes past midnight, a police spokesman told AFP.
According to national broadcaster NHK, Kusakabe told police **he was acting in "retribution for the death penalty"** without giving more precise details.

NHK footage showed a small box vehicle with a smashed front and paramedics carrying people on stretchers into ambulances.
One witness told NHK it was a "ghastly scene."
"I saw some guys collapsed on the street. As I walked closer toward the scene, many more people had fallen on the ground. By the time I reached the exact place, paramedics were already there helping people," he said.

Another witness who runs a clothing shop in the area said: "I am shocked that something like this happened on Takeshita Street."
Police immediately cordoned off the street, which was packed with people celebrating the New Year.
One college student suffered serious injuries during the attack and was undergoing surgery, the police spokesman told AFP.
Kusakabe was arrested on suspicion of attempted murder, police said.
According to local media, Kusakabe hit a total of eight people and assaulted another on the street, which was closed to car traffic at the time as revellers packed the area to celebrate New Year.
Takeshita Street is packed with small shops and is considered the centre of youth culture and fashion in Japan, attracting tens of thousands of international tourists every day.
Unlike in other major cities, New Year in Tokyo is a relatively muted affair. There are no major fireworks display and no central point where drunken revellers gather to see in the New Year. Instead, Japanese people tend to see in the New Year with families and quietly go to the shrine to pray for good fortune in the year to come.

EDITOR'S COMMENT: The first thing that came into mind was the execution of Aum Shirinkyo back in 2018. Could he be a fanatic member of his cult seeking revenge? Is he a lonely wolf? And all that one year before the Olympic Games.

2019 Annual Forecast

Source: https://worldview.stratfor.com/article/2019-annual-forecast-geopolitics-intelligence-global-risk

The Great Power Competition Intensifies
The United States will escalate its strategic offensive against China with tariffs, sanctions, regulatory buffers around emerging technologies, stronger backing for Taiwan and a more assertive posture in the South China Sea. At the same time, failing arms control pacts will accelerate an arms race among the United States, Russia and China. The edgier geopolitical climate will create strategic opportunities for more vulnerable borderland powers, such as Poland and Taiwan, but will also create massive headaches for middle powers trying to find neutral ground, such as Turkey, India and Vietnam.

Stratfor | WORLDVIEW™

Increased Geopolitical Risk for Business
Citing national security threats, the United States will lean heavily on Europe, Japan, Australia, Canada, South Korea and Taiwan to erect stronger barriers to Chinese investment. This will affect research and trade in strategic areas, from artificial intelligence to 5G network rollouts beginning in 2019. China's imperative to catch up in critical areas like aerospace and high-end semiconductor development will only increase cyberthreats to corporations and compel an overall more offensive U.S. policy in cyberspace. In addition, corporations will have to contend with supply chain disruptions and heavier fines and lawsuits for data breaches.

Measuring Trade Volatility in the Global Economy

A U.S. showdown with the World Trade Organization could paralyze the body's dispute settlement process, forcing countries into a less predictable bilateral track to resolve their trade differences. Canada, Mexico, Japan and South Korea have a better chance of negotiating quotas to mitigate the threat of U.S. auto tariffs, but the European Union's trade talks with the United States are doomed to fail. And while additional U.S. tariffs on China will add to trade uncertainty, the overall effect on the global economy from White House trade policy in 2019 will be relatively muted.

Hair-Raising Scenarios for Italy and Brexit

A defiantly populist Italian government will pose the biggest threat to the eurozone in 2019 as concerns grow over the country's rising debt levels and fragile banking sector. Financial markets and dangerously wide spreads in bond yields — rather than threats from Brussels — will prove to be Rome's biggest disciplinarians. Brussels will simultaneously work to avert a no-deal Brexit scenario with the United Kingdom, but a British parliamentary veto remains the single biggest obstacle to its orderly exit from the European Union.

The Next Steps in the Anti-Iran Campaign

With far-reaching secondary sanctions in place, the United States will forge ahead with its campaign to isolate Iran regionally and weaken the country from within. This will increase friction between Washington and Tehran and diminish the already scant likelihood of a constructive negotiation. A common agenda opposing Iran will help insulate strategic, high-level ties between the United States and Saudi Arabia despite rumblings within the royal family and foreign governments over Saudi Crown Prince Mohammed bin Salman's leadership.

An Eye on Growing Supply in Global Energy Markets

Saudi Arabia and Russia will carefully manage oil output to prevent a price plunge as they monitor the effects of residual Iranian exports on the market. There is also the potential for production growth out of Iraq and Libya and a significant easing of export capacity constraints on the United States later in the year. Global liquified natural gas markets will be shaken up when the United States assumes its place among the top three LNG exporters in the world in 2019.

Disruptive Forces at Work in the Americas

Hard-line and U.S.-aligned governments in Brazil and Colombia could drive an atypically proactive regional effort to contain spillover from Venezuela's ongoing crisis. Brazil's efforts to shake up and reform the Mercosur trading bloc will come up against a politically hamstrung

Argentina. The power of the referendum will meanwhile be put to the test in Mexico, where an aggressive populist agenda will raise investor risk.

Ethiopia Drives Big Change in the Horn of Africa
Ethiopia's ambitious agenda is generating economic interest and attracting outside powers to the Horn of Africa. But internal challenges to the current leadership and ethnic strife risk slowing Addis Ababa's momentum.

Manchester, U.K. knife attacks treated as an act of terrorism

Source: http://www.homelandsecuritynewswire.com/dr20181231-manchester-u-k-knife-attacks-treated-as-an-act-of-terrorism

Dec 31 – Manchester, U.K. police said Tuesday they are treating the New Year's Eve stabbing of three people as a terrorist incident.

Greater Manchester Chief Constable Ian Hopkins said two people suffered "very serious" injuries in the attack and remain in the hospital receiving treatment. A police sergeant who was stabbed in the shoulder has been released.

Police have not yet identified or charged the suspect, who has been arrested on suspicion of attempted murder. An eyewitness said he shouted Islamic slogans — "Allah" and "long live the Caliphate" — during the frenzied attack.

The *Independent* reports that the incident happened at Manchester's Victoria Station shortly before 9 p.m. on New Year's Eve. The busy rail station is next to the Manchester Arena, where a suicide bomber killed 22 people at an Ariana Grande concert in 2017.

Police tried to reassure the public that the area is safe despite the attack on a night of celebration.

"I know that the events of last night will have affected many people and caused concern," Hopkins said. "That the incident happened so close to the scene of the terrorist attack on 22 May 2017, makes it even more dreadful."

Prime Minister Theresa May expressed concern for the victims and thanked first responders for their "courageous response."

Police say there is no indication that others were involved in planning or carrying out the attack. The investigation is being led by Britain's counterterrorism police. Assistant Chief Constable Rob Potts said the incident is "not ongoing" and there is "currently no intelligence to suggest that there is any wider threat." Police say extra officers will be on the streets Tuesday

.

Britain's official threat level has long been set at "severe," indicating intelligence analysts believe an attack is highly likely.

The New Face of Terrorism in 2019

Forget the Middle East—it's time to prepare for attacks from the former Soviet Union.

By Vera Mironova

Source: https://foreignpolicy.com/2019/01/01/the-new-face-of-terrorism-in-2019/

Jan 01 – The way Westerners think about Islamist terrorism has grown dangerously outdated. For decades, officials have focused on attacks launched by Middle Easterners. Today, however, the real threat increasingly comes from further east. In the former Soviet states and beyond, militants who once harbored mostly local grievances are turning their attention to the West. They will be the menace to watch in 2019.

The threat posed by Middle Eastern terrorists has been shrinking for some time. Even during the war against the Islamic State, Russian speakers from former Soviet countries were already committing many of the major attacks in the West. Those included relatively simple lone-wolf events, such as the 2017 truck strikes on pedestrians in New York and Stockholm—both conducted by Uzbeks—but also more complicated operations, such as the

2016 suicide bombing of Istanbul's airport—which was allegedly organized by a Russian national—and the 2017 attack on a nightclub in the same city, led by an Uzbek.

There are several reasons for the relative increase in anti-Western terrorism coming out of the post-Soviet world. For starters, in recent years Middle Eastern jihadis have been too preoccupied with local conflicts in Iraq, Syria, and Yemen to head elsewhere. The pull of the Islamic State, meanwhile, has faded after its almost total defeat in Iraq and Syria.

At the same time, the wars in the Middle East have transformed militants from Russian-speaking areas, who previously focused on fighting repressive governments at home, into global terrorists. By 2017, at least 8,500 fighters from former Soviet republics had flocked to Syria and Iraq to join the Islamic State. That experience gave many of these jihadis their first taste battling U.S. and NATO troops, and it left them looking for vengeance, convinced that future operations should be aimed at the West.

Ahmed Chataev, for example, who allegedly organized the attack on Istanbul's airport, apparently first cooked up plans to strike Western targets while fighting in Iraq and Syria. A phone conversation leaked last year between Chataev and another Russian-speaking terrorist, Islam Atabiev, revealed that the two were planning to collect intelligence on several U.S. consulates and restaurants popular with Americans in Turkey and Georgia.

The same dynamic has played out further east, where battle-tested jihadis from the post-Soviet world can travel far more easily than Arabs who hold Iraqi, Syrian, or Yemeni passports.

The same dynamic has played out further east, where battle-tested jihadis from the post-Soviet world can travel far more easily than Arabs who hold Iraqi, Syrian, or Yemeni passports.

As the persecution of Muslims in Asia grows, so do opportunities for grievances to turn international. When I was in Bangladesh in July 2018, I came across at least two separate groups from the Caucasus providing religious aid in Muslim Rohingya refugee camps. A leader of a Russian-speaking group affiliated with militants in Syria said he had likewise planned to send some of his people to Bangladesh. Such contact could boost the capabilities of local jihadis already conducting anti-Western operations in the area, including those who in 2016 stormed a bakery in Dhaka that was popular with expats. And it may win more Rohingya over to the idea that they're involved in a global struggle for Islam, not just a local fight for their own survival.

In the coming years, the terrorist threat from Russia and beyond will only increase. With the fall of the Islamic State, Russian-speaking terrorists were mostly able to flee Iraq and Syria with more ease than Middle Eastern foreign fighters and are now back in hiding in the former Soviet sphere or in Europe. Having escaped the reach of the U.S. military, they may find it easier to bring their plots to fruition. Local sympathies will help. Government neglect and

outright repression have made religious Muslims in Kazakhstan, Tajikistan, and Uzbekistan attractive targets for radicals looking for new recruits. Several popular sheikhs from the Middle East, including the Saudi cleric Abdulaziz al-Tarefe, now have significant Russian- and Arabic-language followings on social media.

As the locus of terrorism changes, the United States and its allies will have to update their strategies for fighting it. Over the last two decades, Washington built up a huge bureaucracy around Middle Eastern terrorism. Untold millions of dollars were poured into finding and training Arabic-speaking researchers and analysts. According to data from a critical language scholarship program run by the U.S. government, out of 550 university students who will be admitted in 2019, 105 will be studying Arabic and only 60 Russian. And according to professors with whom I've spoken—from top policy schools such as the Harvard Kennedy School, Johns Hopkins School of Advanced International Studies, and Texas A&M's Bush School of Government and Public Service—the overwhelming majority of college students who plan to work in counterterrorism still minor in Middle Eastern studies or Arabic. There's also a dearth of experts who've specialized in Central Asia and can teach a new generation of analysts.

Reorienting the West's focus will also involve political challenges, since the United States will have to find a way to cooperate with Russia and its neighbors. Over the last several years, for example, U.S. companies have gotten good at deleting jihadi propaganda from U.S.-based social media platforms, but the same propaganda is still widely available on Russian-language apps such as VK and OK, which are popular across post-Soviet states. Telegram, which was founded by a Russian national, has likewise become a major communications tool for terrorists of all backgrounds, and cell phones captured from the Islamic State revealed that they were operating on Ukrainian SIM cards.

Monitoring these systems and others will require deep cooperation and intelligence sharing with Russia. But such cooperation does not seem likely in the immediate future. There may simply be too much animosity between Washington and Moscow to allow for effective collaboration. There's also the problem of the quality of intelligence. Many of those who end up on domestic terrorist watchlists and even Interpol lists throughout the region are actually members of the domestic opposition. Meanwhile, lots of known terrorists are never singled out: Russia is well-known for providing passports to radicals from the Caucasus on the grounds that letting would-be jihadis leave the country is easier than dealing with them at home.

Russia is well-known for providing passports to radicals from the Caucasus on the grounds that letting would-be jihadis leave the country is easier than dealing with them at home.

Intelligence from the region has become so politicized—and is used so much more often to violate the human rights of religious citizens than to stop real terrorist attacks—that it is hard to know what the United States would do with it.

The West should have recognized this shift long ago. It didn't, but that doesn't mean that it should sit on its hands now. The United States and its allies need to recognize that future attacks are more likely to come from the East than the Middle East and that there is no other option than to cooperate with Russia and its neighbors to stop them. If the United States fails to do so, it could soon see the effects in either a surge of attacks on the United States or the rise of a new post-Soviet-dominated terrorist group in one of the world's many war zones

Vera Mironova *is a visiting scholar in the Harvard University economics department.*

EDITOR'S COMMENT: Why the new threat is coming mainly from the former USSR countries (and not Russia as the subtitle emphatically implies) and not from EU countries that face the same problem with returning fighters and uncontrolled illegal immigration? Author's last name is common in Russia, Ukraine, Belarus and Moldova and the fact that she is a Harvard scolar might bias the objective

analysis of the terrorism threat in the years to follow. And would have been of interest to analyze the background of "war zones" mentioned in the last sentence of this article.

Best Military Technology Innovations of 2018

Source: https://i-hls.com/archives/87887

Jan 01 – Many leading military technology advances have been achieved during 2018. US Army scientists and army sponsored researches have succeeded in developing intriguing technologies supporting the soldier of the future. Dr. Alexander Kott, Chief Scientist of the RDECOM Research Laboratory, the Army's corporate research laboratory (ARL), which focuses on innovation to ensure dominant strategic land power, handpicked the "coolest" advances in 2018, according to military.com:

Number 10: Transporting quantum information with minimum distortions

Future American soldiers will rely on powerful quantum computers and sensors. They'll need to communicate this quantum information through what's known as entanglement. Army scientists who published their findings in the journal Nature discovered how two separated photons can now stay entangled without distortion.

As a traveling photon hurtles through the air or optical fiber, entanglement gets distorted. Now, army scientists found a way to restore the entanglement of the traveling photon by manipulating the one that stayed local. They say this is a big step on the road to ultra-secure battlefield communications.

Number 9: Atomic antenna for faster communication

Army scientists are developing a new quantum antenna using atoms excited to unusually high energy levels. A research effort which is underway seeks to equip future Soldiers with more accurate sensors that operate with less background noise. A new quantum receiver may allow future Soldiers to perform parallel, fast communications with miniature quantum receivers. This research was published in Applied Physics Letters.

Number 8: The future of computing

By mimicking brain functions in computing, researchers opened a new solution space that moves away from traditional computing architectures and towards devices that are able to operate within extreme size-, weight-, and power-constrained environments.

A research team devised a way to factor large integers by harnessing the massive parallelism of novel computers that mimic the functioning of the mammalian brain. These neuromorphic computers operate under vastly different principles than conventional computers. This advance may help future Army computing devices rapidly solve extremely complex problems in the field conditions where power and connectivity are limited.

Number 7: Alternative jet fuel

A new information will help design of future gas turbine combustors that may operate on alternative jet fuels, and to develop engines with higher power density and efficiency.

Previously it was impossible to image and measure the atomization process in a gas turbine combustor. Now, for the first time ever, Army scientists discovered a way to do this with an experiment.

Number 6: Helicopter blades tech stops attacks of sand

A thermal barrier material coats turbine blades of Army helicopter engines, and keeps the blades from overheating. Unfortunately, in places like the desert, tiny particles of sand get into a turbine engine, melting and sticking to the coating. A lot of dust particles blow out, especially during hovering.

The laboratory's Vehicle Technology Directorate scientists created a new material that rejects the sand particles. With this extra protection, the blades survive far longer and Army helicopters keep flying and fighting.

Number 5: Projectiles get extra strength
Army scientists created a nanocrystalline alloy of copper and tantalum with grains of an average size of about 50 nanometers, arranged into clusters. This helps it maintain an exceptionally high and consistent level of mechanical strength and microstructure stability, withstanding extreme impact and temperature, such as in the case of projectiles or armor. This new super strong alloy doubles the material's strength and stability, making it immune to the deformation response. The research was published by the journal Nature.

Number 4: Animal-inspired technology to maximize kinetic energy
In the future, jumping robots may collect battlefield intelligence while remaining unnoticed. Biological systems, for example a grasshopper, to jump incredibly fast and far for its size. Such systems amplify the maximum throwing power of a limb by storing the energy in a bow or sling shot with a latch mechanism for sudden release. A research found applications for these biological principles that are common to animals, plants, fungi and machines that use elastic structures to maximize kinetic energy. The research was published in the journal Science.

Number 3: New and powerful explosive

A new explosive called BODN is 50 percent more powerful than today's most common explosive TNT. Energetic materials can be notoriously unstable and prone to explode. BODN includes molecular features that make it stable. Unlike TNT, BODN is non-toxic. But like TNT, it is easy to melt for manufacturing of artillery shells. Researchers also developed a cost-effective synthesis process for the production of BODN.

Number 2: Human-in-the-loop machine learning
Army scientists have developed new human-in-the-loop machine learning techniques for robots or computer programs to learn faster and with significantly less data how to perform tasks by interacting with a human instructor. The instructor can teach artificial agents in a variety of ways, including demonstration, real-time intervention, and real-time evaluative feedback. Agents using the new algorithms, called Deep TAMER and Cycle-of-Learning, can effectively interpret the instructor's actions and very quickly learn how to perform new tasks in new environments.

Number 1: Alternative energy sources
The nucleus of an atom can store tremendous energies. Army researchers and their multinational partners found a new, safe phenomena to release energy from an atom's nucleus in a controlled manner. This technique, which is not a nuclear reaction, was never demonstrated experimentally before.
The researchers arranged electrons at just the right speeds to be captured by atoms, tickling their nuclei to release energy. This significant scientific achievement, published in the journal Nature, marks a step in the Army's quest to find and access alternative energy sources. Applications may include the capability of harvesting thousands of times the energy of conventional batteries — and that might power the future Army.

GAO: Federal Agencies Falling Short on Physical Access Control Security

Source: https://www.hstoday.us/industry/latest-from-gao/gao-federal-agencies-falling-short-on-physical-access-control-security/

Dec 22 – The Government Accountability Office (GAO) was asked to examine physical access security at federal buildings. Its December 20 report highlights the oversight

difficulties faced by agencies when ensuring physical access control is properly implemented.
A 2004 federal directive and the related standard set forth a vision for using information technology to verify the identity of individuals accessing federal buildings. The vision calls for secure and reliable forms of identification that work in conjunction with access control systems. Interoperability of these systems across departments and agencies is part of the vision. The Office of Management and Budget (OMB) and the General Services Administration (GSA) have government-wide responsibilities related to this effort. The Interagency Security Committee (ISC) provides guidance to non-military executive branch agencies on physical security issues.
For its review, GAO analyzed documents from Commerce, GSA, ISC, and OMB. GAO selected five non-military agencies based on factors including number of buildings and geographic location. GAO reviewed relevant requirements and key practices. GAO also interviewed federal agency officials, physical access control vendors, and knowledgeable industry officials.
GAO found that OMB and GSA have taken steps to help agencies procure and implement secure, interoperable, GSA-approved physical access control systems (PACS) for federal buildings. PACS are systems for managing access to controlled areas within buildings. PACS include identification cards, card readers, and other technology that electronically confirm employees' and contractors' identities and validate their access to facilities.
OMB issued several memos to clarify agencies' responsibilities. For example, OMB issued a 2011 memo citing Department of Homeland Security (DHS) guidance that agencies must upgrade existing PACS to use identity credentials before using relevant funds for other activities. However, GAO found OMB's oversight efforts are hampered because it lacks baseline data on agencies' implementation of PACS. Without such data, GAO says OMB cannot meet its responsibility to ensure agencies adhere to PACS requirements or track progress in implementing federal PACS requirements and achieving the vision of secure, interoperable systems across agencies.
GSA developed an Approved Products List that identifies products that meet federal requirements through a testing and evaluation program. Federal agencies are required to use the Approved Products List to procure PACS equipment. In addition, GSA manages IDManagement.gov, which guides federal agencies through the process of identifying Approved Products List-compliant physical access control system equipment.
GSA also established the U.S. Access program to enable federal civilian agencies to issue common HSPD-12 approved credentials to their employees and contractors. Finally, GSA developed a list of system integrators that can be used to install physical access control systems that have been approved for the Approved Products List. These integrators are listed on the GSA's IDManagement.gov website.
Officials from the five selected agencies that GAO reviewed identified a number of challenges relating to PACS implementation including cost, lack of clarity on how to procure equipment, and difficulty adding new PACS equipment to legacy systems. Officials from OMB, GSA, and industry not only confirmed that these challenges exist but also told GAO that they were most likely present across the federal government.
Officials from four of the five selected agencies we reviewed told GAO that, since 2013, when physical access control system end-to-end testing requirements began, they had only purchased GSA-approved physical access control system equipment for a limited number of their facilities.
According to Environmental Protection Agency (EPA) officials, none of EPA's 72 facilities (including, for example, its headquarters building in the District of Columbia and 10 regional headquarters buildings) currently adhere to the latest physical access control system requirements. EPA officials told GAO that the agency used GSA's Approved Products List to purchase physical access control system equipment in the past. However, because requirements have changed over time, the 72 buildings where EPA is responsible for physical access control need to be upgraded to the latest requirements. EPA will procure these required systems using the Approved Products List and prioritize implementation to those facilities with the highest assessed risk.
According to TSA officials, since 2013, 64 TSA facilities have implemented some physical access control system upgrades using products from the Approved Products List, while an additional 75 leased facilities have been upgraded by GSA.

While the 139 facilities are not fully compliant, the only item missing to make these facilities compliant, according to TSA officials, is the capability for interoperable, secure identification checks among federal agencies. This would allow TSA's physical access control systems to recognize revoked personal identity verifications from any federal agency. TSA told GAO that it plans to roll out this capability in fiscal year 2019. **Over the next five years, TSA plans to spend about $73 million in physical access control system implementation with the bulk of these funds ($51 million) going toward the acquisition of new systems from the Approved Products List.**

Coast Guard officials told GAO that none of the agency's 1,400 facilities where it has security responsibilities fully adhere to the latest federal physical access control system requirements. However, 53 of these facilities have been prioritized for physical access control system implementation. In addition, since 2013, four Coast Guard locations have begun to implement GSA approved physical access control systems using the Approved Products List. Coast Guard officials said that due to the decentralized nature of Coast Guard's decision-making process for physical access control systems, it is difficult to say where purchases have been made, and there is no systematic tracking. The Coast Guard does not have a formal plan for upgrading its physical access control systems, but officials told GAO that they continue to pursue opportunities to upgrade facilities with physical access control system equipment using the Approved Products List.

The ISC, chaired by the DHS and consisting of 60 federal departments and agencies, has a mission to develop security standards for non-military agencies. In this capacity the ISC is well-positioned to determine the extent that PACS implementation challenges exist across its membership and to develop strategies to address them. An ISC official told GAO that the ISC has taken steps to do so including setting up a working group to assess what additional PACS guidance would be beneficial.

As a result of its report, GAO recommends that OMB determine and regularly monitor a baseline level of progress on PACS implementation and that ISC assess the extent of, and develop strategies to address, government-wide challenges to implementing PACS. DHS concurred with the recommendation to ISC and OMB made no comment.

▶▶ Read the full report at GAO

Ancient Greece: The cradle of democracy
Modern Greece: The cradle of absolute idiocy

Taking advantage of his sixth consecutive leave from the (not high security) prisons, the chief executioner of "17th of November", Dimitris Koufodinas, was not limited to the Varnavas village (~40km from Athens downtown), where he still owns a house, but also enjoyed a walk in the embellished center of Athens. Koufontinas, who has been sentenced 11 times to life imrisonment plus 25 years for involvement in 11 murders, explosions, robberies, and participation in the notorious terrorist organization "November 17", was spotted walking in a central busy road in the capital, close to the location where his pistol killed people.

Original Article

What is security: Definition through knowledge categorization

David J. Brooks
Security Research Centre (SECAU) at Edith Cowan University, Edith Cowan University, 100 Joondalup Drive, Joondalup, Perth 6027, Australia.
E-mail: d.brooks@ecu.edu.au

Abstract There have been a number of studies that have attempted to define the concept of security. However, as past authors have indicated, security is multidimensional in nature and diverse in practice. This diversity leads to difficulty in providing a single all encompassing definition for the many applied domains of security. Security cannot be considered singular in concept definition, as definition is dependant on applied context. This study reversed engineered an applied security definition through the critique of 104 undergraduate security degrees, resulting in the presentation of 13 core security knowledge categories. These 13 knowledge categories were then integrated into an existing Australian security framework, resulting in the presentation of the science of security framework model. This framework allowed a greater understanding of security through knowledge structure and placed concept definition within the applied context domain of organizational security.
Security Journal advance online publication, 12th January 2009; doi:10.1057/sj.2008.18

Source:https://www.researchgate.net/publication/247478178_What_is_security_Definition_through_knowledge_categorization

EDITOR'S COMMENT: An article that all security professionals have to read – it will help them organize security multiple domains in their minds!

The Ghost

Read more: https://www.thesun.co.uk/news/8109355/muslim-convert-terror-notes-oxford-street-ram-attack-killing/

These Are the Top 26 National Security Threats Facing America

By Michael Peck

Source: https://nationalinterest.org/blog/buzz/these-are-top-26-national-security-threats-facing-america-40412

Jan 03 – What do China, Russia, bubonic plague and global warming have in common? They are among the top threats to U.S. national security, according to the U.S. government.

The Government Accountability Office polled four government agencies on what they saw as the biggest threats to American security. The result was 26 threats identified by the Department of Defense, Department of State, Department of Homeland Security and the Office of the Director of National Intelligence.

Here are the 26:

- **Chinese global expansion.** "China is marshalling its diplomatic, economic, and military resources to facilitate its rise as a regional and global power," the report said. "This may challenge U.S. access to air, space, cyberspace, and maritime domains. China's use of cyberspace and electronic warfare could impact various U.S. systems and operations."
- **Russian global expansion.** "Russia is increasing its capability to challenge the United States across multiple warfare domains, including attempting to launch computer-based directed energy attacks against U.S. military assets. Russia is also increasing its military and political presence in key locations across the world."

- **Iran.** Iran is expanding the size and capabilities of its military and intelligence forces, as well as developing technology that could be used to build ICBMs and cyberwarfare.
- **North Korea.** North Korea is developing ICBMs that can hit North America.
- **Unstable governments.** Terrorism, extremism and political instability in Africa, Latin America and the Caribbean could tax U.S. resources needed for counter-terrorism and humanitarian relief.
- **Terrorism.** "Terrorists could advance their tactics, including building nuclear, biological or chemical weapons, or increase their use of online communications to reach new recruits and disseminate propaganda."
- **New adversaries and private corporations.** New states could arise that threaten the U.S. Interestingly, the GAO report worries about "private corporations obtaining resources that could grant them more influence than states."
- **Information operations.** Adversaries such as Russia, China and Iran will take advantage of social media, artificial intelligence and data crunching to wage information warfare.
- **Artificial intelligence.** AI will allow adversaries to design better weapons.
- **Quantum communications.** Quantum technology could result in communications that can't be intercepted or decoded by U.S. intelligence, while also making U.S. communications more vulnerable to interception.

- **Internet of Things.** Networks that control critical infrastructure, such as the power grid, are vulnerable.
- **Drones.** "Adversaries are developing autonomous capabilities that could recognize faces, understand gestures, and match voices of U.S. personnel, which could compromise U.S. operations," GAO said. "Unmanned ground, underwater, air, and space vehicles may be used for combat and surveillance."
- **Biotechnology.** States, terrorists and criminals could use DNA modification to create super-soldiers.
- **Emerging technologies.** New technologies such as 3-D printing, which could allow terrorists to manufacture weapons.
- **Weapons of mass destruction.** More actors are developing them.
- **Electronic warfare.** Other nations are developing technology that can disrupt U.S. communications, computers and satellite networks.
- **Hypersonic weapons.** Russia and China are developing Mach-5-plus weapons that can penetrate U.S. anti-missile defenses. Significantly, the report notes that "there are no existing countermeasures" to these weapons.
- **Counterspace weapons.** In addition to Russian effort, "China is developing capabilities to conduct large-scale anti-satellite strikes using novel physical, cyber, and electronic warfare means."
- **Missiles.** Not just land- and sea-based missiles, but also "space-based missiles that could orbit the earth."
- **Intelligence, Surveillance, and Reconnaissance (ISR) platforms.** Future advances in AI, sensors, data analytics, and space-based platforms could create an environment of "ubiquitous ISR," where people and equipment could be tracked throughout the world in near-real time.
- **Aircraft.** China and Russia are developing faster and longer-ranged aircraft, including stealth aircraft.
- **Undersea weapons.** "Russia has made significant advancements in submarine technology and tactics to escape detection by U.S. forces. China is developing underwater acoustic systems that could coordinate swarm attacks—the use of large quantities of simple and expendable assets to overwhelm opponents—among vehicles and provide greater undersea awareness."
- **Cyber weapons.** In addition to Russia and China, Iran and North Korea are developing cyberattack capabilities that could target a variety of systems, such as air traffic control or health care.
- **Infectious diseases.** Climate change, and increased global travel, could spread drug-resistant pandemics.
- **Climate change.** More extreme weather, such as more frequent hurricanes and droughts, and rising sea levels could disrupt food and energy supplies. Melting Arctic ice is opening new sea routes in the north, "potentially increasing Russian and Chinese access to the region and challenging the freedom of navigation that the United States currently has."

- **Mass migration.** Disasters, whether natural or man-made, will spur population flows that could strain U.S. military and civilian resources.

Michael Peck *is a contributing writer for the National Interest.*

January 2019
Hmeland Security Committee
Source: http://opencda.com/wp-content/uploads/2019/01/396705631-SIA-Report-2018.pdf

Since September 11th, 2001, America's national security officials have focused on preventing another catastrophic attack on our homeland by defeating the terrorist threat. This has made it harder for nefarious actors of all different backgrounds to enter the United States. As a result, those who wish to bring harm to America have to explore non-traditional ways of entering our country.
Today, those known as Special Interest Aliens (SIAs) are discovering new and creative routes to cross our border. One such way is through the exploitation of illicit pathways throughout the Western Hemisphere. Offering solutions to close these routes and shut off entry ways into America for SIAs must be a priority moving forward, since some of these migrants have been affiliated with foreign terror groups and organized crime.

Task Force on Denying Terrorist Entry into the United States
Given the threats we face from international terrorism, the House Homeland Security Committee established the Task Force on Combating Terrorist and Foreign Fighter Travel in 2015 and the Task Force on Denying Terrorists Entry into the United States in 2017 to evaluate threats and offer policy solutions to keep the homeland safe. In addition to these two task forces, staff members from the Majority were charged with identifying the exploitation of illicit pathways to America by SIAs throughout the Western Hemisphere.
This team was briefed by American and foreign national security officials, analyzed government documents, conducted research, and traveled to six different countries in Central and South America. The following report is the conclusion of their work.

Results of the Review
The Majority staff makes 10 policy recommendations to mitigate the threats posed by SIAs and others. The full description of these recommendations can be read toward the end of the report. They include:

Authorize Key Programs, an Office, and a New Authority:
- ICE's Biometric Identification Transnational Migration Alert Program (BITMAP)
- CBP's Immigration Advisory Program (IAP)
- DHS's Office of Biometric Identity Management (OBIM)
- Provide DHS Repatriation Authority

Conduct Threat Analyses for:
- U.S. Ports of Entry

- U.S. Maritime Borders
- Southwest U.S. Border

Strengthen Coordination and Cooperation:
- Better Support ICE's Transnational Criminal Investigative Units (TCIUs)
- Increase Interagency Coordination through a Western Hemisphere Task Force
- Creating an Inter-American Information Sharing System

Methodology
The Majority Staff of the House Committee on Homeland Security (Committee) conducted this investigation over a six-month period. The final report was informed by briefings, meetings, site visits to Brazil, Guatemala, Costa Rica, Colombia, Mexico, and Panama, extensive research, and analysis of official government documents. The Committee spoke with current and former federal officials throughout the national security community, relevant departments and agencies, outside experts, and foreign partner government officials.
The Committee examined U.S. government efforts to monitor, track, and prevent Special Interest Aliens (SIAs) from entering the Homeland. The review specifically focused on programs and initiatives that push out the United States borders and increase coordination with foreign partners. Where practicable, the Committee cites publicly available sources, though many relevant topics and materials are classified or sensitive in nature. Prior to publication, the final report was shared with the main departments and agencies that contributed to and assisted in the review. The Committee incorporated their feedback where appropriate.

Previous Committee Action
Over the course of the past two Congresses, this Committee has focused on identifying threats posed by foreign terrorist fighters and offering recommendations for how Congress and the Executive Branch can mitigate these threats to the Homeland.
In February 2015, the Committee created a bipartisan *Task Force on Combatting Terrorist and Foreign Fighter Travel* in response to an unprecedented number of foreign fighters, including thousands of Westerners, flocking to Iraq and Syria to join the Islamic State of Iraq and Syria (ISIS). As a result of that review, the Task Force developed 32 key findings with accompanying recommendations that were incorporated into legislation and some signed into law during the 114th Congress, including the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015*.
By February 2017, while the flow of foreign fighters to the conflict zone had dwindled, the desire of foreign fighters to return to their home countries or travel to the West to carry out attacks, created a new threat dynamic. In response, the Committee established the *Task Force on Denying Terrorists Entry into the United States.* As a result of that review, the Task Force identified seven key security challenges that needed to be addressed in the United States' screening and vetting framework and accompanying recommendations that were incorporated into legislation that passed out of the House of Representatives during the 115th Congress, none of which were passed by the Senate.

Carrying Tasers increases police use of force

Source: http://www.homelandsecuritynewswire.com/dr20190104-carrying-tasers-increases-police-use-of-force

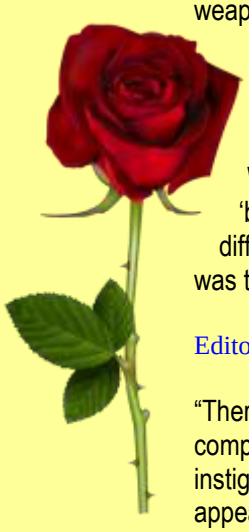
Jan 04 – **A new study has found that London police officers visibly armed with electroshock 'Taser' weapons used force 48 percent more often, and were more likely to be assaulted, than those on unarmed shifts.** However, while use of force can include everything from restraint and handcuffing to CS spray, the **Tasers themselves were only fired twice during the year-long study period**.
Criminologists from the University of Cambridge say the findings suggest that Tasers can trigger the "weapons effect": a psychological phenomenon in which **sight of a**

weapon increases aggressive behaviour.

While the 'weapons effect' has been repeatedly demonstrated in simulated conditions over the last forty years, this is one of the largest studies to show it "in the field" and the first to reveal the effect in law enforcement.

Researchers say their findings, published today in the journal *a* , may well apply to policing situations in which other forms of weaponry – including the lethal variety – are involved.

"We found that officers are more likely to be assaulted when carrying electroshock weaponry, and more likely to apply force," said lead researcher Dr Barak Ariel from Cambridge's Institute of Criminology.



"It is well established that the visual cue of a weapon can stimulate aggression. While our research does not pierce the 'black box' of decision-making, the only difference between our two study conditions was the presence of a Taser device."

Editor's proposal for law enforcement

"There was no increase in injury of suspects or complaints, suggesting it was not the police instigating hostilities. The presence of Tasers appears to provoke a pattern where suspects become more aggressive toward officers, who in turn respond more forcefully," he said.

The City of London force is responsible for policing the "Square Mile" business district in the centre of London. It also holds national responsibility for economic crime and prioritises counter-terrorism, violent crime and public order due to its central location.

The force was the first in England and Wales to test "extended deployment" of Tasers – described as "conducted energy devices" in UK policing – to frontline officers. During the rollout, police chiefs allowed Ariel and colleagues to conduct a major experiment.

Cambridge notes that between June 2016 and June 2017 the researchers randomly allocated 400 frontline shifts a Taser-carrying officer and compared the results to an equal number of unarmed shifts over the same period. A total of 5,981 incidents occurred during the study.

Use of force by police carrying Tasers was 48 percent higher than the officers on unarmed shifts. In what researchers call a "contagion effect", even those unarmed officers accompanying Taser carriers on 'treatment' shifts used force 19 percent more often than those on Taser-free 'control' shifts.

Six physical assaults against police were recorded during shifts with Taser-carrying officers, compared to just three on the unarmed 'control' shifts. While the numbers are small, assaults against officers are rare, and researchers argue that this doubling is significant.

Despite the increased hostility uncovered by the study, actual use of electroshock weapons was minimal over the study period, with just nine "deholsterings" – only two of which resulted in electric shocks applied to a suspect.

"The City of London police rarely discharged Tasers during the study. Yet the very presence of the weapon led to increased hostility between the police and public," said Ariel.

The weapons effect was first shown by psychologist Leonard Berkowitz in 1967, in a laboratory experiment involving the administering of electric shocks in the presence of a rifle – an experiment that Ariel points out has been replicated 78 times.

"For many, a weapon is a deterrence. However, some individuals interpret the sight of a weapon as an aggressive cue – a threat that creates a hostile environment," Ariel said.

"The response is consequently a 'fight or flight' dilemma that can result in a behavioural manifestation of aggression and assault. This is what we think we are seeing in our Taser experiment."

"It would not be surprising to find that serious or violent offenders fit this criteria, especially young males – the very type of suspect that is regularly in direct contact with frontline police."

Half a million police officers in the United States regularly carry Tasers, and electroshock weapons are now becoming part of frontline policing across the UK.

The study author's offer a simple solution to bypass the weapons effect: conceal the Tasers. "The relatively inexpensive policy change of keeping Tasers hidden from sight should not limit efficacy, but could reduce the weapons effect we see in the study," said Ariel.

"This conclusion could be generalised to all types of police armoury, including the lethal

firearms carried by police officers. If the presence of weapons can lead to aggression by suspects, so its concealment should be able to reduce aggression and increase officer safety," he said.

Study co-author Chief Superintendent David Lawes, from the City of London Police, said: "Following the findings of the study, we are exploring whether a simple holster change or weapon position move will nullify the weapons effect issue shown in the experiment. We have also updated our training package for officers carrying Tasers to make them aware of the findings."

"The use of Tasers has been a proportionate and sensible introduction to policing against a backdrop of unsophisticated terror attacks and an increase in violent crime across London.

"The City of London Police seeks to ensure that any major changes to policy are supported by an evidence base and we wanted to be confident that an extension of Taser deployments to our frontline responders was the right thing to do for both our officers and the public they serve.

"A number of other forces are interested in replicating the study to add to the evidence base and see whether the experiment produces the same results outside of London.

"Across our force, we will continue to use evidence to define how we target problems, which tactics we should use and how we can ensure policing is efficient and safer for both the general public and our officers."

— Read more in Barak Ariel et al., "The 'Less-Than-Lethal Weapons Effect' — Introducing TASERs to Routine Police Operations in England and Wales: A Randomized Controlled Trial," Criminal Justice and Behavior (2018).

Could this device prevent future terror attacks? CatClaw gives cars that mount kerbs FLAT TYRES by puncturing them with a sharp steel spike

Source: https://www.dailymail.co.uk/sciencetech/article-5481595/CatClaw-gives-flat-tyres-cars-mount-kerbs.html

Terrorists in vans who try to mow down pedestrians may think again, thanks to a new device that can be installed along kerbs to quickly puncture their tyres.

When a vehicle drives over a CatClaw, which is the size of a small orange, its weight pushes a button down, exposing a sharp steel tube that quickly punctures the tyre.

The device, which is currently only at the prototype phase, will also act as a deterrent against illegal pavement parking.

Its creator envisages it being installed in its thousands along kerbs and other pedestrianised areas around the world.

Yannick Read, from the Environmental Transport Association (ETA), was inspired to invent the device after watching footage of terror attacks involving cars.

To prevent terror attacks at certain locations, physical obstructions such as steel bollards or concrete blocks are the only practicable counter-measure.

The car used to attack pedestrians on Westminster Bridge in March of 2017, for example, would have been rendered undriveable if all its tyres had been punctured by CatClaw.

This could have prevented its driver from reaching high speeds and staying in control of the vehicle.
It's not always feasible to install bollards and blocks, however.
CatClaw provides a 'cheap and effective secondary line of defence over a widespread area,' the ETA says.

According to Mr Read, CatClaw poses no threat to pedestrians as a person standing on top of the device would not be heavy enough to activate it.

He said: '43 people were killed last year by cars and lorries as they walked along a pavement or verge, so I invented CatClaw to reduce this type of terror as much as to tackle politically-motivated attacks.'
The ETA suggests that CatClaw can provide a powerful deterrent against illegal pavement parking where is installed.
Each unit takes three minutes to install, doesn't require an energy supply or upkeep, and costs only a few pounds to produce.
CatClaw's can be installed surrounded by solar-powered LED markers as a warning, if necessary.
Mr Read told the *Bristol Post* that the problem of pavement parking is growing.
'The rise of internet shopping means we hear complaints from many people about delivery drivers - couriers and supermarket delivery vans - who would rather pull up onto the pavement to make deliveries thank risk the anger of drivers stuck behind them,' he said.
Mr Read added that he believes it's not just delivery drivers who are at fault and that our impatient society is also to blame.

'Driving on pavements has become socially acceptable – people don't think anything of it,' he said.
Mr Read said the response to his CatClaw prototype has been mostly positive and that he welcomes any critical input from the public.
'We've shown the principle works,' he said. 'It wouldn't be appropriate to put them everywhere.
'I'd be interested to hear their objections,' said Mr Read.
While it is illegal to park on the pavement in London, it is legal to do so in other parts of the UK if road signs permit it.

WHAT ARE SOME OF THE TOOLS USED TO PREVENT CAR ACCIDENTS?

A number of tools can be used to prevent cars from driving onto pavements and kerbs, crossing into a patch of oncoming traffic or hitting roadside hazards.
These are usually in the form of barriers, which are designed to redirect the vehicle and have a lower severity than the roadside hazard they protect.
According to the **Road Safety Toolkit**, there are three main types of safety barriers:
Flexible barriers: These barriers are made from wire rope supported between frangible posts. Flexible barriers may be the best option for minimising injuries to vehicle occupants. These need to be repaired following impact.
Semi-rigid barriers: These are usually made from steel beams or rails. They deflect less than flexible barriers and so they can be located closer to the hazard, when space is limited.
Rigid barriers: These are usually made of concrete and do not deflect. They should be used only where there is no room for deflection of a semi-rigid or flexible barrier. These barriers are often used at high volume roadwork sites to protect road workers or other road users when another type of barrier is awaiting repair. Rigid barriers provide the highest levels of containment of heavy vehicles.
A new, innovative mechanism to prevent cars driving onto pavements has been designed by Yannick Read from the Environmental Transport Association (ETA).
His prototype, called CatClaw, is the size of a small orange and is designed to be installed in its thousands along kerbs and pavements.
When a car drives over a CatClaw, its weight pushes a button down, exposing a sharp steel tube that quickly punctures the tyre.
While the device is only at the prototype phase, Mr Read says it may one day prevent terror attacks involving cars.

Cuban lovelorn crickets, not a sonic weapon, made U.S. diplomats ill: Study

Source: http://www.homelandsecuritynewswire.com/dr20190107-cuban-lovelorn-crickets-not-a-sonic-weapon-made-u-s-diplomats-ill-study

Jan 07 – A noise heard by U.S. diplomats in Cuba, a noise which causeed some of them to suffer mysterious brain injuries, was not generated by technological weapons but by local crickets, a new study suggests.
In late 2016, U.S. diplomats in Havana began to report ear pain and other symptoms from a high-frequency noise, leading the State Department to withdraw half its embassy staff, and expel Cuban diplomats in retaliation (see "Microwave weapons suspected as cause of U.S. envoys' illnesses," HSNW, 4 September 2018; Tim Golden and Sebastian Rotella, "The sound and the fury: Inside the mystery of the Havana embassy," HSNW, 16 February 2018)
A new study by two biologists, however, assessed a purported recording of the noise and said it matched the mating song of the Indies short-tailed cricket found around the Caribbean.
The *New York Times* reports that the specific cause of the diplomats' ailments was outside the scope of the study, with the researchers not ruling out that the diplomats suffered an attack by a sonic weapons at another point.

"While disconcerting, the mysterious sounds in Cuba are not physically dangerous and do not constitute a sonic attack," said the study by Alexander Stubbs, a graduate student at the University of California, Berkeley, and Fernando Montealegre-Zapata, a professor of sensory biology at the University of Lincoln in Britain.

"Our findings highlight the need for more rigorous research into the source of these ailments, including the potential psychogenic effects, as well as possible physiological explanations unrelated to sonic attacks," they wrote.

The researchers say that the Cuba incident has parallels to the 1981 yellow rain incident, when the United States accused the Soviet Union of deploying in Southeast Asia deadly chemical weapons—which some researchers later concluded to be droppings from bees.

In the Havana incident, the researchers studied a recording made by a U.S. government employee which was sent to the U.S. Navy for analysis and was later published by the AP.

The researchers compared the Cuba recording with data from the Singing Insects of North America database run by University of Florida entomologist Thomas Walker, who found that the Indies short-tailed cricket had the fastest wing stroke rate of any known cricket that calls continuously.

The cricket's calling song matches the recording in "duration, pulse repetition rate, power spectrum, pulse rate stability, and oscillations per pulse," the study said.

The *Times* notes that the research was released last week and has not yet been peer-reviewed or published in an academic journal.

Two dozen U.S. diplomats and several Canadians reported dizziness, anxiety, and mental fog—conditions that University of Pennsylvania researchers described as similar to concussions (see "21 U.S. diplomats in Cuba suffered 'acquired brain injury from an exposure of unknown origin': Experts," HSNW, 20 February 2018).

Other studies, however, have dismissed the conclusion, with a paper in the *International Journal of Social Psychiatry* finding suspicious that no Cubans reported symptoms and theorizing about a mass hysteria (see Robet E. Bartholomew and Dionisio F. Zaldivar Perez, "Chasing ghosts in Cuba: Is mass psychogenic illness masquerading as an acoustical attack?" *International Journal of Social Psychiatry* [2 April 2018]).

The United States has not officially accused Cuba of attacking the diplomats. The Trump administration, however, has charged that Cuba had failed to protect them.

— Read more in Alexander L. Stubbs and Fernando Montealegre-Zapata, "Recording of "sonic attacks" on U.S. diplomats in Cuba spectrally matches the echoing call of a Caribbean cricket," BioRxiv (4 January 2019).

EU Defence: The White Book implementation process

Source:http://www.europarl.europa.eu/RegData/etudes/STUD/2018/603871/EXPO_STU(2018)603871_EN.pdf

Dec 2018 – The question of a defence White Book at European level has been under discussion for some time. Many voices, particularly in the European Parliament, are pushing for such an initiative, while others consider that it is not only unnecessary, but could even dangerously divide Europeans. Concretely, the question cannot be tackled separately from that of defence planning and processes which underpin the development of military capabilities, as White Books are often the starting point for these.

Within the European Union, however, there is not just one, but three types defence planning: the national planning of each of the Member States; planning within the framework of NATO (the NATO Defence Planning Process) and, finally, the European Union's planning, which

has developed in stages since the Helsinki summit of 1999 and comprises many elements. Its best-known component - but by no means not the only one - is the capability development plan established by the European Defence Agency. How do all these different planning systems coexist? What are their strengths and weaknesses? Answering these preliminary questions is essential in mapping the path to a White Book. This is what this study sets out to do.

What we know about the effectiveness of universal gun background checks

By Alex Yablon

Source: http://www.homelandsecuritynewswire.com/dr20190111-what-we-know-about-the-effectiveness-of-universal-gun-background-checks

Jan 11 – This Tuesday, newly dominant House Democrats revealed legislation that would require all gun buyers go through a background check, regardless of whether they buy a weapon from a licensed dealer, collector at a gun show, or stranger in a parking lot.

Universal background checks are popular and enjoy political momentum. Poll after poll shows they win near universal approval. According to a Quinnipiac University poll conducted immediately after the school shooting at a high school in Parkland, Florida, last February, 97 percent of American voters said they approved of the policy, with identical levels of support among respondents living in households with a gun.

But it's worth asking how effective universal background checks are at reducing gun violence. And the real-world evidence that they reduce crime is more complicated than the political momentum might suggest.

"The direct evidence on effectiveness is limited," said Duke University public policy expert Philip Cook, who has studied background checks. "It's very plausible that a state that tries to close this huge loophole and devotes resources to enforcing it will have good results. But not every program is going to be equally effective. It takes a real, concerted effort to get people to change the way they have been doing things for so long."

Why expand the federal gun background check system?

Current federal law subjects a gun sale to a background check only if the seller is a licensed dealer "engaged in the business" of selling firearms. That means collectors who occasionally set up booths at gun shows or individuals who advertise a couple of weapons on a classifieds' website like Armslist don't have to vet their customers.

A number of states have tried to close this loophole by requiring all gun transactions to go through a check, regardless of whether the seller is a licensed dealer or a private individual. California was the first to create a universal background check law, in 1991. Today, 20 states and the District of Columbia regulate private sales, either by mandating checks at the point of every sale or by requiring permits to purchase a firearm.

With private sales unmonitored in so much of the country, it won't come as a surprise that a survey published by Harvard and Northeastern universities in 2017 found that approximately one out of five guns is sold in an unregulated transaction.

There's good reason to suspect that the unregulated gun market fuels gun crime. Interviews with people convicted of gun crimes have found relatively few get their weapons directly from retailers. Instead they rely on informal networks and underground sellers who take advantage of the legal loophole to sell guns free of oversight. Advocates believe that eliminating the private sale loophole could make it harder for criminals to get guns and thus reduce shootings.

How effective are expanded gun background checks?

Academic research suggests that background checks have potential to reduce crime, but in practice the record has been mixed.

A 2001 study by Garen Wintemute of the University of California,

Davis, found that Californians convicted of violent misdemeanors who had been denied a gun sale by the state's background check system were less likely to be re-arrested for a violent or gun crime than people with similar criminal histories who were not denied. That suggests that where the system works as intended, background checks can reduce gun crime.

Yet other research suggests implementation has been spotty. In a recent study, Wintemute and colleague Rose Kagawa found that in California's first decade with a universal background check law on the books, the policy had no significant effect on the number of gun homicides or suicides. Wintemute and Kagawa co-authored another study that found no evidence that Tennessee and Indiana's passage, and later repeal, of comprehensive background check requirements affected homicide or suicide rates.

"In individual cases, people who are denied have lower arrest rates. So there, you're seeing an effect," Kagawa said in an interview. "But at the state level, you're not seeing the impact." In other words, the policy doesn't seem to scale.

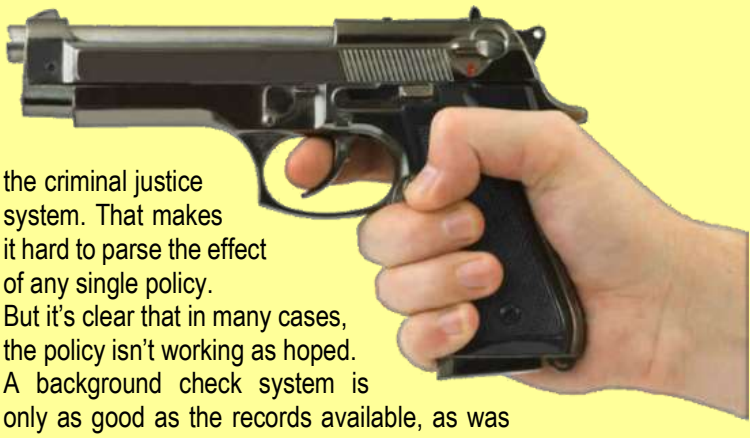
Reviews of broad swaths of research have reached differing conclusions. One 2012 meta analysis found little statistically significant evidence that checks reduce shootings. Two later reviews of academic literature from 2016 and 2017 strongly endorsed the policies. A landmark 2017 review of various gun policies by the RAND Corporation found only moderate evidence that checks reduce suicide and violent crime.

Why is the research all over the place?

The ambivalence of all this research may be partly due to study methodology, and partly due to shortfalls in implementation.

Wintemute and Kagawa's study of California only looked at the first 10 years that the state's system was in operation, when it still had serious kinks to work out. Most criminal records were incomplete. "That's just not true anymore because the data has gotten so much better," Wintemute said. A future study that looked at the state's more recent experience could conceivably find that as operations improved, so did the impact on gun crime rates.

It's also difficult to isolate the effect of one policy on gun violence. The past 30 years have seen violent crime reach historic highs and lows. Wintemute stressed that such volatility is almost certainly the result of multiple interacting factors like the economy and changes to



the criminal justice system. That makes it hard to parse the effect of any single policy.

But it's clear that in many cases, the policy isn't working as hoped.

A background check system is only as good as the records available, as was demonstrated in the Sutherland Springs, Charleston, and Virginia Tech mass shootings. In each of those cases, the gunmen were able to pass background checks despite convictions for domestic violence, a history of drug abuse, or involuntary psychiatric hospitalization, respectively. The relevant records either weren't entered into the appropriate database or weren't clearly labeled as prohibiting. In the Charleston case, the background check was also hampered by a provision that allows sales to go through after three business days, whether or not federal examiners have cleared the buyer.

Additionally, many people just ignore the law. In a study conducted this past October, Wintemute reviewed survey data that found large numbers of California gun owners disregard background check requirements nearly three decades after the policy was first implemented. One in four gun owners said they had purchased a gun without going through a check. That's roughly the same proportion as gun owners in the rest of the country, according to the Harvard/Northeastern survey.

In another study, Wintemute, Kagawa, and others found that in three states that passed universal background check laws — Colorado, Washington and Delaware — only one saw the number of checks increase. Logically, if gun owners complied with the law and got checked for sales that would have previously

been unregulated, the number of checks should have risen substantially.

What's the point if checks might not reduce gun violence?

Shootings themselves are only one kind of criminal activity that policy makers seek to reduce with background checks. Research by Daniel Webster of the Johns Hopkins University Bloomberg School of Public Health suggests that universal background checks effectively constrain the illegal gun market.

Webster found in a 2009 analysis of gun trace data from the Bureau of Alcohol, Tobacco, Firearms and Explosives that universal background check laws reduced trafficking. States with universal background checks, along with more stringent dealer inspections, reduced the rate at which criminals committed crimes with guns they didn't originally purchase at retail within the state, a common proxy measure of trafficking.

Webster said in an interview that this research shows "there is less in-state diversion of guns from legal owners to criminals when private sales are regulated."

The same goes for flows of guns between states. In a book on the effectiveness of gun policy that Webster edited in 2013, he reviewed a wealth of economic literature that found that states with weak gun laws that allowed unregulated private sales routinely exported guns to states with stronger laws — but not the other way around.

What type of screening *does* reduce gun violence?

So-called permit-to-purchase systems have shown a lot of promise. In such a system, all gun buyers must apply for a gun license from local law enforcement. Licenses are only granted to residents who clear a complete background check. Four states (Hawaii, Massachusetts, Illinois, and New Jersey) require a permit for all gun purchases. Six more (Connecticut, Iowa, Michigan, Nebraska, New York, and North Carolina) require permits to buy or own a handgun.

Research by Webster strongly suggests that permit-to-purchase laws reduce gun deaths. That may be because they are straightforward to comply with and enforce: Before a private dealer completes a sale, he just has to ask to see the buyer's permit, rather than initiate a background check through a computerized system and wait for the result. When a police officer apprehends someone with a firearm, the permit, or lack of one, provides strong indication of whether the person is a legal gun owner.

What's more, after Missouri repealed its license law in 2007, Webster and several colleagues found sharp increases in the percent of guns recovered at crime scenes shortly after initial retail sale, a measure known as "time-to-crime" and considered an indication of trafficking. The percentage of guns recovered at crime scenes within three months of their original sale nearly tripled from 2006 to 2011.

In a 2015 paper, Webster and others compared Missouri with Connecticut, which implemented a licensing requirement in the early 1990s. In Missouri, firearm suicides increased 16 percent after the repeal of the permit requirement. In Connecticut, the firearm suicide rate fell by 15 percent after the state imposed its permit law.

If states are addressing this, why does the federal government need to pass its own law?

Even if a state could effectively screen all gun sales within its borders, people banned from owning firearms could still travel to a neighboring state with looser laws to arrange a private sale. That's the case in many of the states with policies that seek to vet all gun buyers. Tough-on-guns California borders Arizona, where firearm regulations are thin. New York borders Pennsylvania, one of the National Rifle Association's strongest bases of influence outside the South and West. Illinois borders Indiana, and so on.

A federal universal background check law would replace the current legal patchwork with one strict standard.

As Webster put it: "We're so far from a comprehensive regulation in sales. There's no way to tackle this without universal background checks."

Alex Yablon is a reporter at The Trace.

Central American Countries Are Helping Middle Easterners Illegally Enter the United States

By Todd Bensman
The Federalist
January 2, 2019
Article:https://www.meforum.org/57568/central-american-countries-are-helping-middle

In December 2018, the Center for Immigration Studies dispatched Senior National Security Fellow Todd Bensman to Panama and Costa Rica to investigate President Donald Trump's widely ridiculed assertions that suspected terrorists had been apprehended among Middle East migrants through Latin America. Panama is a geographic chokepoint, or bottleneck, through which migrants from countries of the Middle East, who are moving out of South America, must push on their way to the U.S. border.
The following article is based on Bensman's on-the-ground research over two weeks. His video reports, photos, and writings from the trip can be found here.

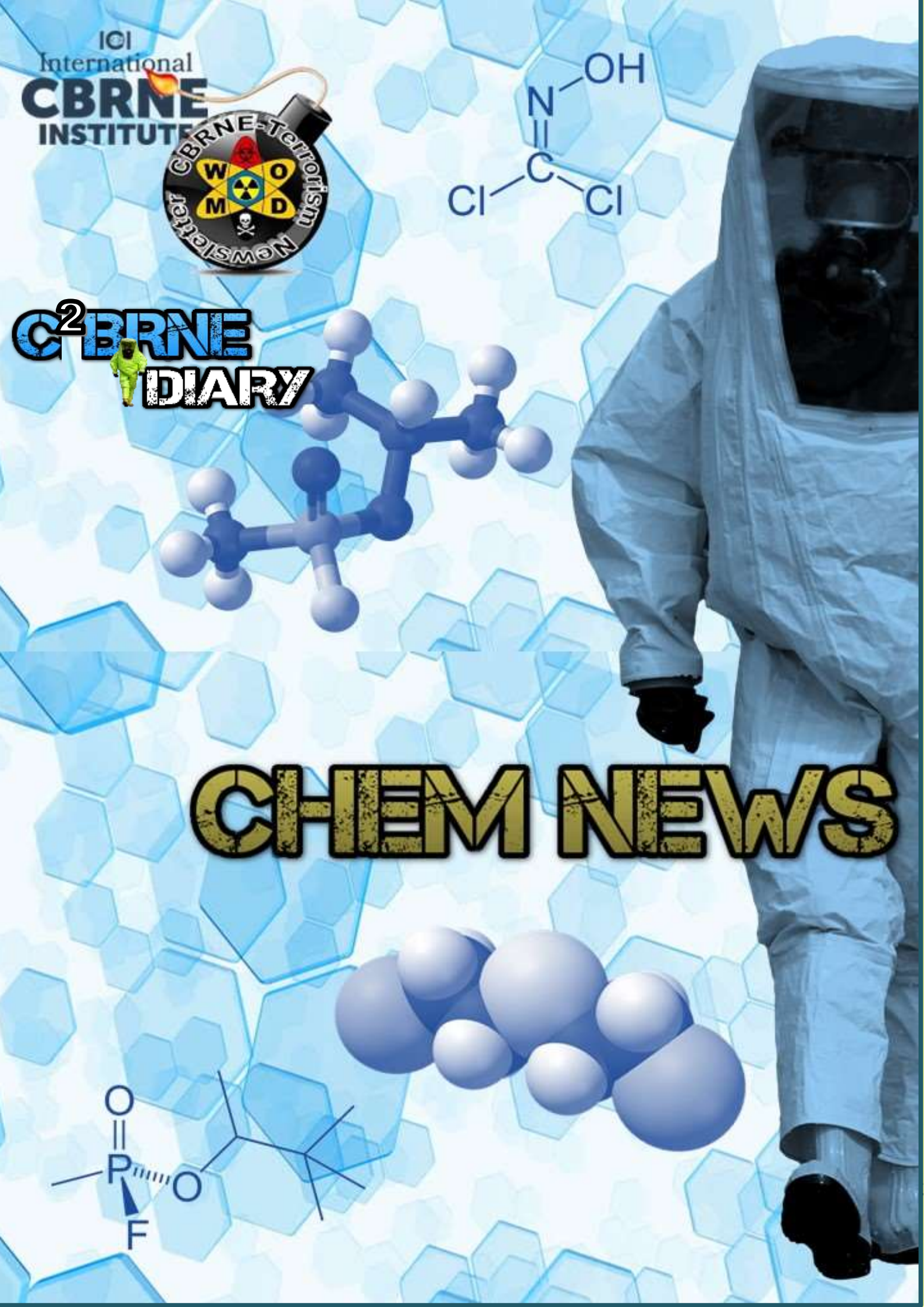
***Todd Bensman** is a Texas-based senior national security fellow for the Center for Immigration Studies. For nearly a decade, Bensman led counterterrorism-related intelligence efforts for the Texas Intelligence and Counterterrorism Division.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CHEM NEWS



Abu Dhabi's CBRN

By Major Dr. Abdullah Al Hmoudi of the CBRN Unit

CBRNe World April 2018

Source: http://www.mastercbrn.com/uploads/various/20180518931070274_Abu_Dhabi_IMS.pdf

The impacts and costs of hazards on people, properties and the environment are often severe when they occur, especially when there's no warning system in place. The lack of an early warning system (EWS), and limited knowledge of the potential impact of hazard in some communities in the UAE have emphasized the need for more effective early warning systems.

This paper examines the use of an innovation lab to improve understanding of the potential impacts of hazards, and as an EWS tool in the UAE. Identifying elements of EWS from literature helped in developing the framework for structuring and implementing activities in the innovation lab, using a comprehensive hazard approach that focuses on CBRN risks, knowledge of which is minimal in the UAE. **The population of Abu Dhabi was surveyed to determine how much people know about CBRN hazards, while eight managers in the Abu Dhabi Police (ADP) were interviewed to further understand the role of the innovation lab in improving the current level of knowledge. The research revealed that knowledge and warning of CBRN hazards in the UAE is low, and may be improved through the use of an innovation lab.**

Introduction

As an essential part of the preparedness phase for any disruptive event, EWS are very important, though underemphasised[1, 2]. Among all the other preparedness activities such as training programs, mutual aid agreements, exercises, resource inventories and management[3, 1] EWS often tend to be overlooked or inadequately conducted at this stage[4].

The limited attention paid to EWS often impacts on response arrangements, and the effect of this further impacts communities that are prone to such hazards[5]. Past hazards and the resultant impacts have shown just how susceptible communities are when faced with hazards while lacking adequate EWS[4]. A 2010 paper on disaster management with regard to rapid onset natural disasters[5] states that concerns about hazards and safety can preoccupy people to the extent that fear overwhelms them to the point of inaction. Such inaction has been linked[3] to lack of public education, awareness and information.

It can be argued[1], however, that the negative impacts of hazards should be strong grounds for investing in effective EWS. Further, the role of emergency officers/agencies and the community in planning for response, and the indicators for EWS for hazards are confusing, and even in best case scenarios they are vague in many countries, the UAE included[4, 6]. Thus, this paper draws upon EWS literature, and identifies the key elements of effective EWS, which are used to evaluate hazard knowledge in Abu Dhabi. These elements also inform police use of the innovation lab for the purpose of improving knowledge levels and educating both emergency organizations and communities on the impacts of hazards, and clarifying their roles in response to CBRN hazards.

Innovation Lab: Concepts and application

The UAE faces various socio-technical challenges one of which is the vagueness surrounding EWS for communities, and the roles of communities and emergency organizations in implementing EWS.

Abu Dhabi residents, for example are unaware of national or emergency plans that define their role and the procedures for EWS[5]. What's more, there is little knowledge, as well as a lack of education regarding EWS signals and confirmation of receipt of EWS in the event of hazards.

The consequences of this lack of an end-to-end approach to preparedness have been identified[5]. But other papers[7] have emphasized how the lack of a people-focused approach to preparedness, and especially EWS, could be devastating immediately and in the long term in Abu Dhabi. Undeniably, the presence of many non-Arabic-speaking expatriates creates further communication challenges, so careful consideration needs to be given to EWS tools and public education in multiple languages.

The weaknesses in the transfer of comprehensible warning messages and preparedness information to those at risk are acknowledged8. Thus, the past lack of networking and communication among all stakeholders[8] has reinforced the relevance of using the innovation lab to generate ideas for brainstorming models that may be used to communicate on CBRN risks.
Brainstorming sessions in the innovation lab, have created solutions for CBRN response and EWS that may lead to more effective integration of technologies for EWS and response processes for CBRN hazards in Abu Dhabi[9].
The model created, integrates monitoring and control measures for hazards, and the means of raising community awareness around potential risks of CBRN. Use of technology in this space has further enabled the use of modern detectors at hazard sites and control. This comprehensive mode incorporates the elements of effective EWS identified in UN recommendations[10] in 2006. **The four elements of effective EWS being; risk knowledge which includes data collection and risk assessment, monitoring and warning, warning dissemination and communication, and response capability.** Taking a lead from these elements, more comprehensive ideas were created in the innovation lab, and then tested through semi-structured interviews and questionnaires.

Methods

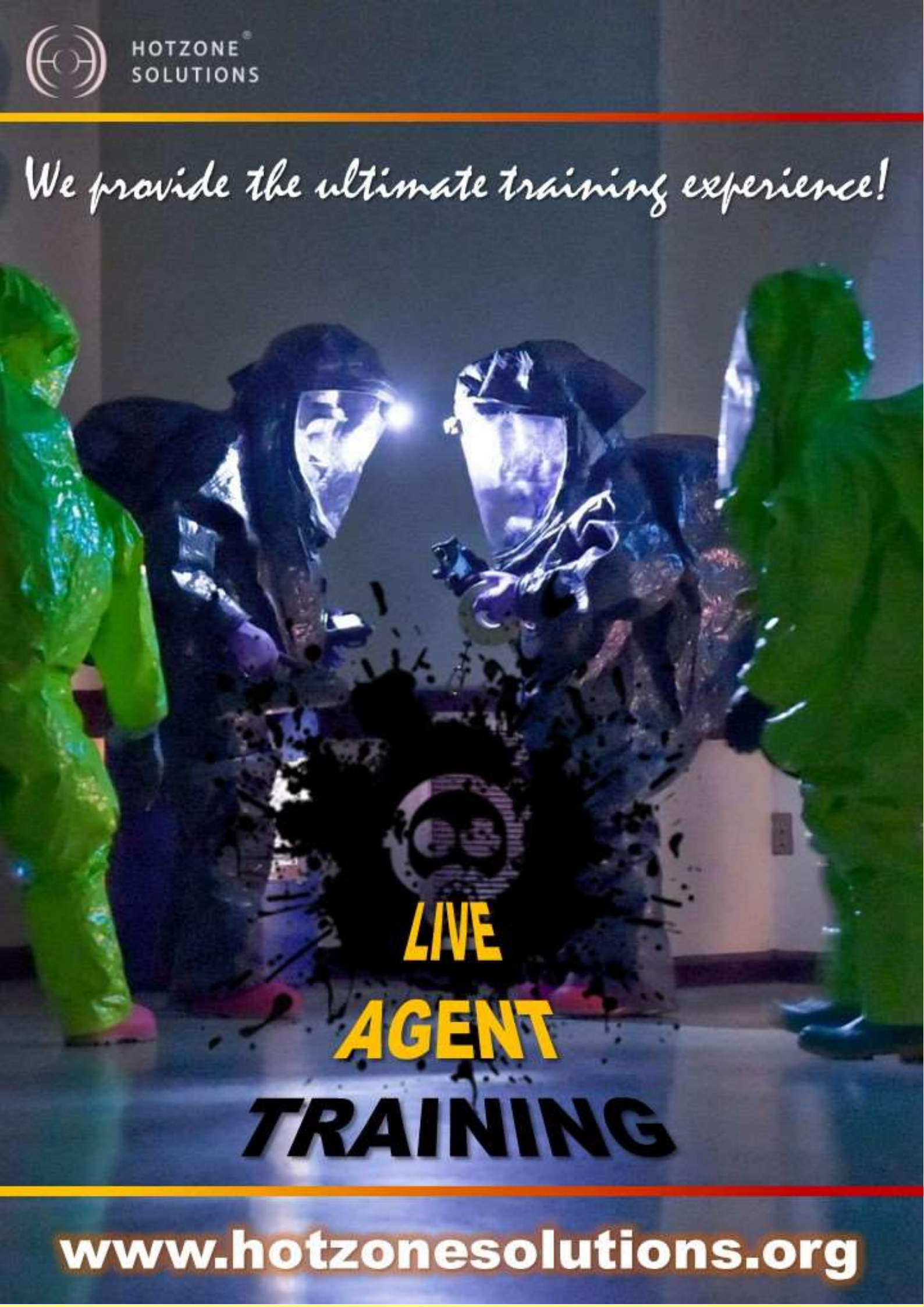
Primary qualitative and quantitative data were collected in the UAE. The qualitative element, which focused on investigating the existing deployment of EWS and the role of the innovation lab in improving knowledge of CRBN, involved a series of semi-structured interviews with emergency organizations in Abu Dhabi. A total of eleven questions were put to eight interviewees, with sessions lasting between 45 and 90 minutes depending on the level of engagement.
The questionnaire set out to determine the risk knowledge level and perceptions of CBRN among people in Abu Dhabi. A random sampling technique[11] was used to determine the required number of participants, and a paper questionnaire was used to encourage wide participation by people living, working and conducting business with close proximity to a potential CBRN hazard. Using this method, a total of 845 responders was achieved, which is a sample size calculated to provide a confidence level similar to that of Gautam and Shivakoti[12] in 2001.
The questionnaire included 25 questions grouped into four main sections based on four interrelated elements or themes for effective EWS. Due to the vast number of foreigners in Abu Dhabi, it was produced in both English and Arabic and was collected five days after being dropped off at homes, offices, commercial centers like malls, stations and community centers, and schools. Copies were also delivered to and collected from staff in hotels, public ministries and other organizations.

Data analysis

The interview data was analyzed using Nvivo[10] software and categorized according to the elements of effective EWS. The questionnaire data analysis was carried out using SPSS software to produce descriptive and inferential statistics[13]. By using SPSS version[16], important data from the community at risk was generated to determine the level of risk knowledge, and the potential impacts of EWS ideas developed in the innovation lab. This process generated data which contributed to developing the framework for effective EWS for mitigating the impacts of CBRN hazards in the UAE.

Results and Discussion

The result revealed that risk knowledge of CBRN hazards is low among the community, while community members believed that hazard monitoring and warning ought to be conducted by the police and disseminated via the media or mobile SMS. It also revealed that the community are unaware that the police run exercises and are trained to respond to CBRN hazards. **They believe that the community should participate in exercises to test evacuation processes.** For instance, 48% of the responders replied that participating in exercises of this nature will help to improve awareness and knowledge of CBRN risks.


HOTZONE®
SOLUTIONS
We provide the ultimate training experience!
LIVE
AGENT
TRAINING
www.hotzonesolutions.org

he semi-structured interviews with managers in emergency organizations revealed a low level of knowledge of the use of the innovation lab to increase risk knowledge. However, ADP managers were aware of the potential and importance of the innovation lab in developing new ideas that can improve community awareness and knowledge of CBRN hazards. Though views vary on which organization should lead the EWS for CBRN hazards, all the managers interviewed emphasized that several multi-cultural mediums should be used to disseminate warnings of CBRN hazards to the community. The interview results indicate that the response capabilities of emergency organizations vary with only civil defense confirming its capability to respond to CBRN hazards. ADP confirmed its ability to use the innovation lab to create an effective EWS model that may be used to improve knowledge of CBRN risks and give warnings that may help to preserve the lives of residents.

Discussion

The pattern of results generated by this research show that improvement is needed in the areas of risk knowledge, and the monitoring and dissemination of warnings concerning CBRN hazards. While the interview results on risk knowledge reveal the lack of expertise and understanding of EWS in Abu Dhabi, the full results also reveal that **any preparedness activities fail to involve the community at risk.** The practice of EWS in the UAE and response lacks the four interrelated elements of EWS identified in the literature. A structured process exists for communicating warnings between organizations, but it lacks community involvement. This suggests that communication only takes place along horizontal lines, which is too limited a process for disseminating hazard warning messages[14]. The results show that there is no effective EWS in Abu Dhabi since the four elements are not sufficiently identified through the survey nor explained by the managers. Consequently, the results were subjected to further brainstorming sessions in the innovation lab, from which the EWS model (diagram, right) was generated. The model shows that multicultural public education has been identified as an important component of any EWS in Abu Dhabi due to its large number of expatriates. Community awareness has been added to the model, and encompasses community participation, media engagement and CBRN training and communication. It was decided in the innovation lab that these elements will enhance response capabilities and the overall early warning systems for CBRN hazards in Abu Dhabi.

Conclusions

The elements of effective EWS derived from the 2006 UN global survey of early warning systems[10] were instrumental in determining what was important for EWS in Abu Dhabi. The research results, however, revealed that improvement is required in Abu Dhabi, and the innovation lab provided the platform from which ADP officers could embark on brainstorming and investigation that involved the communities at risk. While this combined method of inquiry is unprecedented in Abu Dhabi and by ADP, it has emphasized the importance of the innovation lab and its role in enhancing knowledge and creating ideas that can lead to improved systems, procedures and preparedness for CBRN hazards in Abu Dhabi and the UAE as a whole. **While the lab was not popular prior to this investigation**, its role in helping officers to brainstorm and create ideas has pushed it to the fore within ADP as a means of improving preparedness and capabilities for responding to CBRN hazards.

References

1. Sqrensen, Vedeld and Haug, 2006.
2. Coppola, D (2011) Introduction to International Disaster Management. Amsterdam, Butterworth-Heinemann.
3. Alexander, D (2002) Principles of emergency planning and management. Harpenden: Terra.
4. Wisner, B. (2011) "Are We There Yet? Reflections on Integrated Disaster Risk Management after Ten Years." IDRiM Journal 1 (1) (March 4): pp. 1–14.
5. Dhanhani, H, Duncan, A, Chester, D (2010) UAE: Disaster management with regard to rapid onset natural disasters. DOI:10.4018/978-1-61520-987-3.ch005.
6. Alhmoudi, A., Aziz, Z. (2015b) "A guideline for implementing major elements of EWS in the Arab Region: Case studies in the U.A.E", Conference Paper on Disaster Management and Human Health Risk IV (book), Wessex

Institute (WIT Press), British Library Cataloguing-in-Publication Data, Vol.150, No1. pp.135-143, 2015. [Online]www.witpress.com.ISSN 1743-3509.
7 Alhmoudi, A., Aziz, Z. (2015) Developing a framework to enhance early warning response capabilities and resilience in the UAE, Conference Paper on Disaster Management and Human Health Risk IV (book), Wessex Institute (WIT Press), British Library Cataloguing-in-Publication Data, Vol.150, No1. pp.127-133, 2015. [Online]www.witpress.com.ISSN 1743-3509.
8. Al Ameri, F. (2010) Implementing an Effective Public Warning System in Abu Dhabi UAE. Coventry University (MSC-Disaster Management).
9. Alhmoudi, A, Aziz, Z (2015c) Integrated elements of early warning systems to enhance disaster resilience in the Arab Region has been accepted by the Journal of Geodesy and Geomatics Engineering, David Publishing Company New York, USA. [Online] www.davidpublishing.org
10. UN. (2006) "Global Survey of Early Warning Systems". Final Version.46pOnline20/03/2010 http://www.preventionweb.net/files/3612_GlobalSurveyofEarlyWarningSystems.pdf.
11. Kothari, C (2008) Research Methodology: Methods and techniques. New Delhi: New Age International (P) Ltd., Publishers.
12. Gautam, A., Shivakoti, G.P. (2001) Evolution and impacts of community-based forest management in the hills of Nepal, Asian Institute of Technology Thailand.
13. Sawalha, I. (2011) Business Continuity Management and Strategic Planning: The Case of Jordan. University of Huddersfield.
14. Fearn-Banks, K. (2007) Crisis communication: A casebook approach. (3ed.). Mahwah: Lawrence Erlbaum Associates, Inc.; New Jersey.

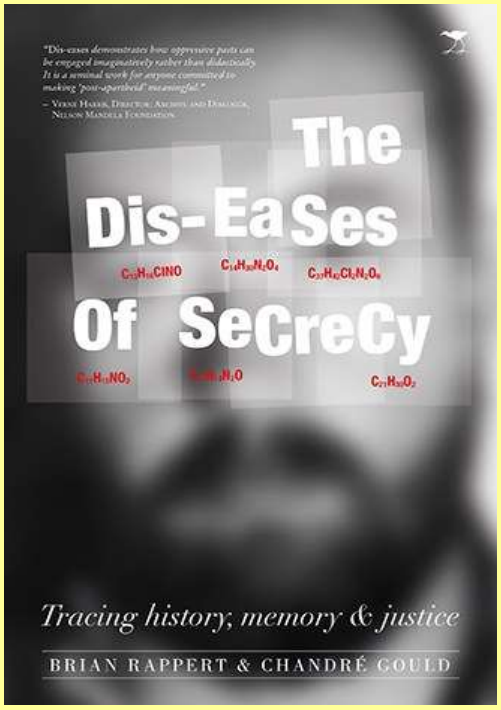
EDITOR'S COMMENT: First of all, the CBRN Lab is an action towards the right direction. On the other hand: (1) Unpreparedness of the civil sector is not a surprise and is consistent to the current situation in almost all countries worldwide. (2) It is good that people trust the ADP and believe that they can handle the situation but reality is a bit different (personal experience). (3) The hospital sector is not ready to deal with mass contaminated victims/casualties. (4) Internet websites and related applications are overrated when comes to dissemination of specialized information and cannot replace traditional teaching of people of all ages. (5) The article addresses the issue of language but does not address the decontamination of female population (local and international) or the lack of female CBRN first responders (at least not in numbers required) to deal with women and children in distress. (6) EWS technologies are nice and useful but they are not the ultimate solution and overdependence on them is not a clever strategy to depend on. We always speak about smart cities and interconnectivity but the human factor will always rule over machines. Even AI – the new fashion – that can certainly help solve certain operational problems, is not enough since it will always be human controlled. It is the human that is the problem! I have spotted all the above from the time I was delivering some classes to ADP personnel some years ago. After all these years I read now what is the situation in 2018 and it is not good. A very rich nation in a fragile geopolitical area, with inspired leaders envisioning and executing unique projects, constructions and innovative ideas whether it is the biggest ambulance in the world, the fastest police car fleet in the world, the tallest building in the world, the biggest artificial islands in the world etc. but still cannot establish a "*CBRN Training Academy*" to provide fast track basic and advanced training in a unanimous way allowing interoperability with the military sector and spreading the knowledge to a wide spectrum of involved stakeholders amongst which population has a prominent role. I wish I had the opportunity to present my vision for such a training facility to HH the Minister of Interior of AD and to explain the necessity but also the urgency of such a proposal. The study mentioned above was most probably conducted at the beginning of 2018 and now we are already in 2019. They disclosed the gaps and identified the attitudes. What did they do to fix them and transform them to lessons learned? I sincerely hope to read about their ongoing actions in a new article describing all the solutions routed after their wake-up article.

Impunity through knowledge management: The legacy of South Africa's CBW programme

Source: https://armscontrollaw.com/2018/12/27/impunity-through-knowledge-management-the-legacy-of-south-africas-cbw-programme/

Book review: Brian Rappert and Chandré Gould, *The Dis-Eases of Secrecy: Tracing History, Memory & Justice* (Jacana Media: Johannesburg, 2017), 261p.

It took me almost a year to write this book review. There are reasons why. First, the book is not that easy to read. While one can read it linearly (that is one page after another, as one would normally do), it instead invites readers to follow the logic of the argument, which entails dashing back and forwards from one part in the book to another. Second, the insights are profound, and the reader needs to let them sink in. Even in a straightforward linear reading mode, it is simply not possible for one to finish the volume in a couple of hours and claim to have understood the authors' arguments. And finally, closely linked to the second excuse, while following the trails of various issue threads, I was simultaneously trying to figure out why it is so difficult, if not impossible, to use a country's past experiences with chemical and biological warfare as a point of departure for education and outreach to prevent the re-emergence of chemical and biological weapon (CBW).



The Dis-Eases of Secrecy tells multiple stories of South Africa's weird CBW activities between 1981 and 1995, commonly known as Project Coast. The stories are not primarily about individuals or their activities. They are about how those individuals or outsiders construct their actions and the narratives surrounding those actions as ways to shape the legacy of Project Coast and define individual responsibilities of Project Coast participants. At the other end of the spectrum stand the victims of Project Coast. Despite the special attention paid to Project Coast by the Truth and Reconciliation in 1997 and afterwards, did the public narrative — incomplete as it still is — bring closure? Facts are different from Truth, but did the Truth that emerged from those hearings suffice to reconcile?

Structuring the threads

How often does one come across a book whose opening chapter of the introductory section is entitled 'How to read this book'?

The whole book is constructed around 11 sutras. A 'sūtra' in Sanskrit means 'thread'; in Buddhism 'narrative part'. A 'thread' can mean a group of intertwined filaments; so little surprise that another introductory chapter is called 'Sewn threads'. Another nod to Sanskrit? 'Sūtra' is semantically linked to 'sīvyati' (he sews). Irrespective of whether etymology or philosophy inspired the authors, their playing around with both words in the chapter title characterises the book well: one has the option to proceed page after page (in which case, one receives a chronological progression of the authors' investigation that led to the book) or one can follow any one of the thematic threads via the red thread identifier and number at the end of paragraphs.

The 11 threads are:

- What was done?
- Total war
- Forgetting and remembering
- Legacies of the past
- Need to know
- International relations
- Best offence
- Silence and the fury
- Transitional justice
- Lessons from the past

- Victims

Inspired by Sven Lindqvist's technique of thread-based entries in '*A History of Bombing*' (2001), both authors equally encourage their readers to take '*one of many possible paths through the chaos of history*' and thus to sense the many different ways a complex social issue can be perceived or experienced.
The threaded approach represents a conscious effort to break through the linearity of communication. As any person will have experienced in an inspired moment, multiple thoughts can near-simultaneously crisscross consciousness and frustrate prose when trying to transpose them into tangible communication. Speak, and phoneme will follow phoneme. Write, and letter will follow letter; word will follow word; and page will follow page. This immutable limitation on verbal communication challenges any author on presenting different angles to an account. A non-linear approach to writing cannot remove this limitation; instead, it places the reader in charge of how and in which sequence she or he wishes to explore individual threads in the narrative twine.
Rappert and Gould use the technique to good effect. Whereas Lindqvist broke with conventional narration to reinforce his view that indiscriminate bombing of civilian targets had its roots in the imperialistic, discriminatory Western views of other cultures, both authors let the reader sense profoundly why a 'fact' (e.g. a reference in a meeting record) acquires meaning only in the presence (or absence) of other information and why 'truth' is a constructed perception based on the selective inclusion of personal experiences and/or access to 'facts' with (selected) meanings.
However, as the previous paragraph makes clear, the technique may be heavy on the reader. It forces one to flip back and forth through the book in search of the corresponding paragraph number while absorbing information just received. Precisely at that moment one will also be processing that information against one's own knowledge and understandings. The flipping back and forth distracts. Yet at the same time, it is difficult to see how the authors could achieve the same intellectual impact without the disruption of the non-linear presentation of arguments. The brain cannot sink into the comfort of a smooth narrative ride.

Challenging the knowledge comfort zone

To most people CBW present a clear-cut case: they are inherently inhumane, the subject of a longstanding and universal taboo on their use and banned under current international law. Therefore, such weapon use is evil and must be condemned by all. Alas, history and current direct challenges to the Biological and Toxin Weapons Convention (BTWC) and the Chemical Weapons Convention contradict the good vs evil tale. (See my paper *International Norms Against Chemical and Biological Warfare: An Ambiguous Legacy*.)
The dichotomy between victim and perpetrator is similarly built on such binary approach. Yet, the types of attributes assigned to each category of persons will be asymmetric. Observation or allegations of collective and individual actions violating the norm or treaties against CBW will feature prominently when designating a perpetrator. In contrast, a range of broad-scope characteristics not specifically related to CBW will habitually define the victim. As Rappert and Gould write (para. 212):
In relation to everyday offences, the 'ideal victim' is generally someone that is regarded as weak compared to the offender (which often translates into being female, very young or elderly), blameless for what transpired, a stranger to a clearly reproachable offender and, importantly, able to elicit sufficient concern about their plight without threatening other interests.
Victimhood becomes more difficult to circumscribe if one begins to consider people who participated in trials involving exposure to CBW agents. Even if the test subjects were volunteers, questions arise as to whether they were facilitators of crimes to be committed later (by others) with weapons they helped to optimise, they had been adequately informed of the risks to their health posed by the experimental agents, how free their choice to participate in such trials was, and so on. The authors also point to potential social and other consequences for the children of staff after Project Coast made press headlines (see interview with a Project Coast scientist, para. 486) and the veil of secrecy behind which many of the activities took place was ripped open in certain parts (but never fully removed). As they note, such children fit several expectations of 'ideal victims',

but just like with relatives of victims who suffered physical harm from CBW use, they only receive secondary consideration.
If 'victimhood' suits political discourse or emotional mobilisation well, then varying degrees of vagueness or abstraction will likely hamper criminal prosecution of the alleged perpetrators. More specifically, how will a specific action by an alleged perpetrator be linked to a specific victim? Rephrased more broadly, how can justice be obtained in CBW cases?

Secrecy, justice and reconciliation
A reply by Dr Wouter Basson, Project Officer of Project Coast, to the question why he does not seem to understand what he did wrong in a radio interview best illustrates the quandary (para. 6):
It's very simple, they must just show me what I did wrong. It's easy, all they need to do is bring one single case of anybody that was either damaged and/or hurt in this process and I'll live with it. But nobody can do that. I mean it's been 20 years that this has been going on and there is not a single scratch and/or blue mark and/or bruise on anybody that could be proven anywhere, so who did I damage and how?
Much of the book turns around two questions: Was there justice for the victims of Project Coast? Did the Truth and Reconciliation Commission (TRC) reconcile victims and perpetrators? The quest to answer those questions raises further questions: How is Project Coast being remembered? How is it being forgotten? And by whom? Indeed, beyond the victims and perpetrators (and their relatives and social communities), other categories of protagonists also play or have played substantial roles in shaping the legacy left by Project Coast. These include government leaders and officials under the Apartheid regime; the post-Apartheid government and officials from the African National Congress (ANC); members of the military and security forces; the scientific community and research institutes; TRC members, research staff and other officials; civil society; the press; and the international community. And probably many more …
Secrecy is an all-pervasive element in the book. Through compartmentalisation and an overall policy principle to disseminate information on a need-to-know basis, few people (if any) had a total overview of Project Coast. It also allowed people who came to suspect certain things through casual conversation to ignore inconvenient knowledge; and later, before the TRC, it enabled people to claim ignorance about certain goals or actions, or deny or minimise their responsibility in them. The fact that Project Coast comprised so many different elements, so many different institutions, without clear lines of overall oversight or even management, easily reinforced the utility of secrecy in 'forgetting'. Paradoxically, the promise of amnesty offered by the TRC to persons willing to admit to norm-breaking or criminal activities as part of the reconciliation process generated exaggerations of complicity. These also tended to obscure rather clarify the past, more so as secrecy and compartmentalisation of knowledge precluded deep verification. One never obtains the certainty that all is (or can be) known and what is supposedly known may be suspect. Ultimately, guesses must fill the gaps, but nobody or nothing can confirm or refute those guesses.
Secrecy was also claimed on the level of national security. However, as Rappert and Gould write (para. 220; emphasis in original):
What the state itself was 'allowed' to know was limited to what was officially told. The new ANC state needed to protect the state secret that it did ***not*** know. What the Project Coast scientists would say when under questioning at the TRC was wholly unknown.
Add an overlay of 'proliferation risk' to whatever might become publicised, and the 'secret' got new keepers. Thus, the post-Apartheid government became the owner of secrets, whose contents it did not and could never fully know. Its officials are today extremely reluctant to talk about Project Coast. Both authors tested, for instance, whether it might be useful for South Africa to at least come clean internationally by revising the information submitted under a BTWC Confidence-Building Measure (CBM) on past biological weapon (BW)-related activities. This was rejected, and Rappert and Gould were strongly encouraged not to pursue this line of enquiry by the (British) funders of their project. The latter aspect also demonstrates international community's contribution to the way Project Coast will be remembered. One international expert suggested that Project Coast was not a typical BW programme and therefore no need exists to discuss it under the

BTWC. Some other diplomats held the view that there is no longer any urgent reason to press South Africa on revising its CBM because the nature of the government had changed, the country had re-entered the international community, and it had stopped the programmes. Even though the authors also interviewed other experts and diplomats holding opposite views, the key point remains that consensus on the step was and remains elusive.

In conclusion

Rappert and Gould present a complex, but nonetheless compelling narrative about how a community – in this case, South Africa – addresses the legacy of a CBW programme and the use of such weapons in an armed conflict. Ultimately, the reader is left with the question: what is justice? Dr Wouter Basson in many ways epitomises the complexity of the question: he testified before the TRC; he faced criminal charges; and he was taken to justice for breaching his professional code of conduct by the Health Professions Council of South Africa (HPCSA). Only in the latter case he was found guilty in December 2013 but procedural battles before the HPCSA and in courts have thus far blocked his sentencing. Would a final guilty verdict in this case bring closure to the victims? To answer, one may refer to the widow of one of the victims of the 1995 sarin attack against the Tokyo underground after learning that senior Aum Shinrikyo members had been hanged. She said that the executions did not bring closure to survivors or victims' families and pledged to continue efforts to ensure that the crimes are not forgotten (*Sarin victim's widow comments on execution*, 26 July 2018; and *Aum victims and bereaved express sense of closure, disappointment and confusion over executions*, 6 July 2018):

What I mean by this is that there are lots of things I wanted them to talk about so we can learn more about future counterterrorism. I really wanted them to speak to experts, for example. It's a disappointment that they can no longer do this.

Arguably, in this instance the direct linkage between perpetrator and victim was much clearer than for Project Coast. Yet, closure does not equal vengeance or mere punishment. It seems to imply the retention of future common value derived from the experiences suffered. It needs to have meaning; remembrance serves the purpose of preventing recurrence.

Towards the end of the book, Chandré Gould reflects on the outcome of the research and the role she and Brian Rappert might come to play in preserving the memory (para. 528):

[…] While most South Africans of a certain generation are likely to be familiar with the name Wouter Basson, artefacts, documents or accounts of the programme are not to be found at significant sites of memory, such as Freedom Park or the Apartheid Museum. What is the reason for this absence of a narrative? I would posit that this has to do with the absence of a coherent, easy-to-relate narrative. With no victims and no voices, or testimony post-TRC to assert the needs or interests of victims, the narrative, staccato and broken as it is, becomes a narrative of 'perpetrators. It becomes a story of motives, intentions and possibilities, all of which have been contested. The stories told by willing witnesses were both ridiculous and horrific, a science fiction of apartheid. Basson, as the person who holds all the answers but refuses to release them, becomes not only the secret-keeper (and in this maintains tremendous power over those who believe they might have fallen victim to the programme) but also the focus of all the attention.

The absence of a victim narrative or account also serves to strip the narrative of credibility or resonance. Personalising the violence of apartheid through victim narratives and testimony rendered it visible. In this case, there was no victim (other than Frank Chikane) to associate clearly with the programme, and no one other than the investigator to keep making the case for its importance or relevance. In this situation, the person investigating becomes the story-teller and the person responsible for the victims' untold victim stories, the placeholder until a more legitimate voice can be heard.

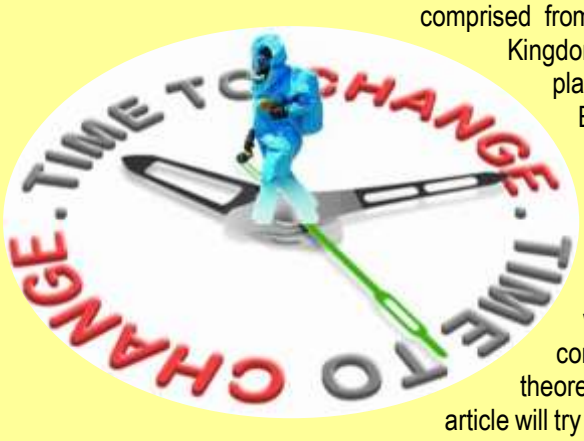
In one of my many discussions on how to use past experiences with CBW in education and outreach, I happened to mention Project Coast, citing a museum exhibition entitled *Poisoned Pasts* then underway. One member of the group, a retired South African academic, replied, '*This is controversial*'. To me, controversy is a good foundation for discussion. Alas, as I have now learned, in plain English the three words meant: '*Do not touch*'.

Thus, one remains stuck with three cardinal questions: What lessons can be *identified* from past CBW programmes? What lessons can be *learned* from those activities? And, how can these insights help *preventing* the re-emergence of CBW programmes?

RESHAPING OUR CBRNE RESPONSE PLANS

By BrigGEN (ret'd) Ioannis Galatas, MD

Athens 2004 Olympic Games was the first Summer Olympiad after 9/11 catastrophe and the subsequent anthrax letters' global scare. Therefore, a CBRN security plan was included for the first time in the overall security plans accompanying all mega sport events. This plan was designed by a group of Greek civilian-military experts (author was amongst them) in collaboration with the Olympic Security Advisory Group comprised from experts from 7 countries (United States, the United Kingdom, Germany, Israel, Australia, France, and Spain). Same plan with minor differences was advocated in following 2008 Beijing Olympic Games and 2012 London Olympiad – and most probably is about to be implemented during the Rio 2016 Olympic Games in a *copy-and-paste* procedure traveling from one organizing country to the next one.



But is this plan good enough to be trusted or do we have to revise it or even change it completely? One might wonder why changing a plan that have never be tested to conclude if it is good or not with another that will also be theoretical until tested under real operational environment? This article will try to pinpoint the pros and cons of the "old/current" plan and propose a new approach where advantages will minimize deficiencies and fill certain existing gaps. Of course "*no plan survives contact with the enemy*" (German Field Marshal Helmuth Karl Bernhard Graf von Moltke The Elder [1800-1891]) and "*a bad plan is better than no plan at all!*" (Emmanuel Lasker – German chess player, mathematician, and philosopher who was World Chess Champion for 27 years [1894-1921]) But if we can make a plan better why not give it a try?

The CBRNE threat

The CBRNE acronym replaced old (Cold Era) NBC first as CBRN and later on as CBRNE. In terms of emergency in urban environment this term should be coined to CRE for two reasons: (1) because B-threat is a gradually progressing emergency depending on the incubation time of the agent released; and (2) because the N-threat is quite remote (but always present).

The release of C/R agents could be overt (attacks in Syria) or covert (Tokyo sarin incident), with or without an accompanying explosion (i.e. RDD/RED). A secondary IED is always expected on site aiming First Responders.

A CR attack can take place during a mega event but also during a normal day. Capital cities and small towns can be equally become targets.

A CR attack can happen in: (1) an anticipated "single" target (i.e. opening/closing ceremony in a mega sport event); (2) "multiple" targets in the same city during a mega event or "multiple" targets in different cities; (3) other target distant to main mega event venues. Agents released can be either "C" or "R" alone or combination (CRE).

The "old/current" plan

According to this plan the state's CBRNE response plans follow the timeline below:

- Notification of an incident resulting in casualties in a mass gathering place (i.e. stadium);
- Traditional First Responders (police, fire service, ambulance service) rush to the scene;
- Initial evaluation of the scene is indicative that it is not a traditional explosion or that victims experience symptoms and signs resembling release of hazardous materials.

- General state alert and activation of specialized First Responders rushing to the incident site;
- When on site they deploy their decontamination equipment, dress their PPE (usually Level-A) and enter the Warm Zone to extract victims;
- Fast triage is conducted in place;
- Ambulatory victims are directed to a mass decontamination tent;
- Non-ambulatory victims are decontaminated and roper First Aids are provided;
- Following verification of successful decontamination, "clean" victims are transferred to the nearest hospital for further evaluation (triage) or hospitalization if in serious condition.

The Tokyo subway sarin experience (March 20, 1995)

- There was no bomb explosion;
- Commuters were exposed to sarin vapors (purity: 30%) released from a plastic bag left in one of the wagons during rush hours with hundreds of passengers stepping in it;
- Many commuters experienced symptoms and signs of exposure to chemical warfare agent in many stations of the subway system;
- Severely affected victims remained in place unable to move or escape (estimated ~20%);
- Those with less severe symptomatology (~80%) escaped the scene and rushed to the nearest hospitals on their own (by foot, with taxis, cars, motorcycles, buses);
- Although St. Luke's bore the brunt of the disaster (641 patients that day, and over 1,400 patients the following week), 278 Tokyo hospitals and clinics saw 5,510 patients, seventeen of whom were deemed critical, thirty-seven severe, and 984 moderately ill. The cases classified as moderate complained only of vision problems (e.g., myosis). In all 5-6,000 persons were exposed. 3,227 went to hospital, of whom 493 were admitted to 41 of Tokyo's many hospitals. Only 17 developed severe symptoms requiring intensive care. In all twelve people died from the sarin exposure;
- Of the 1,364 firefighters who rushed to the various subway stations, 135 reportedly were injured while attending to victims. This number equates to roughly 10 percent of the firefighters, but the injuries were not of a serious nature. At St. Luke's, the medical staff saw a few symptomatic police and a group of about twenty firefighters, who exhibited only mild effects (e.g., eye problems, headache) and were therefore released in the afternoon. Similarly, a total of 135 Tokyo EMTs, or about 10 percent of those who responded on March 20th, showed exposure symptoms and required medical treatment. The majority of these EMTs became symptomatic while transporting patients, probably because of off-gassing from the victims in the poorly ventilated ambulances. Authorities ordered the windows of ambulances opened which alleviated the problem. The secondary exposure problem in Tokyo was not too grave because no rescuers required antidote treatment. Although the on-scene rescuers after Aum's June 1994 attack in Matsumoto were similarly vulnerable, just over 7 percent of the first responders there became symptomatic, and only one of the affected rescuers sought medical assistance."
- It took almost 3 hours to recognize the nature of the agent released
- Two workers died after they removed the newspaper that had concealed the agent and absorbed some of it.
- Because no information that the incident was caused by poison gas was available in the first few hours of the attack, patient decontamination was not initially attempted, and 23% of the 472-house staff that were exposed to contaminated patients showed signs of sarin poisoning.
- 85 percent of the patients were "psychogenic cases," or worried well. Mathewson claimed, without a supporting reference, that 9,000 psychogenic patients presented themselves to local health care facilities.

Pros of existing plans

Just the existence of a plan leading to a deployment of forces in order not to be accused that the state under attack was not prepared to deal with new emerging threats. This along with the realistic excuse that no nation worldwide is able to counter such an attack in urban

environment no matter how strong the nation is or how thoroughly it is prepared. This combination will provide a subconscious reassurance to populace that the problem was immense to handle but we did our best to confront it. Partially true! But what if we can do better and greatly minimize the consequences of such brutal attack?

Cons of existing plans

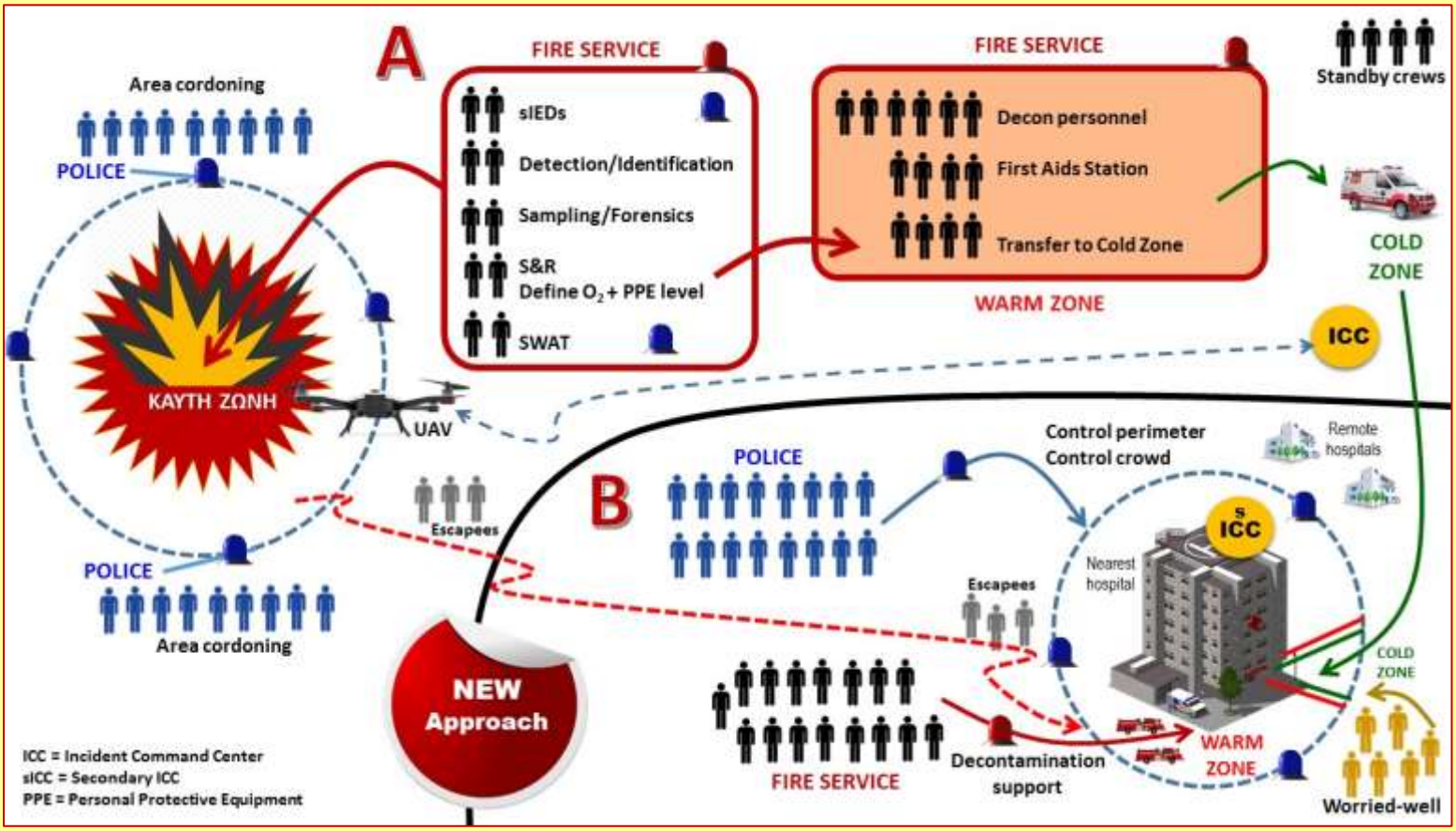
- Problems identified in the aftermath of Tokyo sarin attack indicate the importance of three important numbers mentioned above: (1) ~20% will remain in place (dead, severely wounded or contaminated or both); (2) ~80% will escape the scene and rush to all hospitals and clinics in the affected city; and (3) worried well in a ratio approximately 1:5 (contaminated vs. worried well) will overwhelm hospitals or lead health system into collapse.
- Due to traffic jam (prominent in many big cities and capitals of today) heavy response vehicles will not achieve their normal times of intervention (i.e. 5-15 min for ambulances or fire engines). First Responders cannot fly and victims will surely not wait for them (especially when information about chemicals' release will become virulent among the public). And do not count on the fact that emergency lanes would be free of cars and that traffic deviations will be effective with the press of a button!
- Traditional First Responders most probably will be victimized due to lack of personal protective equipment and specialized knowledge and training.
- All victims will end up at the hospitals.
- Hospitals (especially those in close proximity) do not have fixed decontamination stations and adequately trained personnel to deal with mass CR casualties.
- CBRNE Medicine is not included into the curricula of universities' medical and nursing schools. In that respect why do we expect front-line health professionals to be able to recognize the signs and symptoms of such an attack?
- Populace that is the most important player in every state's CBRNE response plan is emphatically left out of the game conjuring the global excuse of "not to panic the people!"

The proposed approach – see graphic below

The new proposal is based on four pylons: (1) The fact that casualties will end up at all city's hospitals and clinics; (2) The fact that First Responders will not approach Hot Zone on time; (3) The fact that EDs personnel (and hospitals) are not able to recognize and manage mass CR casualties (but also B-casualties as it was recently proven with Ebola virus outbreak – or better pandemic); and (4) The fact that populace is totally unprepared to follow directives in case of CBR release. To the above one can add the renewed interest of terrorists (mainly Islamic State) on the possibility to use CBR agents against their enemies both in their areas of operations and in our part of the world.

Based on the above, the proposed plan's timeline could be unfolded as following:

- Notification of an incident resulting in casualties in a mass gathering place (i.e. stadium);
- Traditional First Responders (police, fire service, ambulance service) rush to the scene;
- Initial evaluation of the scene is indicative that it is not a traditional explosion or that victims experience symptoms and signs resembling release of hazardous materials.
- Traditional First Responder put their "escape hoods and rubber gloves" on (standard operational gear) and establish a pre-defined cordon (e.g. 500m-1km) around the incident site (Hot Zone);
- At the exit sites of the roads leading away from Hot Zone they guide escaping victims to a given hospital destination (if affected from agents released) or an assembly point (if not obviously affected); police make necessary traffic deviations to provide fast access to people on foot or vehicles of all kinds. If the nearest hospital is at a distance for those on foot then fire service will guide them through "water curtains" (high volume, low pressure [60psi] "wet" decon), redress them and load them into mass transportation means that will carry them to destination hospital(s).



- In parallel CBRNE/HAZMAT First Responders fortify the premises of nearby hospitals (crowd control, decontamination facilities, First Aid Stations etc). At the same time specialized responders' approach and enter the Hot Zone to conduct specific duties as fast as possible (due to time/oxygen limitations of their Level-A PPE): (1) scene assessment, casualties at scene, exploitation for secondary IEDs, sampling [air, liquid, soil], detection (CRE) and report to HQ or Incident Commander. They can be accompanied by ground robots (UGVs – for expected victims' evacuation and later for collection of dead bodies). Simultaneously UAVs map the incident site and together with info provided by entry teams state's experts design the contaminated plume released and its direction within the urban web.
- Contaminated plume might require "sheltering-in-place" and populace act accordingly because they are aware what this means and how to do it.
- Hospitals and front-line health professionals recognize the "toxidrome" (a portmanteau of toxic and syndrome) as a result of their university training and drills and act accordingly in a safe mode.

Practically instead of First Responder going to the Hot Zone, I propose Hot Zone victims' going to First Responders. This approach overcomes the following gaps present in current planning: (1) traffic jam/late arrival; (2) uncontrolled inflow of victims at hospitals; (3) unavailability of hospitals' decon stations; (3) uncontrolled flow of worried well; and (4) escape of mildly contaminated victims returning to their homes.

New proposal is not easy to accomplish since it requires careful study and continuous updating of targets and cordon/redirection/management process. But when the new prototype operational algorithm is set then it would be easily applicable to any given CRE incident saving time that equals lives.

Testing the new approach

Drills are the tools to test any plan. But we have to change the way we conduct drills as well. Usually CBRNE drills: (1) end the moment that casualties are inside the ambulances; (2) are

organized in a pre-defined date and time; (3) are conducted during working hours. These common global features have nothing to do with reality! In that respect and following the right procedure of preparation (education-training-tabletop exercises-in-hospital drills) we have to simulate real life into specialized drills. A high official arrives at the ED of a major hospital and declares the type of drill (e.g. C/R/E or CE/RE). This can be done at 07:00 or 19:00 or in a national holiday or during summer vacations. Because this is when bad things happen in real life!

Same realistic conditions apply for the scenarios tested as well. Take for example the "single" attack in a "given" target like the opening ceremony of Olympic Games. In a setting like this all our response forces are in high alert surrounding the venue-target. But do you think it is possible to control the out coming flow of 80,000 contaminated spectators? Can you imagine the space we need to deploy our assets and the huge effort when comes to crowd control – not to mention the sources that would be needed during the first hour following the incident. We design scenarios where a small airplane sprays a deadly chemical over the stadium and then we confront the casualties as if they were 100 or 200 the most. Play the game with 1,000 and you will see the difference! Play it with 10,000 and you will see the Apocalypse – this is war not terrorism!

CBRNE Medicine

So far in all mega events' organizers and nations give priority to the Hot Zone intervention (80%) and only small portion (20%) of the overall budget is allocated for medical/hospital response. Whether we like it or not, the consequences are of medical content and they might last for days, months or years (personal experience following a medical training organized by OPCW (2003) during the preparatory phase for 2004 Olympic Games in a central military hospital in Tehran where thousands of chemical victims from the Iran-Iraq war (1970s) were still treated on daily basis). Inclusion of "CBRNE Medicine" into the curricula of medical/nursing university schools is mandatory and will enhance both the knowledge and differential diagnosis capabilities of future front-line health professionals manning EDs of our hospitals. A second step towards the same direction could be a "European CBRNE Medical Training Academy" providing unanimous training (both theoretical and practical/hands-on) in a massive way to EDs physicians and nurses of major hospitals in all EU member-states.

International cooperation and assistance

We must keep in mind that each and every country will face the CRE crisis alone. There is no time to wait for international assistance (means and experts) and if given (even within hours) it would be too late to be effective due to the nature of the agents released. International cooperation and assistance would be surely effective during the prevention period (intelligence sharing, training, etc) and the aftermath period (rehabilitation, massive ground/infrastructure decontamination, bone marrow transplantation etc).

Populace awareness campaign

Modern populace all over the world grew up not only into contact with traditional disasters (wildfires, massive floods, catastrophic earthquakes/tsunamis etc) but also by watching live wars, conflicts, bombings, decapitations, chemical weapons usage in urban areas to name a few of 21st century terrifying threats. It would be naïve to support the "panic" excuse. If we manage to accomplish a successful CBRNE awareness campaign we will achieve to incorporate populace as important asset to our response plans. If we start this campaign from elementary schools all the way to professional groups then, half the battle would have been won. Simple measures and basic information might one day save the lives of many. It has been done for earthquakes; why not for new emerging threats. Knowledge is power and sharing this power will have a positive effect in the overall state defense and life continuation.

In conclusion

"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!"

Sir John Harvey-Jones (BBC "Troubleshooter" series)

Experience has shown us that there is a gap between the planning phase and the actual "human" response to major incidents, especially chemical ones. Hence, human factors must be taken into consideration during preparation as plans designed on ideal responses (old/current plan) from both citizens and emergency responders will simply fail. Plan for what people will actually do, not for what they should do (new approach/plan). In that respect CBRNE planners should be characterized by two qualities: (1) personal hands-on experience on CBRNE operations and peculiarities (in most cases they do not); and (2) be able to sincerely answer a very simple question: "What would have been my personal reaction if I was involved in a real C(B)R(N)E incident in my living environment". Rio2016 Olympiad is only 18 months away and perhaps it is a good time to think of reshaping our CBRNE response on more solid and logic grounds. ■

Sources

Carol Migdalovitz (2004): **Greece: Threat of Terrorism and Security at the Olympics.** CRS Report for Congress (RS21833). http://www.fas.org/irp/crs/RS21833.pdf

Robyn Pangi (2002): **Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System.** BCSIA Discussion Paper 2002-4, ESDP Discussion Paper ESDP-2002-01, John F. Kennedy School of Government, Harvard University http://belfercenter.ksg.harvard.edu/files/consequence_management_in_the_1995_sarin_attacks_on_the_japanese_subway_system.pdf

Fred P. Stone (2007): **The "Worried Well" Response to CBRN Events: Analysis and Solutions.** The Counter-proliferation Papers Future Warfare Series No. 40; USAF Counter-proliferation Center, Air University Maxwell Air Force Base, Alabama http://fas.org/irp/threat/cbw/worried.pdf

Judith Mathewson (2004): **The Psychological Impact of Terrorist Attacks: Lessons Learned for Future Threats.** Homeland Security Papers, eds. Michael W. Ritz, Ralph G. Hensley, Jr., and James C. Whitemire. Maxwell AFB: USAF Counter-proliferation Center; p.197.
http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hls_papers/mathewson.pdf

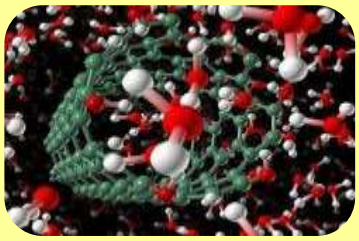
'Nanoscavengers' could protect people from sarin gas, other nerve agents

Source: https://www.sciencemag.org/news/2019/01/nanoscavengers-could-protect-people-sarin-gas-other-nerve-agents

Jan 02 – In the 1980s, thousands of Iranians were killed from exposure to the nerve agents' sarin and tabun unleased by Iraqi forces. Similar chemicals have been used against soldiers and civilians in recent wars and terrorist attacks. Now, researchers are reporting a new therapy that may be able to provide long-acting protection against these agents. **Though the treatment has only been tested in rodents, some scientists say it could one day prevent lasting brain damage or death in people exposed to these deadly chemical weapons.**

Nerve agents like sarin belong to a family of chemicals called organophosphates. Although some of these compounds are widely used in much lower concentrations as pesticides, the nerve agents are highly lethal because they get into the body quickly through the respiratory tract, eyes, or skin. Once inside cells, they inhibit an important enzyme whose normal function is to break down acetylcholine, a neurotransmitter that helps muscles contract. When too much acetylcholine builds up, victims experience violent muscle spasms and eventually stop breathing.

Current antidotes must be given as soon as possible, and although they can help mitigate the symptoms of poisoning, they don't act directly on nerve agents. As a result, researchers have been trying to develop prophylactic "scavenging" molecules capable of seeking out and degrading nerve agents in the body upon exposure. But such "bioscavengers" have only been able to provide brief protection in various lab animals, and no such therapies have been approved by the U.S. Food and Drug Administration.



In the current study, researchers at the University of Washington in Seattle tried a new tack. They wrapped an organophosphate-targeting enzyme called OPH in a flexible polymer gel coating. The end result was nanometer-size particles capable of going undetected by the immune

system and staying in the body longer than the enzyme alone. When given before exposure to nerve agents, the nanoparticles clear the chemicals from the bloodstream.

Rats given a single injection of the "nanoscavenger" were completely protected against organophosphate exposure for up to 5 days without side effects. In treated guinea pigs, the nanoscavenger protected animals from multiple sarin injections for 8 days, the team reports today in *Science Translational Medicine*.

The nanoscavenger could essentially act as a vaccine in people, says chemical engineer Shaoyi Jiang, a member of the team. If the therapy is optimized, the protection could potentially last for weeks or even months, he says.

Previous bioscavengers haven't remained in the body long enough to confer protection, or they've sparked the body's immune system to neutralize the antidote with antibodies, notes Jin Montclare, a protein engineer at New York University in New York City, who was not involved with the study. The new work appears to circumvent both of these concerns, she says.

Nerve agent nanoscavengers would be most practical for people who are at high risk of exposure to the chemical weapons, such as soldiers or first responders going into a contaminated area, says Janice Chambers, a toxicologist at Mississippi State University in Starkville who wasn't involved in the work. But she says the therapy probably wouldn't be useful for short-notice assaults such as terrorist attacks. "By the time you would be exposed and showing the signs of tremors or convulsions, it would be too late" to give the treatment.

The authors say the treatment could also help protect people working with certain pesticides. According to the World Health Organization, pesticides containing organophosphates cause 200,000 poisoning deaths per year in developing countries.

Next, the researchers plan to test how long the nanoscavenger works in monkeys, and they will also see whether multiple doses can be given. After that, a clinical trial would be needed to test the safety of the therapy in humans.

Methodology: How we Tracked the Illegal Shipment of Sarin Precursor from Belgium to Syria

Source: https://www.bellingcat.com/resources/case-studies/2018/04/19/methodology-tracked-illegal-shipment-sarin-precursor-belgium-syria/

On 18 April 2018 Syrian Archive and Knack revealed information that Belgium violated EU sanctions against Syria according to the summons of an upcoming lawsuit. The Belgian customs found that without having requested the appropriate export licenses three Flemish companies have exported 96 tonnes of isopropanol in a concentration of 95% or higher to Syria since sanctions came into force in September 2013.

The Syrian Archive has worked with Belgian news outlet Knack on this investigation for the past year. All of the information was publicly or collaboratively sourced through searching online databases, submitting Freedom of Information Requests and requesting statements from authorities, courts and companies involved.

This article documents some of the open source investigative methods employed in our investigation that discovered several key pieces of information.

Global trade figures

Syrian Archive staff began our investigation in the aftermath of last year April's sarin attack in Khan Sheikhoun in which the Organisation for the Prevention of Chemical Weapons (OPCW), that oversees compliance with the Chemical Weapons Convention, examined samples from and around the impact crater in Khan Sheikhoun, finding in laboratory tests that isopropanol was used in the production of sarin used in the attack.

We consulted The UN Comtrade database to identify whether any shipments of isopropanol, a sanctioned chemical from EU Member States to Syria, were reported after sanctions were put in place in 2013. Comtrade, coordinated by the United Nations Statistical Division, collects monthly and annual trade statistics from more than 170 countries and displays these figures online in a public, downloadable and queriable format. The OCCRP similarly queried the Comtrade database in their investigation of Croatian arms sales being diverted to Syria.
Below is a walkthrough of the search we conducted on the Comtrade database.
While amounts reported to Comtrade may potentially under-represent true trade export figures due to self-reporting bias, the data shows that since 2014, an estimated 1.28 million kilos of propanol and isopropanol were exported by various countries to Syria (both propanol and isopropanol are registered under the same code). See below:

Reported exports of isopropanol and propanol to Syria in kilograms (2013-2017)

	Year of Year				
Reporter	2013	2014	2015	2016	2017
Belgium		22,000	20,000	72,160	
China		1,920		640	
India			26,000		
Lebanon	12,800	25,600		279,120	
Malaysia				39,120	
Netherlands				1	
Other Asia, nes			38,000		
Rep. of Korea	64,000	115,200	76,800	51,200	
Singapore			117,386		
Switzerland		5,120			
Turkey	16,026	2,055	6,010		12,645
United Arab Emirates	217,546	174,720	195,440		

Source: UN Comtrade. Reported exports of isopropanol and propanol to Syria in kilograms (2013-2017)
The distinction between propanol and isopropanol is essential. While isopropanol in concentration of 95% or higher is prohibited without prior approval, propanol is not.

Data collectors
In order to find out whether the figures provided by Comtrade referred to propanol or isopropanol, we contacted the Trade Statistics Branch of the United Nations Statistics Division in April 2017 to inquire as to whether disaggregating figures was possible. Comtrade confirmed that they only have a single code in use for both for propanol and isopropanol (HS 290512). As a result, divorcing isopropanol from propanol figures within Comtrade figures was not possible.
In May 2017, we requested any additional information from the European Commission Service for Foreign Policy Instruments Restrictive measures team to inquire as to whether any Member States sought authorisation for the trading of isopropanol to Syria. In their answer, the European Commission stated they were "not in a position to provide advice on whether a concrete product falls under the technical specifications of an Annex to a Regulation" and that "Responsibility for the application of EU restrictive measures falls with the competent authorities of each Member State, as listed in Annex III to Regulation 36/2012."

Through the Comtrade database we found that Belgium was the only EU Member State to continue exporting propanol/isopropanol to Syria since sanctions came into force in 2013, so we decided to focus efforts on investigating Belgium.

Courts and industry

Reaching a roadblock, and needing in country expertise, we reached out to investigative reporter Kristof Clerix of Knack, a Belgian weekly magazine. Clerix wanted to see what was going on out of public view and begun to file Freedom of Information Requests to various Belgium entities.

Belgium is divided into three regions: Flanders; Brussels; and Wallonia. Each with their own freedom of information policies. In Flanders, information about export licenses is published by the authorities on a monthly basis in public documents. So Clerix submitted Freedom of Information Requests to the other two regions.

Brussels and Wallonia replied to Freedom of Information Requests stating that no licenses were requested for the approval of isopropanol export to Syria during the 2013-2017 period.

After receiving those answers, Clerix also contacted Essenscia, the Belgian chemical sector umbrella organisation. After waiting six months to hear back, Essenscia stated that after extensive research and consultation with relevant stakeholders, it seemed "most likely that the export of (iso)propanol from Belgium to Syria is related to a trading company that has purchased the product abroad and then has handled it and exported it via Belgium." Continuing on, the statement explains (emphasis in original):

"We have no indication whatsoever that the exported (iso)propanol to Syria has been produced or shipped by a chemical company located in Belgium. Moreover, the exported goods are fully approved by the customs authorities who severely monitor any trade with Syria since several years. All of this indicates that our country and our industry, who both support the Chemicals Weapons Convention and the Organisation for the Prohibition of Chemical Weapons (OPCW) in every possible way, cannot be linked to the intolerable incident in Syria."

The statement was proven inaccurate by court documents received in subsequent months.

A publicly available document found by a Belgian expert consulted by Clerix revealed that in October 2016 in the Flanders region, authorities denied a permit request, preventing the export of €1.93 million of banned dual-use chemicals to Syria specified under Annex IX of the European sanctions against Syria. It has been confirmed by the Flemish authorities that this did not relate to isopropanol.

Belgian Customs confirmed that indeed shipments of (iso)propoanol to Syria had been made, although propanol and isopropanal figures were not disaggregated.

According to the summons cited by Antwerp Criminal Court press judge Roland Cassiers, a criminal case is currently being pursued by Belgian customs against three companies and two individuals. This case is set to begin on the 15 May 2018.

Our year long investigation revealed many key pieces of information located through open source investigative techniques. The Syrian Archive along with Knack will continue to pursue and document the case as it unfolds.

▶▶ Read the comments related to this article, at source's URL.

Over 63,000 Iranians Suffer Chemical Weapons Injuries

Source: https://ifpnews.com/exclusive/over-63000-iranians-suffer-chemical-weapons-injuries-statistics-say/

Jan 05 – **An Iranian official says statistics show more than 63,000 Iranians are confirmed to be suffering from chemical weapons injuries and the number is still increasing, thirty years after the devastating invasion of Iran by Iraq came to an end.**

"According to estimates, around 400,000 people were exposed to chemical gas during the Iran-Iraq war. The injury of over 63,000 of whom has been confirmed by medical commissions," said Mohammadreza Sediqi Moqaddam, the head of the chemical warfare victims of the Foundation of Martyrs and Veterans Affairs.

He noted that over 100,000 people had undergone medical treatment following the Iraqi chemical attacks, but some of them did not suffer long-term complications, Fars News Agency reported.

"These [63,000] people have been diagnosed with chronic complications and approved to be disabled by medical commissions," he noted.

The medical commissions are still active as injuries caused by chemical warfare agent exposure could go severe anytime, underlined Sediqi Moqaddam.

Iran has accused western governments, notably France and Germany, with providing the former Iraqi dictator with requirements for building chemical weapons.

Sardasht in western Iran is the first town in the world to be attacked with poisonous gas and the third city, after Japan's Hiroshima and Nagasaki, to be deliberately targeted with weapons of mass destruction. In total, the Iran-Iraq war left over 225,000 Iranians martyred and over 574,000 people injured.

EDITOR'S COMMENT: A good opportunity to reschedule the CBRN preparedness funds distribution issue. Instead of spending 80% for on site response and 20% for the medical/hospital sector where ALL casualties end, we should reverse it and make the allocation of funds more pragmatic and logic since the consequences of exposure will last for decades. If one wants to actually meet chemical victims try to attend the special course that OPCW organizes from time to time at the Baghiyyatollah al-Azamof Military Hospital in Tehran. Only then, you can see things in a different way.

Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies

Source: https://www.gao.gov/assets/700/695981.pdf

Terrorism, WMDs, climate change today's critical challenges: Sushma Swaraj

Source: http://www.newindianexpress.com/nation/2019/jan/09/terrorism-wmds-climate-change-todays-critical-challenges-sushma-swaraj-1922883.html

Jan 09 – **Terrorism, proliferation of weapons of mass destruction (WMDs) and climate change are the three critical challenges the world is facing today, External Affairs Minister Sushma Swaraj said on Wednesday**.

"There was a time when India would talk about terrorism, and it would be treated as a law and order issue on many global platforms," Sushma Swaraj said while addressing 2019's Raisina Dialogue, India's flagship annual geopolitical and geostrategic conference, organised by the External Affairs Ministry in partnership with the Observer Research Foundation (ORF) think tank.

"Today, no country, big or small, is immune from this existential threat, particularly terrorism, actively supported and sponsored by states," she said.

"In this digital age, the challenge is even greater, with a greater vulnerability to radicalisation."

Sushma Swaraj recalled that in 1996 India proposed a draft Comprehensive Convention on International Terrorism (CCIT) but lamented it has remained just a draft till today "because we cannot agree on a common definition".

"Ensuring zero-tolerance towards terrorism, and those who use it as an instrument of convenience, is the need of the hour," she said. The second threat, she said, is the threat of proliferation of WMDs.

Thirdly, she said, developing and under-developed nations are the worst victims of climate change, with neither the capacity nor the resources to meet the crisis.

"We have risen to meet the challenge. India, in partnership with France, launched the International Solar Alliance (ISA) with the participation of 120 countries," Sushma Swaraj said.

In her address, she also outlined the five elements of India's global engagement over the last four-and-a-half years.

Firstly, Sushma Swaraj said, India has rebuilt its bridges with its immediate and extended neighbours.

"In particular, Prime Minister's strategic vision of SAGAR has spurred a qualitative transformation in India's engagement with the Indian Ocean Region in recent years," she said.

"Our revitalised Act East and Think West paradigms have further broadened the reach of our strategic and economic neighbourhood."

Secondly, Sushma Swaraj said, New Delhi is shaping its relationships in a manner that synchronises with India's economic priorities.

"With this 'diplomacy for development' approach, each global interaction is now focussed on building partnerships to promote our transformative flagship programmes such as Make in India, Smart Cities, Digital India, AMRUT and Namami Gange," she stated.

"Third, we are focussed on making India a human resource power to be reckoned with by connecting our talented youth to global opportunities.

"This is being achieved through Skill India partnerships with several countries, as well as under the aegis of the GIAN programme and various private sector partnerships under Digital India."

Fourthly, the External Affairs Minister said, India is building sustainable development partnerships stretching from the Indian Ocean and Pacific Islands to the Caribbean, and from the continent of Africa to the Americas.

"These initiatives have expanded; both in geographical reach and sectoral coverage, and now include Lines of Credit and grants, technical consultancy, educational scholarships and a range of capacity-building programmes," she said.

Finally, Sushma Swaraj said, India is leading the way in reconfiguring and reinvigorating global institutions and organisations.

"Whether it is by founding the International Solar Alliance, which will benefit our energy security and also combat climate change; or our active role in humanitarian and disaster relief operations in our neighbourhood; or our membership of key institutions of global governance - India is a proactive and constructive contributor to promoting and upholding global peace and security," she said.
This year's Raisina Dialogue, which is in its fourth edition, is being attended by over 600 delegates from 92 countries, including influential political leaders, strategic thinkers, policy practitioners, technology innovators, business representatives and academics.

Advanced Nanotechnologies for Detection and Defence against CBRN Agents

Editors: Petkov, P., Tsiulyanu, D., Popov, C., Kulisch, W.
NATO Science for Peace and Security Series B: Physics and Biophysics (2018)
Source: https://www.springer.com/gp/book/9789402412970

This volume gives a broad overview of advanced technologies for detection and defence against chemical, biological, radiological and nuclear (CBRN) agents. It provides chapters addressing the preparation and characterization of different nanoscale materials (metals, oxides, glasses, polymers, carbon-based, etc.) and their applications in fields related to security and safety. In addition, it presents an interdisciplinary approach as the contributors come from different areas of research, such as physics, chemistry, engineering, materials science and biology. A major feature of the book is the combination of longer chapters introducing the basic knowledge on a certain topic, and shorter contributions highlighting specific applications in different security areas.

Marines set up specialist Novichok unit in response to Salisbury attack

Source: https://www.telegraph.co.uk/news/2019/01/10/marines-set-specialist-novichok-unit-response-salisbury-attack/

Jan 10 – The Royal Marines have set up a unit specialising in chemical warfare skills to prepare for a repeat of the Novichok attack on Salisbury.

Zulu Company from 45 Commando, based in Arbroath, Scotland, will be the first marines to respond to a chemical, biological, radiological or nuclear (CBRN) incident at home or abroad.
The commandos were given the training in response to the heightened threat following the nerve agent attack on former Russian spy Sergei Skripal, which left him and his daughter Yulia seriously ill.
Dawn Sturgess, 44, fell ill in nearby Amesbury months after the incident in Salisbury, and died in hospital in July after coming into contact with a perfume bottle believed to have been used in the attack on the Skripals and then discarded.
Her partner, Charlie Rowley, 45, was also exposed to the nerve agent but was treated and discharged.

The marines carried out their training at the Defence Chemical Biological Radiological Nuclear Centre at Westdown Camp on Salisbury Plain in Wiltshire.

This involved a week of classroom learning before a week of practical training in a simulated attack on Imber - a deserted village used for military training.

Sergeant Ben Fail said: "The recent attack on British soil highlighted the importance of this capability and it is more important than ever for us to be able to operate effectively in this environment should the need arise."
The final assault included pyrotechnic and electronic battle simulators to make the experience as real as possible.
Lieutenant Oliver Crow, of Zulu Company, said: "The Royal Marines are high-readiness troops who need to be able to react to all threats at short notice anywhere in the world.
"This is a very important skill for us to maintain in view of the current threat."
The Skripals' home in Salisbury is set to be dismantled as decontamination work continues.

Half a tonne of Captagon seized in Dubai

Source: https://www.thenational.ae/uae/half-a-tonne-of-captagon-seized-in-dubai-1.812405

Jan 12 – Smugglers have been caught attempting to bring 5 million Captagon tablets into the country.
The illegal pills were seized by Dubai Customs, who had received intelligence about the Rilo is a regional intelligence network used by customs authorities to share information and track suspect shipments.

The pills, weighing half a tonne, were concealed in a container of vehicle spare parts that arrived at Jebel Ali Free Zone.
The container was scanned and examined by K9 sniffing dogs, who alerted customs officials to the contraband.
"Up to 5 million Captagon pills, weighing 500kg, were seized," said Ahmed Musaibih, director of Dubai Customs. "This raises the number of Captagon pills seized since January 2018 to 15 million."
Since 2016, more than 225 million pills, and 51 kilograms of other prohibited drugs, have been seized by the Jebel Ali and Tecom Customs Centre in 19 raids.

EDITOR'S COMMENT: Recently, a container with lead rods (24 pallets; 544 rods; 10,000 pills in each rod), sized in the Port of Pireaus, Attica, Greece containing a substrantial number of Captagon

pills as well. And this was not the first time. The container was shipped from Latakia, Syria with final destination Croatia [why?].

How to assess the true cost of simulators for CBRNe training

Source: https://www.argonelectronics.com/blog/assessing-cost-of-simulators-cbrne-training

Jan 21 – There is increasing recognition of the the importance of conducting HazMat and CBRNe training for first responders in the most realistic conditions possible.
But that need for an authentic training environment isn't always best served through the use of actual detector equipment - whether due to health and safety risk, environmental considerations or the increased administrative burden of working with potentially hazardous simulants.
In such situations, the use of intelligent electronic simulator detector equipment can offer significant benefits in terms of CBRNe and HazMat training outcomes.

Arguing the case for simulator detector technology

Given the choice, many instructors will opt for a simulator detector over an actual detector when planning their training scenarios. Arguing the case for the training benefits of simulator detectors isn't a difficult one. They offer safe and realistic hands-on training opportunities in any setting, exercises are easy to set up and replicate, there is vastly reduced administrative effort and freedom from regulatory constraints.
But given that the purchase of simulator detector technology inevitably comes at a higher price than buying an actual detector - how can instructors best argue the case for procurement of such equipment for their training?

A key factor when comparing using real detectors with using simulators is to calculate the actual lifetime cost of ownership of each device, taking into account all the costs (direct and indirect) that may be involved in purchasing and operating that product over its lifetime.

If you are deploying actual detectors in your training scenarios, for example, then it will be necessary to budget for the acquisition, transportation and handling of any simulant chemicals, gases or radioactive sources - all of which are subject to significant regulatory control with associated administrative cost.

Using real detectors will also rely on the purchase and fitting of essential replaceable consumables - such as hydrogen cylinders or sieve packs. If these consumables are incorrectly fitted there is also the risk of damage to the device. Also of course is the teaching time lost due to lack of availability of functional detectors.

Assessing the true cost

Another key consideration in using actual detectors for training is whether you can afford to risk damaging valuable detector equipment in the process. While an electronic personal dosimeter (EPD) might be a less onerous item to replace, when it comes to more sophisticated items of detector technology, some of which could be worth in the tens of thousands of dollars, the unplanned replacement of damaged stock is a major financial consideration.

We also know that training exercises don't always go to plan and that, whether through accident or misuse, trainees don't always get things right. The question is whether you can afford using your actual detectors for the purposes of training if there is a risk of those devices being compromised?

Using actual detectors will, at best mean having to allow for the decontamination and servicing of your detector equipment to ensure operational readiness. At worst, you could be looking at having to completely replace an item that's been damaged beyond repair.

Simulator detectors, while they may be more expensive at the outset, can prove a more cost-effective option once whole of life expenses are taken into account. Simulators require little in the way of consumables (aside from the replacement of batteries), and will need no regular calibration and no preventative maintenance.

And in situations where it is important for students to practice the replacement of consumables, a well-designed simulator is able to replicate that consumable so the student can safely carry out the procedure. Clever use of technology also means that trainees can experience the effects of contamination of their equipment, but without the use of any simulant or substance that could potentially harm the device.

Safeguarding operational readiness

Perhaps most crucially of all, the use of simulator devices for CBRNe and HazMat training exercises safeguards the operational readiness of actual detectors to ensure that all safety-critical equipment is available when it's needed.

When assessing the true cost of your CBRNe or HazMat training systems it can definitely pay to look beyond the initial purchase price in order to evaluate the true total cost of ownership.

The performance and operational readiness of actual detectors should never be compromised in favour of training. And it is here that simulator devices can fulfil a crucial role in ensuring the highest levels of authentic training with no risk to safety-critical detector equipment

The Evolution of the Islamic State's Chemical Weapons Efforts

CTCSentinel October 2017, Volume 10, Issue 9

By Columb Strack

Source: https://ctc.usma.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/

In late July 2015, the Islamic State fired several mortar bombs at Kurdish People's Protection Units (YPG) positions near the city of Hasakah in northeastern Syria. A statement released by the YPG after the attack described how the explosions had released "a yellow gas with a strong smell of onions," and that "the ground immediately around the impact sites was stained with an olive-green liquid that turned to a golden yellow after exposure to sunshine."[1] Soldiers exposed to the substance reportedly suffered from nausea and burning sensations. U.S. officials later confirmed that samples taken from the site of the attack had tested positive for a small amount of mustard agent, in low concentration.[2] This was not the first time the Islamic State or one of its predecessors had used chemicals as a weapon, but never before had a non-state actor developed the capability to combine production of a banned chemical warfare agent with a projectile delivery system.

The attack near Hasakah marked the culmination of nearly two decades of experimentation by Sunni jihadi groups, leading to the establishment of a dedicated chemical weapons (CW) program in the Iraqi city of Mosul, following the declaration of the Islamic State's self-proclaimed 'caliphate' in June 2014. In the last three years, the Islamic State carried out attacks using chemicals on at least 76 occasions, according to IHS Markit's Conflict Monitor open-source dataset. The graphic below (Figure 1) shows the distribution of these recorded events, which were gathered from a range of local news reports and social media.[a]

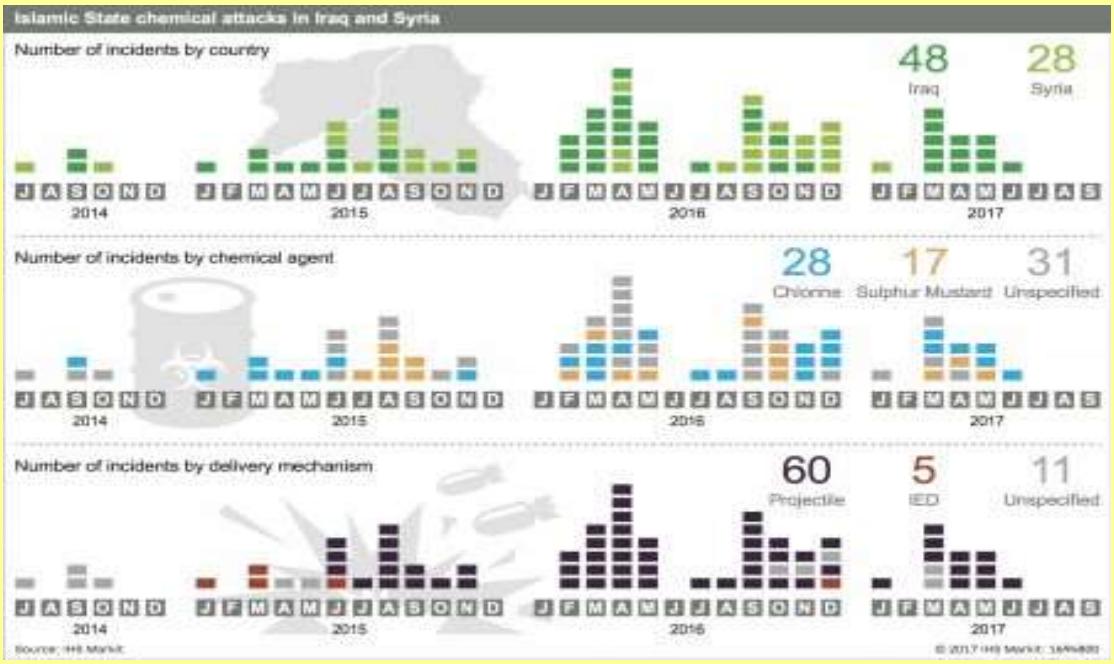


Figure 1: Timeline of Islamic State chemical attacks in Iraq and Syria

The Islamic State's use of chemical agents in Iraq and Syria is characterized by three phases. During the initial phase, which encompasses the first year of the caliphate's existence (between June 2014 and June 2015), chemical attacks drew on tried and tested techniques, adapted to include widely available industrial chemicals—mainly chlorine and phosphine—from stockpiles captured as part of the group's territorial expansion. These attacks were carried out using crude delivery mechanisms, in most cases adding canisters of chemicals to roadside or vehicle-borne improvised explosive devices (IEDs). The second phase, from July 2015 to January 2017,

represents the enhanced capability the group had achieved by combining the production of sulfur mustard agent with the means to deliver it using projectiles, such as mortar bombs and improvised rockets. During this period, chemical attacks were carried out simultaneously across the caliphate, from Syria's Aleppo province in the west to Iraq's Kirkuk province in the east, indicating the existence of multiple operational units with the required expertise. Attacks peaked in April 2016, with eight separate recorded chemical attacks in one month. The third phase began with the last recorded chemical attack in Syria on January 8, 2017, and ended with the Islamic State's apparent abandonment of its CW production following the loss of Mosul in July 2017.

A History of Intent

The Islamic State's CW program builds on nearly two decades of experimentation by other Sunni militant groups based out of Iraq. The Jordanian jihadi Abu Mus'ab al-Zarqawi showed an interest in developing CW as early as 1999. He initially established a jihadi training camp in Herat, Afghanistan, where his followers experimented with the production of toxins,[3] but later moved this to Khurmul in northeastern Iraq after the U.S. invasion of Afghanistan in 2001. The Khurmul facility was captured by U.S. coalition forces in 2003, which reportedly found equipment and manuals for the production of CW, as well as traces of ricin and other poisons.[4] In 2004, another laboratory linked to al-Zarqawi's network was discovered in Fallujah, Anbar province, suggesting that the group had developed a rudimentary capability to build chemical IEDs.[5] Other Sunni militant groups were experimenting with the use of CW at the same time. These include the al-Abud network, which also operated in the Fallujah area, and another unspecified group operating a laboratory discovered in Mosul, which contained more than 6,000 liters of chemicals.[6] The most elaborate attempt to use chemicals in an attack during that period came in April 2004, when the Jordanian government announced it had thwarted a plot by al-Zarqawi's network against the headquarters of the General Intelligence Directorate (GID) in Amman. The plot involved the intended use of three large trucks as vehicle-borne improvised explosive devices (VBIEDs) and up to 20 tons of mixed industrial chemicals. The mix of these chemicals was designed to enhance the explosive power of the IEDs and create a toxic cloud that would spread around the city, aimed at causing mass civilian casualties.[7] Before his death in a U.S. airstrike in 2006, al-Zarqawi pledged allegiance to Usama bin Ladin, forming al-Qa`ida in Iraq (AQI), which later became the Islamic State of Iraq (ISI) and eventually formed the core of the Islamic State.

Al-Zarqawi's network continued with the development of chemical IEDs and was widely assumed to be behind a series of chlorine VBIED attacks in Anbar province, beginning in October 2006.[8] However, these had limited effect, as the containers designed for the safe transport and storage of chlorine were sub-optimal for its explosive dissemination by IED. The relatively low toxicity of the chemical was further decreased by the heat and blast pressure.[9] In practice, the addition of chlorine did not increase the lethality of the IEDs beyond that of the conventional explosives. The psychological and political impact, however, attracted the attention of U.S. coalition forces, to track down and eliminate any individuals believed to be involved.[10] The chlorine attacks stopped in 2007 after the arrest of a 'key leader,' believed to be Umar Wahdallah Dod al-Zangana,[11] and no further reports of Sunni jihadis using chemicals emerged until June 2013, when Iraqi forces disrupted an ISI cell of five men who had set up three makeshift laboratories with the reported intent of manufacturing chemical agents and releasing them with remote-controlled helicopters.[12]

Expertise and Sourcing

Although the intent to develop a CW capability had existed for some time, it was the security of unchallenged territorial control, access to laboratory equipment in Mosul, and the relatively unrestricted availability of precursor chemicals—afforded by the establishment of the caliphate— which gave the Islamic State the opportunity to do so. Publicly available information on individuals killed or detained by the U.S. coalition in connection with CW suggests that the Islamic State assembled at least one dedicated team of technical experts to develop its CW program, using improvised laboratories hidden in Mosul's residential neighborhoods to avoid U.S. coalition airstrikes.[13] Available reporting suggests the group drew upon a combination of

foreigners from Chechnya and Southeast Asia with relevant technical expertise who had migrated to the caliphate[14] and those who had previously been involved in CW research for AQI and other Iraqi jihadi groups prior to the establishment of the Islamic State.[15]

Several Islamic State members killed or detained by U.S. forces for their involvement with CW in the last few years were reported to have been employed in Saddam Hussein's CW program in the 1980s. One such individual, Abu Malik, who was killed in a coalition airstrike on January 24, 2015, was a chemical weapons engineer who worked at the Muthanna CW production facility before joining AQI in 2005.[16] However, the level of expertise these individuals provided, and the importance of that expertise to the success of the Islamic State's program, is sometimes overstated. None of the individuals reportedly killed or captured by the coalition were confirmed to have been senior members of Saddam's program. The relatively low level of expertise demonstrated by the Islamic State suggests that those individuals recruited by the group, if they were in fact employed under Saddam, would likely have been lower-ranking members of the program.[17] It is telling that no evidence has come to light publicly that the Islamic State has succeeded in producing more lethal chemical warfare agents, such as sarin or other nerve agents. The types of chemical agents used by the Islamic State, including low-grade mustard agent, do not require a high level of technical expertise to produce, and the knowledge is widely available.

There has been speculation over whether the Islamic State could have sourced CW from existing stockpiles belonging to the Iraqi or Syrian governments, both of which ran extensive CW programs in the past. The large number of CW munitions stockpiled in Iraq under Saddam Hussein and poor government documentation mean that many of these remained unaccounted for after the United Nations Special Commission's (UNSCOM) process of reconciling the number of agents and weapons manufactured with what was consumed and remained. Even a one-percent margin of error would have resulted in thousands of abandoned or forgotten munitions.[18] In fact, the CIA-led 'Operation Avarice' reportedly purchased 400 CW munitions between 2005 and 2006 that had found their way onto the black market.[19] In Syria, interviews with army defectors suggest that some refused orders to deploy CW against civilians and buried their weapons stocks. For example, defected General Zahir al-Sakit claimed in an interview with Al Arabiya in 2013 that he had been ordered to use CW against the Syrian opposition near Houran in southwestern Syria, but he instead "ordered all chemical weapons to be buried."[20]

During its period of rapid territorial gains in 2014, the Islamic State seized control of military sites where chemical munitions could have been hidden, abandoned, or lost. When the Islamic State took control of Saddam Hussein's largest CW production and storage facility at Muthanna in July 2014, the U.S. Department of State acknowledged that a limited amount of CW precursors remained there.[21] UNSCOM inspectors dismantled all CW production facilities and removed all equipment from Muthanna in the 1990s, with the exception of two bunkers, which were sealed by UNSCOM in 1994. Bunker 13 contained 2,500 sarin-filled 122mm artillery rockets, which were partially damaged or destroyed in a U.S. airstrike on the first night of the 1991 Gulf War. Leaking munitions, unstable propellant, and explosive charges made it too hazardous for U.N. inspectors to enter. Nearby, Bunker 41 was used to bury contaminated materials left over from the UNSCOM destruction program.[22] When Iraqi forces regained control of the facility in late 2014, Iraq's Deputy Foreign Minister Mohammad Jawad Al-Doraky stated that neither of the sealed bunkers had been penetrated by the Islamic State.[23]

The Organisation for the Prohibition of Chemical Weapons (OPCW) removed the last of Syria's declared CW precursors and agents from the country in June 2014. But the lack of any overt process to verify the Syrian declaration led to speculation that Syria may have retained CW capability in some form, particularly compared with pre-declaration intelligence estimates.[24] In May 2015, the Syrian local news channel All4Syria quoted a defecting army colonel, identified as 'Ziad,' who claimed that the government retained CW stocks at Sayqal Air Base, around 80 kilometers northeast of Damascus.[25] When the same air base came under attack by the Islamic State in April 2016, government forces reportedly used sarin against them to avoid being overrun, according to a senior Israeli official quoted by *The Telegraph* newspaper.[26]

Although the Syrian government almost certainly retains stockpiles of CW,[27] there is no evidence in the pattern of the Islamic State's recorded use of chemical agents to suggest that the group acquired anything beyond rudimentary precursor chemicals. The precursors

required for the production of chemical agents that have been used as weapons by the Islamic State, primarily chlorine and sulfur mustard, were, however, also available at industrial plants located in the territory of the caliphate. These include, for example, the Misraq chemical plant and sulfur mine, around 30 miles south of Mosul, which is believed to have held thousands of tons of sulfur and hydrogen sulfide,[28] as well as numerous water treatment and fertilizer production plants, which tend to store large quantities of chlorine.[29]

Degradation of Capability

There were no recorded chemical attacks by the Islamic State in Iraq or Syria between June 2017, when it lost control of Mosul, and the time of writing in October 2017. Although there have previously been periods in which no chemical attacks were recorded for several weeks, a three-month break is unprecedented and is especially notable given that the group faced an existential threat to its core territory, including the city of Raqqa, during that time. The last chemical attack (at the time of writing) carried out by the Islamic State in Syria was on January 8 at Talla al-Maqri in Aleppo province. This compares with 13 such attacks in Syria over the previous six months, which were concentrated in the same area of Aleppo province. All other recorded attacks in 2017 were in Iraq, with 11 in Mosul and one near al-Atheem in Diyala province. The concentration of chemical attacks in Mosul after it had become cut-off from the rest of the caliphate in late 2016 suggests that the blockade on Mosul by Iraqi forces prevented the transfer of those weapons to Syria and that no further production sites were established elsewhere to compensate.

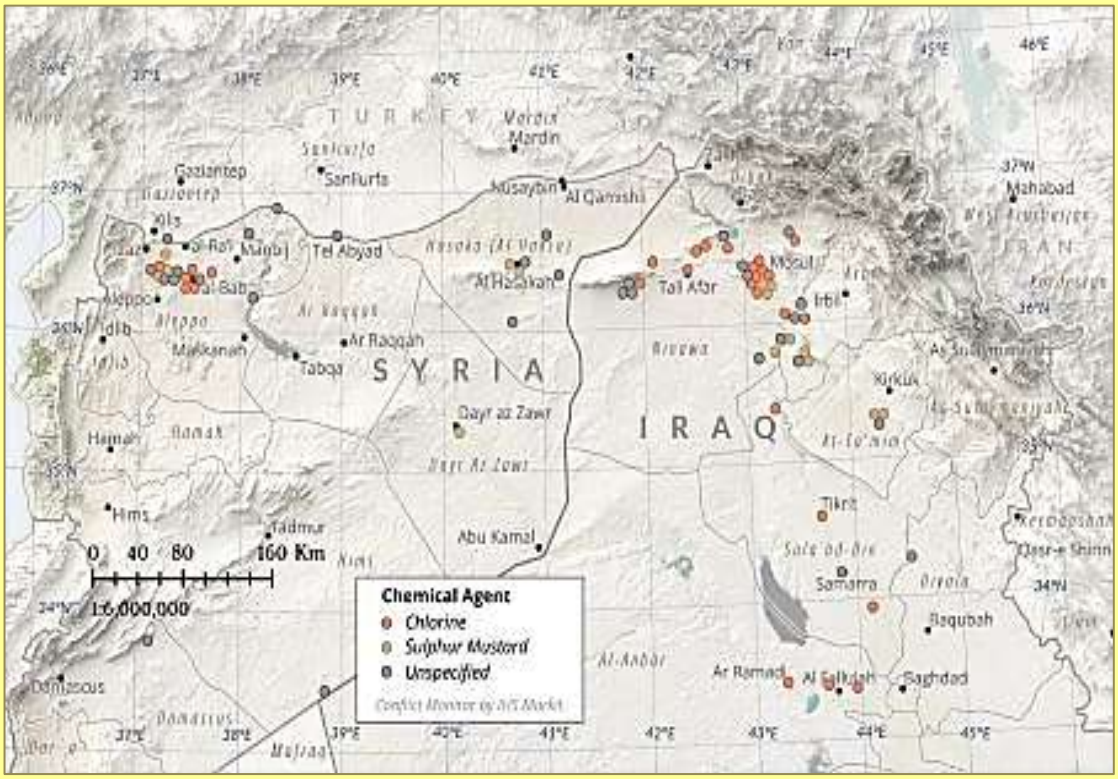
The Islamic State's CW capability had already been significantly degraded before the loss of Mosul, as a result of U.S. coalition airstrikes against individuals and facilities associated with the program. A major breakthrough for the U.S. coalition came in February 2016, when U.S. Special Operations forces captured Suleiman Daoud al-Bakkar (aka Suleiman Daoud al-Afari) in Badoosh, a village north of Mosul. He was a leading figure in the group's CW program and a reported former expert in chemical and biological weapons under Saddam. Al-Bakkar was interrogated for about a month and gave the United States unprecedented insight into the nature of the Islamic State's program, including the names of key individuals and locations at which chemical agents were being produced and stored. The information led directly to a number of airstrikes against the program.[30]

The U.S. coalition's success in disrupting the Islamic State's CW program meant that the effort required to conceal and keep it running increased significantly in relation to the impact the weapons were having. In addition, the utility of CW on the battlefield is likely to have been displaced to some extent by the development of other weapons systems that achieved a similar psychological effect. In early 2017, the Islamic State began systematically using unmanned aerial vehicles (UAVs), primarily from the Phantom series of quadcopters produced by the private company DJI, to drop IEDs on enemy troop concentrations up to several kilometers behind the front line. In much the same way that the Islamic State used the release of chemical agents in Mosul to halt enemy advances by forcing them to take countermeasures, the presence of potentially armed UAVs had a similar impact. Due to the absence of reliable UAV countermeasures, Iraqi forces in most cases would be forced to take cover and engage the UAV with small arms fire.[31] For the Islamic State's UAV attacks, as for its chemical attacks, the psychological and harassing effect was far greater than the actual lethality of the weapons system, which did not exceed that of conventional indirect fire weapons. UAVs are cheaper and easier to use than chemical projectiles for that purpose, as the latter require specialist operators and equipment, which were in limited supply, and presented high value targets for U.S. coalition airstrikes.

Although the Islamic State appears to have abandoned the use of CW on the battlefield, it has most likely retained the aspiration, and at least the expertise, if not the equipment and precursor materials, to produce small batches of chlorine and low-grade sulfur mustard agent. Experts involved in the Islamic State's CW program are likely to have been evacuated from Mosul to Syria alongside other senior members of the organization before it became isolated in late 2016. According to a U.S. official quoted by CNN in May 2017, the Islamic State was assembling a new chemical weapons cell in the Euphrates River Valley, somewhere between Mayadin and al-Qaim on the Syria-Iraq border.[32] Although U.S. intelligence at the time assessed that the cell was

seeking to consolidate its CW capabilities to support the defense of its remaining strongholds, that had not yet materialized at the time of writing.

As the remaining core of the Islamic State's caliphate in the Euphrates River Valley comes under increased military pressure in late 2017, the group will be looking to transfer key figures, particularly individuals with high-value expertise—including in IED-making and the manufacture and use of CW—out of Iraq and Syria to other safe havens, most likely in Libya and the wider Sahel. This is likely to be enabled by the extensive people-smuggling networks that operate out of Kurdish-held territory in Iraq and the rebel-held Idlib pocket in Syria, bordering Turkey's Hatay province.[33]



Recorded allegations of Islamic State chemical weapon use by location and chemical agent between July 2014 and mid-October 2017. Each circle represents a single alleged incident. (Rowan Technology)

Threat to the West

There have been several Islamic State plots to carry out chemical terrorist attacks elsewhere, drawing on the expertise developed in Iraq and Syria. Australian authorities in Sydney disrupted a plot in July 2017 by two brothers, Khalid and Tarik Khayat, to deploy a device designed to release hydrogen sulfide, a toxic gas used briefly by the British Army, with limited effectiveness, as a chemical weapon in WW1.[34] According to the Australian police, instructions on how to construct the device came from an Islamic State 'controller' in Syria. Military-grade explosives had been shipped to the pair with air freight via Turkey for a separate aborted plot to bomb a passenger jet. The brothers had also acquired in Australia some of the precursor chemicals for the poison gas plot, although they were reportedly "a mile and a half away" from constructing a viable chemical dispersal device.[35] The plot illustrates how the Islamic State has the capability not only to transfer the know-how to produce toxic chemicals via secure online communications to operatives already living in target countries, but also to ship materials, including explosives, undetected. Germany's Federal Criminal Police Office (BKA) published a report in January 2017 highlighting the risk of chemical contamination of the water supply or food in grocery stores in Europe.[36] The Islamic State has published English-language guides on its Wilayat Furat Telegram channel, such as the 'Knights of the Lone Jihad' series, which details how to do so by injecting groceries with cyanide poison or widely available pesticides, such as strychnine.[37] However,

most self-radicalized individuals carrying out attacks in the West have so far selected methods that are likely to result in their own death, or martyrdom, at the hands of the security forces. This partly explains the use of fake suicide belts and the combination of knife attacks with vehicle-impact attacks. The 'anonymous' poisoning of food and water supplies is likely to be a less attractive option for such individuals.

There is no publicly available evidence to suggest that the Islamic State has transferred sulfur mustard agent or other chemical weapons developed in Iraq and Syria to Europe. Although the Sydney plot demonstrates that the group has been able to ship explosives to a Western country undetected, it is far less likely that ready-made chemical weapons, such as sulfur mustard agent, could be shipped this way. The highly corrosive nature of such agents, and the highly controlled environments they must be stored in, mean that they are very difficult to transport over long distances without leaking.[38] For that reason, the Islamic State would probably need to develop the agents shortly before they intend to deploy them, most likely in the target country.[39]

If the Islamic State were to organize a chemical attack in a Western city, the logistical challenges of transporting CW manufactured in Iraq and Syria and the generally low level of expertise the group has demonstrated suggest that an attack using widely available toxins or industrial chemicals would be far more likely than the use of blister or nerve agents like sulfur mustard or sarin. This significantly limits the potential lethality of such an attack.

Substantive Notes

[a] Given the nature of the source material, many of the reported incidents have not been independently verified.

▶▶ Citations (available at source's URL).

Columb Strack *is a senior Middle East analyst with Jane's by IHS Markit. He leads the company's Conflict Monitor service, which provides data-driven insights and analysis into jihadi factions operating in Iraq and Syria.*

Islamic State Chemical Weapons: A Case Contained by its Context?

CTCSentinel, March 2018, Volume 11, Issue 3

By Markus K. Binder, Jillian M. Quigley and Herbert F. Tinsley

Source: https://ctc.usma.edu/islamic-state-chemical-weapons-case-contained-context/

During the Islamic State's brief control of territory in Iraq and Syria, its forces repeatedly employed chemicals in both offensive and defensive operations.[a] In the absence of access to appropriate sources, whether human or documents, it is difficult to draw firm conclusions about the Islamic State's desire to acquire and use chemical weapons. Furthermore, the question remains as to why the Islamic State did not extend this capability into its far-reaching foreign terrorism campaign. Indeed, there is open source evidence of only one instance in which the Islamic State directed the transfer of chemical warfare (CW) related skills to its *al-Amn al-Khariji* (External Operations) operatives or their remote associates.[b] Moreover, Islamic State CW activities in theater were possibly relegated to a "special operations" unit—known as "*Jaysh al-Khalifa*" or "*Jaysh Dabiq*"—which may have been responsible for all CW deployments in Syria and Iraq.[1c] Considering these notions, available evidence reveals no trends concerning the Islamic State's present and future chemical terrorism ambitions. The more critical question becomes: can the Islamic

State's CW experimentation reveal anything about future chemical terrorism threats? This article will argue it cannot.

The Islamic State's Use of Chemical Weapons

The Islamic State has demonstrated a willingness to use any means to maximize the harm and disruption it inflicts upon its enemies. Starting in 2014, these means came to include chemical weapons, which were utilized in possibly 37 discrete attacks in Syria and Iraq,[d] causing a handful of confirmed deaths and a limited number of injuries.[e]

In the course of its operations, the Islamic State has utilized two basic classes of agents: weaponized toxic industrial chemicals (TICs) and warfare agents. The use of weaponized TICs, dominated by the use of chlorine, illustrated the Islamic State's willingness, and capacity, to effectively adapt resources that came into its hands. It also clearly demonstrated that the group had no compunctions about adopting CW. Chlorine was deployed frequently between August 2014 and June 2015 but slowed to a trickle thereafter. In total, there were at least 20 strongly supported instances of the use of chlorine by the Islamic State.[f] In addition, there are indications that Islamic State forces may have used chlorine grenades and other small-scale delivery methods extensively in the course of their defense of Mosul and other sites in north-central Iraq, although these attacks have not been recorded in detail.[2] A noteworthy feature of these deployments is that they all occurred in Iraq.

In addition to chlorine, the Islamic State appears to have employed other TICs on an experimental or opportunistic basis. Phosphine, an organophosphorus compound commonly used as an agricultural fumigant, was allegedly used in a series of attacks in the vicinity of Hasakah, Syria, on June 28, 2015.[3] Islamic State forces reportedly used vinyltrichlorosilane, a compound used in the production of plastic and rubber products,[g] in at least one attack,[4] although this agent's use is not strongly supported, with only two sources of doubtful reliability mentioning it.[5]

In a grave development, the Islamic State also made use of the CW agent sulphur mustard. The initial deployments of mustard agent occurred in August and September 2015. A second set of attacks took place in February and March 2016.[h] Significantly, it appears that this agent was actually produced by the group, which would make it only the second violent non-state actor (VNSA) to have produced warfare agents in any useful quantity.[i] Although there was a suspicion that the Islamic State had simply deployed agent taken from Saddam-era stockpiles, analysis of samples gathered at the site of the August 21, 2015, attack in Marea, Syria, clearly refuted this. The analysis revealed that the agent employed had been produced using the Levinstein method[6] rather than the Meyer-Clarke method used in the Saddam-era program,[7] strongly supporting the contention that the agent was self-produced.

The Islamic State's CW activities have been almost entirely confined to battlefields and their immediate environs, using a variety of artillery and mortar systems for agent delivery. Otherwise, the Islamic State's CW use seemed designed to slow enemy advances through the extensive use of roadside bombs. The Islamic State's CW approach is markedly different to that adopted by its precursor organization, al-Qa`ida in Iraq (AQI). AQI carried out an explicit chemical terrorism campaign between October 2006 and June 2007.[8] All told, AQI conducted approximately 20 attacks using vehicle-borne improvised explosive devices (VBIEDs) charged with varying quantities of chlorine gas.[9] These attacks struck residences, marketplaces, and other public gathering areas, and in one attack, U.S. military personnel, northeast of Baghdad.[10] AQI demonstrated a capacity to refine its methods with early attacks "poorly executed, burning the [chlorine] rather than dispersing it"[11] whereas in March 2007, AQI coordinated two to three massive chemical attacks in Fallujah and Ramadi, exposing as many as 300 civilians in a single incident.[12] Not long after this successful operation, the campaign ceased.[j] In contrast to AQI's progression, there was no apparent evolution in the generally unsophisticated delivery systems employed by the Islamic State.

As for the broader reaches of the putative caliphate, there are apparently no open source reports of a single chemical IED among the scores of devices the Islamic State has used in other theaters or terrorist operations.[k] It is true that jihadis do not differentiate between "terrorist" and "tactical" applications, preferring to see all such operations as "military" in nature. This all-inclusive approach raises questions about why the Islamic State has largely refrained from employing CW abroad in pursuit of the strategic goals it associates with terrorism.

Propagandizing or Not

One rich vein of data on Islamic State activities comes from its own propaganda—less so the famously slick Dabiq and Rumiyah, more so the battlefield chronicler, al-Naba.[13] The toll of the Islamic State's far-flung operations, as well as its Syria and Iraq actions, can be read in the weekly's pages. As part of an effort to assess potential chemical terrorism pathways last year, the authors surveyed over 80 issues of the above titles.[l] The absence of any mention of chemical agents or allusions to chemical capabilities in any of the issues published within a week or less of some 16 chemical incidents is quite surprising.[m]

The Islamic State's use of chemical weapons on the battlefield overlapped mere tactical objectives. For example, at Taza Khurmatu, Iraq, in March 2016, chlorine and mustard agent were mixed in with artillery barrages targeting areas just beyond the battlefield proper, exposing civilians and combatants in rear areas and along likely supply routes.[n] The Islamic State's understanding of CW's potential use to generate panic amongst local enemies connects to the fact that the organization considers psychological warfare, terrorism, and tactical combat as part and parcel of the same operational doctrines. The Islamic State's choice to employ CW agents, as it did, suggests that a link between the group's operational calculus and its strategic objectives may have had some initial traction in its leaders' minds.

It is difficult to perfectly substantiate the Islamic State's knowledge of Iraqis' fear of chemical weapons, but circumstantial evidence is abundant. A British CW expert who has had extensive contact with Iraqi, Syrian, and Turkish medical and military professionals reports that many of these individuals profess to a dread of "gas" and basic misunderstandings of the nature of various CW agents for preparedness and defense purposes.[14] In Iraq, this dread is predicated on the Saddam-era use of chemical weapons for internal suppression. On a number of occasions, Iraqi political figures have dismissed or denied the very existence of Islamic State CW capabilities, likely in the hope of allaying civilian fears.[15] For example, Hakim al-Zamili, chairman of the Iraqi parliament's security and defense committee, alleged in 2016 that the notion was an American fiction and that claims that the Islamic State's CW specialist, Suleiman Dawoud al-Afari, had been captured were baseless.[16] Islamic State propagandists are likely to have been aware of these official statements and their motivation.

Since Aum Shinrikyo's spectacular mid-1990s attacks, the West has manifested a growing and somewhat sensational fear of chemical terrorism—as potentially threatened by the Islamic State itself against Europe, if not the United States—reflected in both official analyses and news reports.[17] Whether one believes that the media drives public perceptions or that media aligns to the public's thought life, Islamic State propagandists may have easily read this trend themselves. John Cantlie, a British journalist forced into Islamic State propaganda services after late 2012, either chose to exploit or was ordered to stoke Western fears of nuclear terrorism in Dabiq #9.[18] In that issue, the feature article implies that the Islamic State was well aware of European and American psychological vulnerabilities related to CBRN.[19]

Certainly, the linkages between Islamic State propagandists and the organization's leadership are imperfectly understood. But considering that the group's propaganda was most likely intended to hype "statehood" through the boasting of state-level technical prowess, and, more critically, to draw followers into its fold or convoke them to homespun violence, Islamic State propagandists saw fit to talk up even the most ambiguously successful operations. Why then omit such an obvious accomplishment as the CW program? Could the effort have been too important or too unsatisfying to propagandize? Did Islamic State insiders quickly begin to consider the program ineffective or non-strategic by nature? Might they have feared moral outrage from their supporters or cadres? Again, the exact answers are unclear but to believe that the Islamic State neglected this opportunity without good motive is very difficult.

Implications

The clarion contrast between the Islamic State's lack of propaganda output on CW and its regular media celebration of even the smallest tactical activities, and the determination to demonstrate technological achievements as seen with the adoption and publication of advances in the employment of drones as weapons, suggests Islamic State leadership did not unambiguously support the CW effort. There are several reasons why this might be the case, including the possibility that the effort was a low priority, pet project of a limited number of actors within the organization.

The Islamic State's leadership, and the organization more generally, is likely to have learned a number of lessons from the CW effort. First, the organization (and at least some of its members) is likely to have an enhanced understanding of the difficulties of producing, weaponizing, handling, and effectively deploying CW agents. Secondly, the organization may, based on results from field deployments, have concluded that CW agents are ineffective tools for generating significant numbers of casualties, which may affect any consideration of future use of these agents in terrorist operations.[o] To date, there is only one indication that the skills and training required to weaponize chemicals (or produce CW agents) have been transferred out of the Syria-Iraq theater.[p] While it is possible that some survivors of the units involved with the production and use of chemical agents have escaped from the territory of the former caliphate, only the Sydney hydrogen sulfide plot offers any suggestions about what Islamic State chemical terrorism may actually entail.

Certainly, the New South Wales Police discovery of hydrogen sulfide precursors in the possession of aspiring Islamic State allies could seem to indicate a strategic evolution toward chemical attacks. But this single data point may speak more to the tactical improvisation of the Islamic State handler who directed the plot from afar.[q] When the Khayat brothers failed to get an IED onboard a passenger flight in July 2017, the handler probably instructed them to quickly set up a fake powder coating company and begin experiments in TIC weaponization and dispersal.[r] Hydrogen sulfide is among the less difficult substances to produce outside of an industrial setting, but poses impressive risks to the layman and furthermore to successful lethal deployments.[20] Switching from an IED to this particular chemical may have been driven more by a newly chosen target or by the prerogative of the handler.[s] More confounding to a connection between Islamic State strategy and the Sydney plot is the status of the remote controller. If an *al-Amn al-Khariji* coordinator, as is plausible, then his personal initiative to option a TIC would not necessarily have needed a superior's review or approval, though this does not eliminate leadership involvement.[t] New details may change this assessment, but the Sydney chemical plot seems best understood as a context-specific innovation instead of an organizational trend.[u]

Be that as it may, the Islamic State's use of CW is primarily of interest for its illustration of the potential for quasi-state organizations with territorial control to employ military capabilities typically associated with state military forces. In the case of the Islamic State, the adoption of chemical weapons is clearly unusual when compared to other insurgencies with territorial pretensions or active control throughout the MENA region and throughout history more generally. It is likely, though difficult to prove, that the Islamic State's employment of chemical weapons was very much a product of the circumstances of the group's rise. This surely helps to explain both the Islamic State's interest in developing CW capabilities as well as perhaps why those capabilities have not been applied outside Iraq and Syria. Iraq, after all, has a long history of production and use of chemical weapons, which is likely to have ensured the availability of the necessary technical personnel, awareness of the associated technologies, and its probable utility in theater. In addition, the extensive use of chemical weapons by the Syrian government since late 2012 is likely to have been a further factor in attracting attention to chemical weapons and commercially available TICs.[v]

While the Islamic State has demonstrated on multiple occasions an essentially unrestrained willingness to engage in attacks on civilian populations, its CW activities show a tight association with battlefield tactics. As such, although the Islamic State's CW activities undoubtedly represent an interesting data point, not least in terms of the scientific and engineering capacity of insurgencies, and its ability to address the challenges of production and weaponization of CW agents, that data point does not tell us much of anything useful about how the Islamic State or a successor organization might seek to employ chemical weapons against remote Western targets. It may, however, be relevant for those planning future operations against insurgencies with territorial control in so far as it suggests the need to consider that insurgents may employ chemical weapons against Western forces or their local proxies.

This does not diminish the fact that terrorist organizations or their operatives may come to fetishize chemical and other warfare agents because of the fear they can induce, much as Aum Shinrikyo did. However, given the Islamic State's limited chemical warfare activities, the concern generated by these deeds does not yet justify seeing the Islamic State as an inevitable chemical terrorism danger. And though Western security agencies are correct to monitor this threat vector, publicized warnings remain alarmist for the time being.

Substantive Notes

[a] This article's findings are based on research conducted by the authors as part of a predictive analysis of potential Islamic State chemical terrorism pathways against the United States and its allies and interests. The work was funded by the Department of Homeland Security and the report furnished to the funding office. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security or START. All information contained in this article is solely derived from open sources and represents the authors' integrative opinions on what the research offered which is of pertinence to the broader question here posed.

[b] That exception is the July 2017 plot allegedly involving Australian brothers Khaled and Mahmoud Khayat. An individual identified by the Australian Federal Police as a senior Islamic State figure in Syria instructed the Khayats in constructing a device that could disperse hydrogen sulfide, a toxic industrial chemical. See "AFP (Australian Federal Police) and NSWP (New South Wales Police) discuss the two Sydney men charged over terrorist acts," AFP on *Periscope*, August 3, 2017. *The Sydney Morning Herald* alleges a public transit target for the chemical device. See Rachel Olding, "Khaled Merhi pleads not guilty to weapons charge after Sydney 'bomb plot' raid," *Sydney Morning Herald*, August 24, 2017. This development followed a failed attempt to down an Emirati airliner using an improvised explosive device. While some aspects of this plot are still unclear, the authors discuss the pertinent implications toward the end of this article.

[c] This certainly does not rule out other Islamic State assets with chemical weapons expertise or experience. Most importantly, there does appear to have been a group responsible for CW testing and development, which U.S. military efforts seem to have degraded by the summer of 2016.

[d] This figure, and all other data unless otherwise cited, is from the authors' open source research and is included in the report referenced in footnote a. The exact number of attacks is difficult to pin down. Many have likely gone unreported, whether in local news reports or in the international media. The authors compiled incident data from three different sources in order to focus their research efforts. However, of those that were indicated, some have been disproven, some reports retracted, and still others were documented on the basis of dubious open source evidence. The authors have come to the conclusion that the majority of available data on Islamic State chemical weapons incidents is non-authoritative, particularly in the cases of chlorine and other weaponized industrial chemicals. Generally speaking, reports on mustard agent attacks are better supported due to the potential to test for specific breakdown products in biological or soil samples. The authors chose to focus on sulfur mustard-related attacks in their report to the Department of Homeland Security partly because of the technical prowess its production suggests.

[e] Figures on deaths and casualties are incomplete and often inconsistent, particularly where chlorine or commercial toxic chemicals were employed. The following casualty figures for mustard agent are, however, reasonably well supported: one minor was killed following mustard agent exposure at Marea, Syria, in August 2015. See "S/2016/738: Third report of the Organization for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism," United Nations Security Council, August 24, 2016. Thirty-five injuries were reported after a mustard attack on a Kurdish Peshmerga position near Makhmour, Iraq, in August 2015. See "Blood tests reveal traces of mustard gas used by IS in attacks on Peshmerga forces," ARA News, October 9, 2015, and Barbara Starr, Jim Sciutto, and Elise Labott, "U.S. investigating 'credible' reports that IS used chemical weapons," CNN, August 14, 2015. At least three Peshmerga soldiers were injured in a second Makhmour attack in February 2016. See "Peshmerga endure fresh ISIS chemical attack," Rudaw, February 17, 2016, and Matthew Vickery, "Eyewitness account: ISIL steps up chemical weapons attacks on Kurds in Iraq," *USA Today*, March 10, 2016. A Peshmerga officer was seriously wounded in early March 2016. See Peshmerga News, "Major Jamal, brave #Peshmerga who defused many ISIS IEDs, is hospitalized after ISIS used Mustard agent near Zummar," Twitter, March 4, 2016. This comprises a total of one confirmed death and 39 probable injuries. Other reports were not evaluated for their credibility due to imprecise or inconsistent numbers.

[f] This figure is based on open source research by the authors and is included in the report referred in footnote a.
[g] Also identified as trichlorovinylsilane. See "Trichlorovinylsilane," National Center for Biotechnology Information, PubChem Compound Database.
[h] Testing of samples from a suspected mustard attack against U.S. forces in September 2016 initially suggested mustard agent was used, but subsequent testing produced inconclusive results. Ryan Browne, "US: ISIS did not use mustard agent in base attack," CNN, September 27, 2016.
[i] The other example is Aum Shinrikyo, which mastered the production of sarin and VX nerve agents.
[j] As to why this campaign ended, plausible explanations include the possibility that AQI had been starved of chlorine supplies. The Iraqi government appears to have suspended chlorine shipments, which may partly be substantiated by high incidences of cholera due to a lack of chlorine for civilian water treatment. See James Glanz and Denise Grady, "Cholera Epidemic Infects 7,000 People in Iraq," *New York Times*, September 12, 2007. Otherwise, AQI's operational latitude may have changed considerably due to the Anbar "Awakening" and the U.S. troop surge.
[k] This is to exclude the plans for a chemical dispersal device as developed by the Sydney plotters and their handler. Otherwise, UWT researchers surveyed 77 international terrorism incidents associated with the Islamic State, all of which occurred between May 2014 and January 2017. The primary purpose of the survey was to derive Islamic State TTPs in sophisticated, high-casualty, and other types of attacks. Another incident that could turn out to have links to Islamic State CW is a chlorine charged IED discovered by Indonesia authorities in a Jakarta mall in February 2015. While the chlorine itself did not disperse and was "crafted inside a cardboard box," Indonesian police claimed that the culprits were Islamic State foreign fighter returnees. No additional information was supplied by which to analyze this claim. As compared to the Sydney case, as described below, this incident is far more difficult to square as an organizationally driven plot. Kate Lamb, "Indonesian police blame jihadis returning from Syria for chlorine bomb," *Guardian*, March 25, 2015.
[l] Researchers reviewed issues #5 through #77 of al-Naba, corresponding to the time period November 15, 2015, through April 20, 2017. This time period covers 14 of the 37 Islamic State-related chemical weapons events considered for the UWT report (eight sulfur mustard related events and six events related to other weaponized chemicals.) Researchers also reviewed all available time-period relevant English issues of Dabiq and Rumiyah, especially in order to account for CW incidents occurring prior to November 2015. Though al-Naba is more exhaustive in its coverage than Dabiq and Rumiyah, it is, in fact, more interesting, in the context of this argument, that these magazines do not mention chemical weapons or chemical releases. After all, the latter two titles were Islamic State's flagship efforts for Western audiences.
[m] Certainly a more exhaustive search could yield different results. However, in order to keep within the time allotted for the research mentioned, the authors had to restrain their search.
[n] In this case, the target was a Shi`a Turkmen-majority town significantly to the east and south of what was then considered the Makhmour front, approximately 150 kilometers southeast of Mosul. This area was plausibly within the AOR of the Iraqi Army's Nineveh Operations command, if not along that command's supply corridor. (There was no evidence, however, that the units under this command had stationed any of their elements in or near the town of Taza Khurmatu.) BBC News reported that 24 "shells and rockets" fell on Taza Khurmatu on March 8. VICE News claimed "more than 40 rockets," alleging that all of these carried chemical warheads. A Shi`a Popular Mobilization spokesman told Al-Sumaria news that two more "Katyusha" rockets had struck on the evening of March 11. See Nafiseh Kohnavard, "Iraqi town Taza 'hit in IS chemical attack' appeals for help," BBC News, March 25, 2016, Campbell MacDiarmid, "Inside Taza, the Iraqi Town Gassed by the Islamic State," VICE News, March 9, 2016, and "Taza Subjected to New Attack by Ordnance Carrying Toxic Gas," Al-Sumaria, March 11, 2016.
[o] This observation is not intended as an explanation for the 2017 cessation of Islamic State CW use in theater, which was likely driven by other factors, including loss of personnel, infrastructure, and territory.
[p] The exception may be the Sydney hydrogen sulfide plot. Nevertheless, the Sydney suspects did not attempt to produce chemical warfare agents, but to weaponize

commercially available toxic chemicals. The distinction is very important in terms of the threat posed and the technical sophistication involved.

[q] Australian Federal Police Deputy Commissioner Michael Phelan announced that the suspects were in conversation with a senior Islamic State figure from April 2017. See "AFP and NSWP discuss the two Sydney men charged over terrorist acts." The conversations were allegedly facilitated by the suspects' brother, who had traveled to Syria as a foreign figher more than a year before. Phelan characterized these interactions as the provision of inspiration and instruction on how to plan, resource, and then execute a civilian aviation plot. The Islamic State figure was not identified, but this plot is similar to the "virtual planner" model described by Daveed Gartenstein-Ross and others, possibly suggesting an *al-Amn al-Khariji* operative like Rashid Qassim or Abdselam Abbaoud. See Rachel Olding, "Lebanese authorities monitored Australian bomb plot suspects: minister," *Sydney Morning Herald*, August 22, 2017, and Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," War on the Rocks, January 4, 2017.

[r] Deputy Commissioner Phelan indicates experimentation was conducted, but says that the device itself was "very far" from completion. See "AFP and NSWP discuss the two Sydney men charged over terrorist acts." See also Rachel Olding and Ava Benny-Morrison, "'Catastrophic': How Australia narrowly escaped two 'sophisticated bomb plots,'" *Sydney Morning Herald*, August 4, 2017.

[s] Both of these points are arguable. *The Sydney Morning Herald* alleges that the chemical device target would have been "crowded spaces or public transport." Olding and Benny-Morrison. As to the handler's prerogative, see the following footnote.

[t] According to one understanding of Islamic State foreign terrorism operations planning, *al-Amn al-Khariji* operatives conduct attack creation and logistics largely according to their own cognizance, provided that they respect Islamic State leaders' strategic vision and mandates. Like the somewhat similar *auftragstaktik*, or "mission-based tactics," model used by the Imperial German Army in the late 19th and early 20th centuries, this operational doctrine emphasizes the innovation and initiative of Islamic State controllers.

[u] Whether the "mission-based tactics" model was or continues to be accurate can be disputed for at least two reasons. First, *al-Amn al-Khariji* operations may have changed after the group lost its primary coordination and training center in late 2016 (months before the Sydney plot). Second, former *al-Amn al-Khariji* leader Abu Mohammed al-Adnani is said to have involved himself with most of the group's ongoing operations and was undoubtedly part of the Islamic State's highest echelon. His successor may have also been routinely involved in decision making, to include the hydrogen sulfide choice. If so, chemical terrorism may feature in an as yet unclear way in Islamic State strategizing. Future evidence surrounding the Sydney incident may be key to understanding its wider associations.

[v] The first widely documented use of CW agents or weaponized industrial chemicals by the Islamic State dates to July 12, 2014. See Jonathan Spyer, "Did ISIS Use Chemical Weapons Against the Kurds in Kobani?" *Middle East Review of International Affairs* 18:3 (2014): pp. 90-94.

▶▶ **Citations are available at source's URL.**

***Markus Binder, Jillian Quigley**, and **Herbert Tinsley** are staff researchers at the Unconventional Weapons and Technology Division (UWT) within the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START).* *This article arose from their Department of Homeland Security-funded work on an Islamic State chemical and biological weapons behavioral profile, which analyzes the group's potential CB attack modalities against U.S. and Western interests.*


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
BIO NEWS

Gene Drives – An Emerging Terrorist Threat

By Richard Schoeberl

Conventional acts of terrorism will likely never fade away, and advancements in technology will continually raise concerns for governments and global security practitioners. The increasing threat and possibility of chemical, biological, radiological, nuclear, and explosive (CBRNE) use is evolving. Terrorist groups are actively seeking materials and the expertise to manufacture and utilize those materials in future operations. One of the frontiers in terrorism today involves a developing technology known as "gene drives."

DomPep Journal. Volume 14, Issue 12, December 2018
Source: https://www.domesticpreparedness.com/journals/december-2018/

Gene-drive technology uses genetic engineering to "drive" desirable or undesirable traits through a population. Without gene drives, genes have a 50/50 chance of being passed on during the reproduction phase, the gene-drive technology can cheat the reproduction phase to ensure that the desirable pair of chromosomes can or cannot be inherited by all offspring. In addition to altering the genes in an organism, the gene drive also makes the altered trait inheritable, thus passing it down to ensuing generations.

Richard Schoeberl *has over 23 years of security and law enforcement experience, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency's National Counterterrorism Center (NCTC). He has served in a variety of positions throughout his career, ranging from supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before these organizations, he worked as a special agent investigating violent crime, international terrorism, terrorist financing, cyberterrorism, and organized drugs. He was also assigned numerous collateral duties during his FBI tour – including a certified instructor and member of the agency's SWAT program. In addition to the FBI and NCTC, he is an author and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, Al Hurra, and Sky News in Europe. Additionally, he has authored numerous articles on terrorism and security. He is currently a Professor of Criminology and Homeland Security at Martin Methodist College and works with Hope for Justice – a global nonprofit combatting human trafficking.*

Biothreat Magnifies Critical Need to Ensure Appropriate Laboratory Security

By Robert Smith
Source: https://www.hstoday.us/subject-matter-areas/pandemic-biohazard/perspective-biothreat-magnifies-critical-need-to-ensure-appropriate-laboratory-security/

November 2018 – Over 100 years ago, the planet was ravaged by the 1918 Spanish Flu pandemic. This grim anniversary could serve to remind us of the magnitude of the catastrophe. The mortality rate was 20 times higher for 15- to 34-year-olds than previous years' flu outbreaks and actually depressed the average lifespan in the U.S. by 10 years (Tautenberger 1997). People died within hours of developing symptoms due to the rapid onset of secondary pneumonia infection, many with horrible effects (Grist, 1979). The recurring waves of outbreaks during the pandemic took the lives of 50 million worldwide (National Center for Immunization —). It is likely that most people cannot fully appreciate the level of suffering from a pandemic. The passage of time helps us to heal, helps us to forget.
Since the emergence of Highly Pathogenic Avian Influenza, experts have warned about a probable return of pandemic flu due to the continuous genetic recombination within the virus. Experts generally agree that a 1918-type pandemic could be one of the most disastrous

events to befall the planet. Besides the tragic loss of lives and wide-ranging human impacts, a pandemic

could also overwhelm limited resources from mass care, emergency response, public health and medical service sectors. In addition, the cascading effects of lost productivity and economic impacts could divert attention and consume resources from other critical sectors such as agriculture, natural resources, public safety and national security (FEMA 2016).

Still, the average person would not likely place this risk at the top of their daily concerns. Similar to other emerging health threats such as global warming and antibiotic resistance, the causative factors and warning signs for a pandemic may not rise to a sufficient level of significance in the cognitive consonance and the public demand for action may not occur short of the event horizon.

We have been fortunate not to suffer the re-emergence of a killer flu in human populations. However, a natural flu outbreak is far from our only biothreat. In recent decades, the likelihood of a new pandemic caused by the intentional release of a dangerous biological agent has increased. In this regard, we potentially face dual-threat scenarios – namely, international conflict and terrorism. The deliberate use of biological agents for terror and warfare dates back nearly 1,000 years. In recent history, the Japanese waged biowarfare against China during WWII using plague, cholera and typhus. The U.S. initiated a bioweapon development program in 1960 and terminated it in 1969 (Frischknect, 2003). The Soviet Union is reported to have developed biowarfare agents from plague, anthrax, and smallpox (Frischknect 2003). Prior to the first Gulf War, Iraq under Saddam Hussein built a biological weapon program (Zalinskas 1997) and there is reason to believe that North Korea, Syria, and Iran may have developed biowarfare programs. The risk persists despite international agreements against the development and use of biological weapons (UNOG 2018; UNODA 2018).

It is also well known that non-state actors seek access to biological agents for terrorist agendas (Coats 2018; Wagner 2017, Harris 2002). Rogue nations that conduct dark-web transactions in bioagents or failing states that lose track of bioassets during periods of political or economic instability are potential sources. The Defense Threat Reduction Agency (U.S. Department of Defense) works to reduce the prevailing likelihood of this threat (DTRA 2018).

Perhaps an even more likely source for access to potential bioterror agents is inadequate biosecurity in laboratories. Many U.S. labs store biological agents considered dual use, defined as having legitimate scientific purpose but also characteristics that could be used for bioterror. The 2001 anthrax attack (Amerithrax), the most lethal and widespread act of bioterrorism in the U.S., is believed to have originated in a U.S. lab (FBI 2010). There have been other bioterror attempts in the U.S., some limited in scale and others failed or thwarted by authorities. Following the anthrax attack, concerned scientists identified the biological agents most likely to be successfully employed for bioterror according to certain characteristics such as high infectivity, high mortality rate, long prevalence in the environment, and inadequate medical prevention and countermeasures. Laboratories maintain viable bioagents with these characteristics in sufficient concentration, properly preserved, and capable of generating a reproducing and infectious population within a few days.

In 2002, Congress passed the *Public Health Security and Bioterrorism Preparedness and Response Act* providing the authority for the Select Agent Rule, which requires registration and strict security measures at laboratory facilities possessing these types of agents (Federal Register 2007). Since then, security in U.S. laboratories improved significantly but, in many cases, not sufficiently. Frequent security assessments have demonstrated that it is possible to surreptitiously remove select agents from some laboratories without detection. Despite enhanced laboratory security, the theft and diversion of pathogenic and toxic agents from laboratories remains a likely scenario for individuals, groups or organizations with intent to access potential bioterror agents (NTI 2007, Coats 2018, Holgate 2017). It raises the question of whether enough time has passed since Amerithrax to make us forget the lost lives and the masses of people in line for the antibiotic ciprofloxacin.

One might think that the complex, scientific knowledge and processes required to prepare and disseminate biological disease agents to enable their survival and infectivity would reduce the threat probability. However, it is troublesome to consider that, of 13 separate biological attacks or attempted attacks in the U.S. from 1984 to 1996, nine were committed by individuals with scientific knowledge and laboratory access (professor, physicians (5), nurse, dentist and a lab technologist). The 2001 anthrax attack is believed to have been committed by a federal laboratory researcher (FBI 2010). The insider threat overcomes many traditional biosecurity protections. The Nuclear Threat Initiative states that "biosecurity remains an under-emphasized and under-financed global security priority (NTI 2007)."

Several modern realities elevate the probability of the bioterror risk:

- Proliferation of laboratories possessing select agents in the U.S. and in other countries
- Advancements in genetic engineering technology
- Simplified Do-It-Yourself (DIY) biotechnology kits and equipment

- The wide dissemination of terrorist organizations such as al-Qaeda and the Islamic State and their unconventional terror tactics
- Unstable foreign governments with unsecure laboratories and manufacturing facilities
- Dark web trafficking in unconventional weapons
- Greater international travel
- Declining funding for laboratory security
- Funding needs for increased incidence in emerging disease outbreaks and other emergencies
- Complacency on the part of laboratory organizations regarding the threat

Each of the above factors merits full analysis in a current biothreat assessment. However, for many biosecurity experts, recent technology in genetic modification (also called gene editing) could produce the most worrisome consequences (Coats 2018; NSABB 2018). In 2005, scientists collaborating from several research organizations used reverse genetics to reconstruct the 1918 Pandemic Influenza virus containing all eight viral gene segments (required for pathogenicity) (Tumpey 2005). Other researchers in 2017 reconstructed horsepox, a relative of smallpox, the agent of several horrific pandemics eradicated in 1980 through vaccination. It is believed that the smallpox virus could be reconstructed by the same technique (Kupferschmidt, 2017). Other genetic modification research called 'gain of function' creates or enhances disease-causing characteristics in otherwise harmless biological agents. The recent development of CRISPR-Cas9, a technology adapted from a naturally occurring gene editing process in bacteria, has significantly increased the speed and accuracy of genetic editing (Slaymaker et al 2016).

These new technologies place extraordinary power in the hands of the researchers with relevant expertise as well as increase the consequence of an intentional release. Considering the high stakes of a worldwide outbreak of a genetically engineered pathogen that is highly communicable, lethal, and unknown to our immune system, and for which we have no adequate prevention or countermeasures, our national leaders, regulators, and biodefense industry must stay ahead of the technology and events, and develop top-down and ground-up preventative and response strategies and controls. Locally, laboratory directors, biosecurity managers, and Institutional Biosafety Committees (IBCs) must be frequently retrained and reinvigorated to keep pace with new technologies and research objectives (Note: the NIH Guidelines are currently under revision) (NIH Guidelines, 2018).

The National Science Advisory Board for Biosecurity (NSABB), established by Congress through the *Public Health Service Act* (GPO 2011) and amended by the *Pandemic and All-Hazards and Preparedness Act* (U.S. Congress 2006), serves as a federal advisory committee that addresses issues related to biosecurity and dual-use research at the request of the United States government. This organization provides "advice, guidance and leadership regarding biosecurity oversight of dual use research." However, the NSABB's advisory oversight role is limited to federally conducted or supported research (NSABB 2018).

Many have called for the complete cessation of gain of function research that could have severe impacts. This may not be prudent. Even if all reasonable nations, scientific organizations, and researchers agree to abandon this genetic exploration, a single rogue actor would be sufficient to engineer a novel and lethal pathogen and the world's responders could be helpless to counteract it, at least not before considerable human loss. The only practical approach is to anticipate the risk, own the technology, and develop specific and effective countermeasures – i.e. we need the new microbe to develop the new vaccine. This approach is consistent with the NSABB charter, which takes into consideration "both national security concerns and the needs of the research community to foster continued rapid progress in public health and agricultural research" (NSABB 2018).

The ever-increasing pace of biotechnology compounds the need to ensure appropriate laboratory biosecurity. After all, some of this research is equivalent to creating precursors to bioweapons. The scientists that worked the U.S. Bioweapon Program in the 1960s were required to have top security clearance.

Of the aforementioned 'modern realities' contributing to bioterror risk, complacency is the one vulnerability that could be readily rectified. Although laboratories are more secure since the 2001 anthrax attack, there may be increasing reason for concern that some organizations have become lax. First, it is common for laboratory organizations to downplay the likelihood

of a bioterror event since few have occurred, and to direct their limited resources where they perceive the greatest need. There has been no major bio attack since the 2001 Anthrax attack. A small number of isolated attempts have occurred, mostly by individuals with personal or political agendas (Holgate 2017, James 2018). This should not downplay the threat. Although our terror-sponsoring enemies and their homegrown aspirants have recently resorted to low-investment, high-probability-of-success attacks such as vehicle ramming of pedestrians and random shootings and stabbings, they have always proven themselves to be adept and creative in transforming their terror game plan when they have detected new vulnerabilities. They have declared their interest in obtaining biological weapons (Coats 2018; Wagner 2017, Harris 2002).

Second, federal funding for emergency preparedness has declined since the 2001 Anthrax attack and the $3.8 billion allocation in 2005 to counter the threat from bird flu (CIDRAP 2005). Recent allocations to battle Ebola in Africa have been effective but are due to expire in 2019 (Yong 2018). Declining funding limits our medical response to intentional bioterror attacks as well as natural disease outbreaks as they produce similar consequences. U.S. investments to improve medical infrastructure and medical capabilities in developing and undeveloped nations, facilitate timely response to localized outbreaks, and prevent international spread of disease protects human health with the added benefit of reducing the future risk of bioterror. Most experts would agree that we need to do more to strengthen our medical and scientific capabilities to handle the unexpected.

Most laboratory organizations have developed security and emergency plans. However, far too many have not adequately maintained their plans with current information, have not provided regular security training to employees, and/or have not regularly exercised their plans to identify gaps and vulnerabilities. This lesson was obvious when Ebola crossed our borders in 2014 and CDC and local medical centers needed to quickly enhance laboratory infrastructure, equipment, and training (NHSC 2015; Bell 2016). It is clear that unprepared and poorly trained responses to medical crises could readily create new biosecurity vulnerabilities that result in diverted biological agents. Like most emergencies, the diversion of biological agents for terrorist ambitions will likely originate at a single location and, therefore, prevention and response must have a local focus.

Therefore, there may be a need for a more refined national biodefense strategy that goes beyond high-level national security standards by providing more specific direction to research and diagnostic laboratory organizations. The Select Agent Rule requires regular assessments of laboratory organizations and enforcement of infractions through fines and

possible criminal convictions. However, there are too many ways to circumvent these security requirements, especially for the insider threat.

New ideas and additional incentives are needed to achieve practical stopgaps against theft and diversion of dual-use agents and equipment. I offer some general laboratory recommendations for consideration.

- Government or the scientific industry should establish incentives for biosecurity through a biosecurity certification, accreditation or a rating system to reward those facilities with high achievement in security and preparedness and to encourage others to meet standards. Model biosecurity programs should be publicized and socialized within the industry.
- An Inter-organizational Biosecurity Working Group should be established for sharing information, processes, and ideas that have proven successful at the laboratory level (to some extent, this already occurs within some associations and during certain industry conferences).
- Government and industry should ensure sufficient funding for biosecurity to lessen vulnerability and prevent the accidental or intentional release of dual-use agents. At the same time, the level of annual operational funding for laboratory facilities could be contingent upon meeting biosecurity standards in full. This represents a conundrum and a potential for vulnerability unless laboratory directors and their funding organization maintain effective dialogue toward resolution.
- Within organizations, Institutional Biosafety Committees could take on the additional mantle of biosecurity planning and validation, or the organization could develop a separate Institutional Biosecurity Committee under the guidance of the National Science Advisory Board on Biosecurity.

For genetic modification research

- Government and the scientific industry should sanction and appropriately fund research programs to expand the realm of scientific research on genetic recombination that could lead to gain of function products. At the same time, a separate scientific body should be responsible for exploring the potential risks as well as monitoring the effectiveness of governmental controls. Researchers engaged in this program or any research or analysis of genetic recombination or reconstruction of microbes with the potential for catastrophic outbreaks should be required to obtain a Top-Secret classification prior to initiation.
- Government should require regular re-assessment of the full range of potential security risks within laboratory environments. The Federal Select Agent Program is limited to 'listed agents' only, does not cover emerging pathogenic agents and does not effectively cover novel agents due to genetic manipulation.
- The public should be continuously engaged in the discussion and the processes of considering approval of research in genetic modification of biological agents if their accidental release could have a significant impact on public health, agriculture, food security, or the ecosystems.

It is essential for the U.S. to continue to strengthen our biosecurity within U.S. laboratories, hospitals, and manufacturing facilities as well as develop better strategies for surveillance and countering unsanctioned development and application of bioterror weapons. The recommendations offered here may not be popular among laboratory directors and managers who already struggle with limited resources and time for regulatory compliance. However, the stakes are too high to permit continuing gaps in security and incident response planning. We should not wait until the next disaster occurs to complete the job of securing our nation's laboratories possessing dual-use materials. And we should understand that providing sufficient funding to prevent or respond effectively to the next major public health challenge inside and outside the U.S. is the most cost-effective approach in the long run.

The process of biosecurity requires careful analysis of the spectrum of current and emerging biological threats and their impacts as well as the effectiveness of disease prevention, identification, monitoring, and medical response. Throughout all these functions, regulators, public health planners, and responder agencies must analyze the complexities of cost and benefit, and make effective decisions on investments and actions. While the stakes are potentially very high from bioterror attacks, they still must be analyzed with proper perspective to the higher probability and equally high impact of natural disasters.

As the Director of Emergency Programs at Communications Resource Inc. (CRI), ***Robert E. Smith*** *manages and provides expertise for federal departments and agencies in emergency preparedness, emergency response, continuity of operations, continuity of government, security risk assessment, and security planning. Mr. Smith joined CRI in 2002 to improve security and resilience at federal laboratory facilities throughout the U.S. following the 2001 anthrax attack. Mr. Smith specializes in consultative services for projects with chemical, biological, radiological, and explosive (CBRE) risk components. Since 2002, he has conducted on-site security risk assessments for over one hundred federal laboratories, irradiator facilities and High Hazard dams. Mr. Smith obtained a Bachelor of Science degree in biological sciences and a Master of Sciences degree in microbiology from the University of Maryland, and a Master of Science degree in Biodefense from George Mason University.*

Hazmat team combs raided apartment in Niagara Falls after FBI agents get sick

Source: https://buffalonews.com/2018/12/26/hazmat-team-combs-raided-apartment-in-falls-after-fbi-agents-get-sick/

Dec 27 – Niagara County hazmat team and police from at least two agencies swarmed a unit at the Packard Court Apartments in Niagara Falls Wednesday after several members of the FBI's Joint Terrorism Task Force got sick in the wake of a Dec. 14 raid that resulted in the arrest of the occupant for possessing drugs, firearms and improvised explosives.

Niagara County sheriff's deputies and Niagara Falls police officers were on the scene on Pine Avenue, along with FBI Special-Agent-in-Charge Gary Loeffert, as hazardous materials investigators probed the apartment for any signs of what caused the mysterious respiratory ailments.

Officials took samples and conducted initial tests that will be examined by the Niagara County Health Department, but won't have results right away and haven't drawn any conclusions yet.

Agents from the FBI and the U.S. Bureau of Alcohol, Tobacco and Firearms, along with Niagara Falls police and sheriff's deputies, raided the apartment nearly two weeks ago and arrested 28-year-old Jeffrey Richards, after finding cocaine, heroin, marijuana, 10 guns and ammunition, and an improvised explosive device. He faces a series of criminal charges.

Wednesday's mobilization came in response to a request by the FBI, which only learned after the Christmas holiday that "a handful of agents and investigators" from the task force had independently "developed flu-like symptoms" in the days after the team executed a search warrant at the apartment, said FBI spokeswoman Maureen Dempsey.

"People didn't realize other people were sick that had been on that search," Dempsey said, citing the holidays and vacations. "When it came to light in the last day or two that people had symptoms and they were all at the search, they wanted to go back and check the location."

Dempsey stressed that the symptoms did not materialize on the scene or immediately after the search, but in the following days, so it's not clear if they were connected to anything in the apartment. She said no one was hospitalized as a result, but "quite a few people did go see the doctor."

Still, she said, "it just seemed like a big coincidence, so we're just trying to make sure there was nothing at that location that caused any of the illnesses."

EDITOR'S COMMENT: Strange story! In class, we always make a point that it is difficult to spot a bioterrorism attack because all category "A" pathogens trigger a flu-like prodrome symptomatology that lasts according to the incubation period of the specific agent released. This incident is a good

opportunity to establish a protocol on post operation health procedure lasting a week or so of daily reporting of health statuse of the personnel participated in the operation. Might be a bureaucratic overloading but it can act as a limited syndromic surveillance that can save us from future troubles.

Sidra Medicine launches poison treatment wing

Source: https://www.gulf-times.com/story/617803/Sidra-Medicine-launches-poison-treatment-wing

Dec 29 – Sidra Medicine, Qatar's specialist women's and children's hospital, announced the expansion of its emergency medicine services with the launch of its clinical toxicology services. This includes a "poison helpline", training workshops and courses and introduction of "multiple new poison antidotes".
The initiatives are part of Sidra Medicine's efforts to treat poisonings and poison exposures for patients nationwide and support Qatar's healthcare networks in preparedness for toxicology related incidents.
The 'Qatar Poison Center' is a free call center service by Sidra Medicine's Department of Emergency Medicine. The helpline provides poisoning management and treatment advice for both children and adults.
This helpline is open to the general public and hospitals. **It accepts calls in English and Arabic on 4003 1111 from 9am to 1am seven days a week.** Callers will receive expert and timely poisoning management advice over the phone from pharmacists and physicians with training and expertise in clinical toxicology.
Sidra Medicine's chairman, Emergency Medicine Dr Khalid al-Ansari said, "Every year globally, emergency departments have visits by frantic patients and parents who are worried that they or their child have been poisoned. Often, ER visits after poison exposures are unnecessary, but sometimes they are lifesaving.
"People can call our free helpline and receive information and advice about a poison exposure. They will be advised what to do at home, and whether a visit to an emergency department is needed. As with poison centers in North America, UK, and Australia, our services are for both adults and children of all ages. The service is based on best practice models that have been successfully applied in North America. We are proud to bring this level of service and expertise to Qatar."
The Qatar Poison Center can help with questions about exposure to or poisoning with household products; chemicals at work or in the environment; drugs (prescription, over-the-counter, or herbal medicines); gases and fumes; and all envenomations such as snake bites, scorpion sting, spider bites, and jellyfish stings.
As part of its goal of preparedness and improving poison related assistance and care, Sidra Medicine has brought in new antidotes that were previously unavailable in Qatar or the GCC. I**t will also house antidotes to treat a wide variety of poisonings including radioactive isotope exposures.**
In addition to this, the healthcare organisation will participate in a new antidote-sharing program, where new, costly, or infrequently-needed antidotes will be available for patients at other hospitals in Qatar. **To support Qatar's capacity to respond to radiological, chemical and HAZMAT (hazardous materials) incidents, Sidra Medicine will also be hosting a series of cutting-edge courses and training programs.**
Endorsed by the American College of Medical Toxicology, the courses are scheduled for the first quarter of 2019, and will cover Radiological Incidents & Terrorism, Chemical Terrorism, and Advanced HAZMAT Life Support. More details will be shared in the new year.
Sidra Medicine's Department of Emergency Medicine is collaborating with the Medical Education department to offer clinical toxicology training for physicians, pharmacists, medical students, and pharmacy students and other trainees. The first trainees are scheduled to begin at Sidra Medicine in March 2019.
Al-Ansari explained, "We are making great strides in developing and advancing Qatar's healthcare offering. The development of our clinical toxicology services and programs is a testament to our goal to provide comprehensive services as a healthcare provider.
"Our toxicology services are not just for our patients but has been extended to support the safety and well-being of people of all ages throughout the entire country. We look forward to

working closely with our partners in Qatar's healthcare network in our ongoing commitment to keep patients and families safe and well cared for."

The Qatar Poison Center helpline does not replace 999 emergency services. In the case of a medical emergency, immediate danger, or need for critical medical attention, calling 999 is recommended.

PAE Lands $75.2M BioWatch Contract

Source: https://www.prnewswire.com/news-releases/pae-lands-75-2m-biowatch-contract-300771513.html

Dec 31 – PAE, a leader in supporting the U.S. government's counter-terrorism and counter-threat efforts, has won a $75.2 million contract with the Department of Homeland Security, Countering Weapons of Mass Destruction Office, BioWatch Program, a multi-city federal program dedicated to detecting airborne biological threats. With internationally renowned experts in counter-weapons of mass destruction and chemical, biological, radiological, nuclear and explosives successes, PAE secured the contract.

"This new opportunity stems from our growing base of experts specializing in counter-WMD and CBRNE solutions," Heller said. "We're proud that we can meet the needs of the U.S. government as it works to ensure the safety of us all."

Throughout the war on terror, PAE has worked with the intelligence community and the Department of Defense to develop counter-threat solutions to support the work of the U.S. government abroad and the safety of its citizens at home. Including more than a decade of counter-threat work throughout Iraq and Afghanistan, PAE has built advanced expertise the U.S. government continues to rely on.

PAE-led scientists will work in state-of-the-art labs supporting monitoring systems that are the frontline early warning system against possible airborne attacks. BioWatch was created in the wake of post 9/11 anthrax threats. From dozens of locations, BioWatch runs the nation's network of air sensors designed to identify and locate potential pathogens released into the air and alert federal authorities. In addition to screening major cities, BioWatch also monitors major public events such as the Super Bowl.

About PAE

PAE is a leading provider of enduring support for the essential missions of the U.S. government, its allied partners and international. With over 60 years of experience, PAE supports the execution of complex and critical missions by providing global logistics and stability operations, technical services and national security solutions to customers around the world. PAE has a global workforce of approximately 20,000 people, operates in more than 70 countries on all seven continents and is headquartered in Arlington, Va.

U.S. health worker monitored as DRC Ebola nears 600 cases

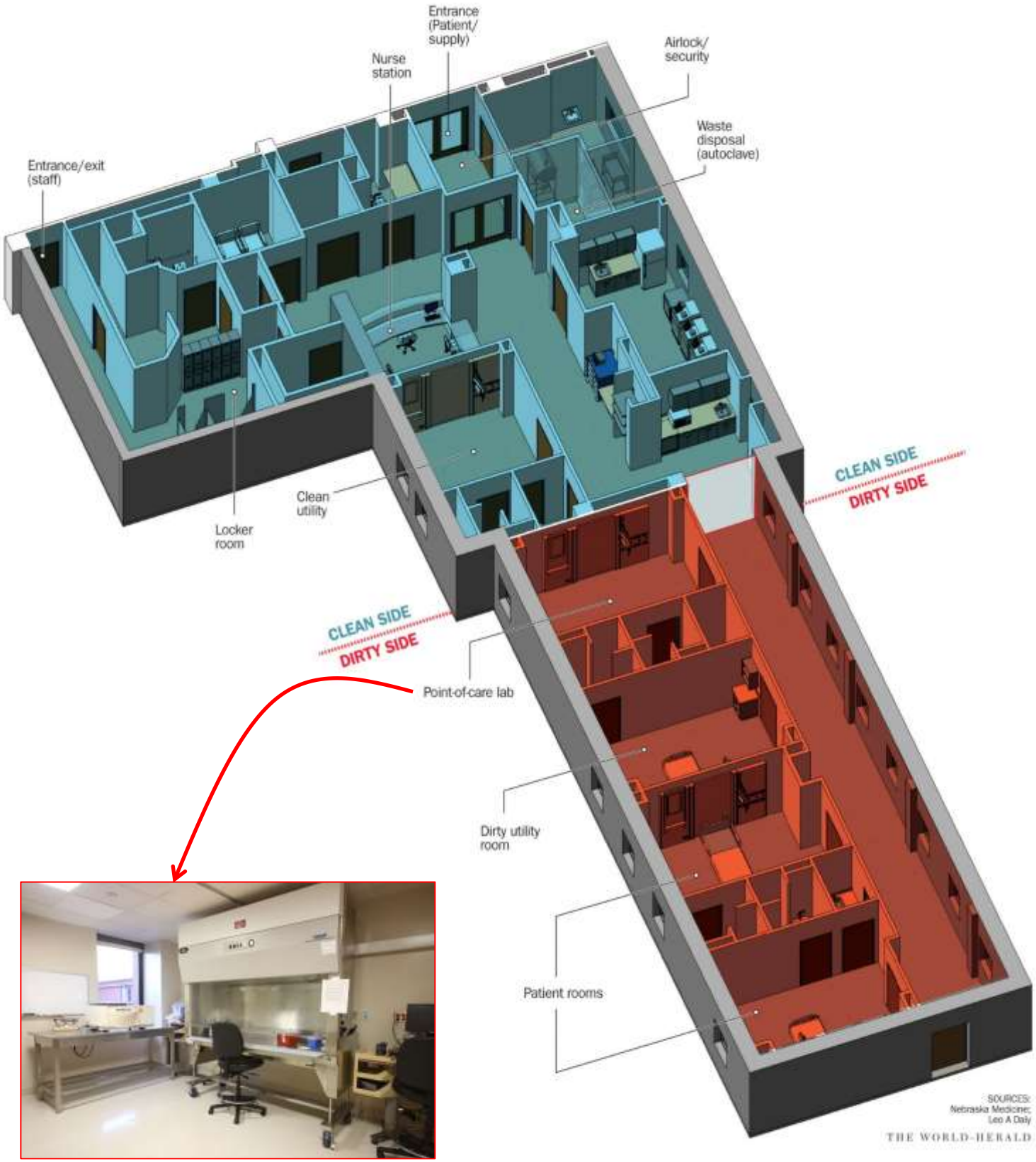
Source: http://www.homelandsecuritynewswire.com/dr20181231-u-s-health-worker-monitored-as-drc-ebola-nears-600-cases

Dec 31 – **A U.S. healthcare worker has been flown to the United States for observation after potential Ebola exposure in the Democratic Republic of the Congo (DRC), where the Ebola outbreak has now grown to 598 cases amid violent protests.**

Monitoring in Nebraska

An American providing medical assistance in the Democratic Republic of Congo recently experienced a possible exposure to the Ebola virus and is in Omaha for monitoring," the Nebraska Medical Center said in a 29 December news release.

The health worker has no symptoms, the medical center said. If symptoms begin, the patient will be housed in the Nebraska Biocontainment Unit at the center, which was established to treat people who have serious, high-risk diseases.



22 nurses, 10 lab workers, 6 respiratory therapists, 5 care techs and dozens of physicians

"This person may have been exposed to the virus but is not ill and is not contagious," said Ted Cieslak MD, infectious diseases specialist with Nebraska Medicine and associate professor of epidemiology in the University of Nebraska Medical Center College of Public Health.

The healthcare worker was transported by automobile and private plane to Nebraska. Monitoring could last 2 weeks, but Nebraska Medical Center said it would not provide updates "unless the need arises" or if the person is transferred to the biocontainment unit.
Staff at the unit treated three patients who had Ebola in 2014 during West Africa's outbreak, including one who died. The center monitored several others in 2015 who never developed the disease.
Politico identified the person as a 39-year-old physician.

Five new DRC cases amid violence
CIDRAP reports that over the weekend the DRC health ministry reported 5 new Ebola cases, 2 in Butembo and 1 each in Oicha, Komanda, and Mabalako. They bring the outbreak total to 598 cases, 548 of which have been confirmed.
Four new deaths were also confirmed 29 December through today, in Beni, Oicha, Mabalako, and Komanda, bringing the total to 363, for a case-fatality rate of 61 percent. All of the newly reported deaths were recorded in the community, which means greater virus exposure to family and caregivers and a higher risk of further cases.
On 29 December the DRC health ministry reported no new confirmed cases "because of the paralysis of the activities of the riposte [response] in Beni, Butembo, Komanda, and Mabalako." Immunization, contact tracing, and other response efforts have been stopped or dramatically curtailed in recent days because of violent protests.
For example, three health centers in Beni were ransacked on 27 and 28 December, and two of them burned, Media Congo reported late last week.
The health ministry said on 29 December, "The activities of the response resumed timidly this Saturday, December 29, 2018, in Beni and Butembo. The rehabilitation works of the

Beni Transit Center are underway. The removal of barricades placed on the roads by the demonstrators allowed the ambulances to circulate and recover some sick patients.
"Laboratories in both cities were operational. No vaccination activity took place for the third day in a row. Some dignified and safe burials were made in both health zones."
In its update today, the DRC health ministry said Ebola vaccinations have yet to resume, keeping the number of people vaccinated at 53,737. Officials said, however, that they are investigating 47 suspected cases.

Several weeks ago, the DRC Ebola outbreak grew to become the second-largest in history. The immense West Africa outbreak of 2014-2016 affected 28,616 people, including 11,310 deaths, for a case-fatality rate of 40 percent.
The third-largest Ebola outbreak occurred in Uganda in 2000, with 425 cases and a death rate of 53 percent.

EDITOR'S COMMENT: Just two remarks on the design of the biocontainment unit: (1) airlock should be the only entrance/exit struction for both staff and patients. Here there is a separate door for staff only. If so, how do they keep steady negative pressure inside the unit? Airlock (or better, a secnd airlock) should work better in the clean/dirty border area; (2) There is a door in the "dirty side" of the unit – what is it for? In addition, I did not like very much the windows in this part of the unit. Patients' condition does not allow them enjoying the views! (3) There is no clear view [?] on the showers available for staff when ending their shift and doff their PPEs.

The Government's Bioterror-Response Website May Be Leaking Sensitive Data

By Patrick Tucker
Source: https://www.defenseone.com/technology/2018/12/governments-bioterror-response-website-may-be-leaking-sensitive-data/153518/

Dec 13 – **DHS inspectors and a whistleblower say the site, which would be used to coordinate federal responses to a bioterror attack, isn't secure.**
The U.S. government's chief tool to coordinate responses to bioterror events has for years suffered from big security problems, according to DHS inspectors and a former employee.
For more than 15 years, the United State's first line of defense against a major biological incident has been a program called BioWatch. Its sensors, mounted (600 in more than 30 cities across the U.S.), works like canaries in a coal mine. If a terrorist released, say, a deadly

aerosolized biological toxin into Grand Central Terminal, sensors would pick up the toxin. Healthcare workers collect samples from the sensors and bring them to BioWatch labs every day.

If the analyzed samples indicate a threat (and not a false alarm, which happens more often than DHS likes to admit) a BioWatch Actionable Result sparks more work and a lot of coordination from local public healthcare workers, law enforcement, and officials. Hopefully, that happens in time to avert a pandemic or other public-health crisis.

That coordination between health workers and government would occur over a website called Biowatchportal.org. It's a restricted-access website and DHS considers the information on it to be very sensitive. In theory, it's the sort of information that an adversary could use to compromise the system, find sensor locations to disable or spoof them, and even target the health workers or officials who use the site. That includes officials in the Departments of Defense and State, the FBI and other law enforcement agencies, and many others.

But biowatchportal.org may be exposing this information, according to the DHS inspector general and a former DHS employee.

In 2016, Harry Jackson, the information systems security manager for the BioWatch system, alerted his superiors to the fact that the .org domain wasn't safe enough for the sort of information that people posted to the site. The portal was being externally hosted outside of the DHS firewall (rather than at a .gov domain, which would have been safer.) That presented a big security problem. He also found five subdomains connected to the portal, each with its own vulnerabilities.

But his superiors weren't interested, Jackson said in a recent interview. So last year, he published his work in the *Journal of Bioterrorism and Biodefense*, describing the system's fundamentally flawed architecture.

He said that program officials tried to pull his security clearance, but that the DHS Chief Security Office determined that he had done nothing wrong.

In November 2017, the DHS Office of Inspector General essentially agreed with Jackson's conclusions. Their audit found that the DHS OHA office was failing to secure the sensitive personal information of BioWatch users. What's more, OHA was undermining their own privacy officer — the person in charge of making sure the site wasn't leaking important personal information— by denying the officer "adequate authority and resources to carry out the various required privacy management responsibilities." The report added that the officer did not have the support of leadership.

The report made 11 recommendations for fixing the program, including "Establish a plan of action and milestones to bring the BioWatch system to a moderate rating for confidentiality, including the security controls required to safeguard privacy-sensitive systems," and "Move the BioWatch system to a trusted domain to comply with system security requirements and thereby safeguard sensitive and personally identifiable information."

Officials with the DHS's OIG said that auditors had completed a new review in November. OHA, they said, had fixed some of the problems and had submitted a "corrective action plan" to address the remaining issues.

"In our latest review of OHA's corrective action plan, we are satisfied with the component's progress and have formally closed seven of the eleven recommendations. While progress is underway for the remaining four recommendations, they will remain open," a DHS official said.

The statement is tantamount to an admission that four issues still exist. The OIG declined to say which of those recommendations remained open but Biowatchportal.org remains the portal in use for the program.

DHS is looking to replace BioWatch with a new system, one that uses sensors to alert the government to the presence of biological weapons in something closer to realtime, rather than every 24 hours (at the earliest.) Until that happens, the U.S. is stuck with BioWatch as its first line of biodefense.

Patrick Tucker *is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for* The Futurist *for nine years. Tucker has written about emerging technology in* Slate, The Sun, *MIT*

Technology Review, Wilson Quarterly, The American Legion Magazine, *BBC* News Magazine, Utne Reader, *and elsewhere.*

EDITOR'S COMMENT: I do not know if the website is secure or not. What I know is that donning of PPEs of first responders shown in the photo used in this article is far from perfect. I can see skin! And one of them is the Incident Commander!

New Ebola case reported in Sweden with patient isolated in Uppsala hospital

Source: https://www.independent.co.uk/news/world/europe/sweden-ebola-alert-hospital-uppsala-burundi-patient-isolated-a8711301.html

Jan 04 – A man suspected of suffering from the deadly Ebola virus is being treated in isolation in a Swedish hospital.

The patient is in Uppsala University hospital, in the city north of Stockholm, after vomiting blood, and had reportedly returned from a three-week trip to Burundi in East Africa.

In a statement, the Uppsala authorities said it was so far **"only a matter of suspicion",** adding: "Other diseases are quite possible."

The hospital in the town of Enkoping where the patient was first admitted had its emergency room shut down and staff who treated the patient were "cared for", *AP* reports.

The patient was later transferred to the infection clinic in Uppsala. Test results are expected later today.

"The patient came in Friday morning and reportedly was vomiting blood which may be a symptom of Ebola infection," hospital spokesman Mikael Kohler told local newspaper *Upsala Nya Tidning*.

There is no known Ebola outbreak in Burundi, but it borders the Democratic Republic of Congo, which has been fighting an outbreak for almost six months.

The disease has killed 356 of the 585 people known to have been infected.

The epidemic in a volatile part of Congo is the second worst ever, according to the World Health Organisation.

The largest outbreak was in 2013-2016 in West Africa, where more than 28,000 cases were confirmed and over 11,000 died by the time the WHO declared the epidemic over.

The haemorrhagic fever's virus is spread through contact with the bodily fluids of those infected.

Symptoms can appear similar to those of flu, before the onset of vomiting, diarrhoea, a rash and internal and external bleeding. It is often fatal.

All major outbreaks have been in Africa, though isolated cases have been reported outside the continent.

In August 2014, British volunteer nurse William Pooley became the first Briton to contract Ebola after working in Sierra Leone. He was flown back to the UK for emergency treatment and went on to make a full recovery. The same year, Scottish nurse Pauline Cafferkey was also contracted the virus after returning from Sierra Leone and fell severely ill, spending several weeks in London's Royal Free Hospital.

EDITOR'S COMMENT: Almost four years after the big outbreak (why we call it outbreak???) in Western Africa, it seems that the European hospital sector is still not prepared to deal with a single case of a category "A" pathogen like Ebola virus (if proven to be EVD). The initial receiving hospital

was closed and personnel was under surveillance. Perhaps again nobody asked "have you recently travelled abroad" until the bloody vomiting happened (just like the Texas case in the past). Preparedness is still only for big cities' hospitals forgetting that the unexpected can happen anywhere, anytime – this time in Enkoping. And of course, a huge struggle to identify patient's contacts and examine the route he followed from Burundi to Sweden and then airport personnel, taxi/buss used, neighbors, super market, etc. where he might spread the virus to other people. If he survives, authorities (and the patient) must keep in mind that the virus is able to survive in semen for 565 days!

Measles outbreak reported in Skopje

Source: http://outbreaknewstoday.com/measles-outbreak-reported-skopje-21226/

Jan 02 – Health officials in FYROM are reporting (computer translated) a measles outbreak in the capital city of Skopje. Minister of Health Assoc. Dr. Venko Filipce announced the outbreak declaration today.

In addition to the seven cases that appeared in the Skopje settlement, Radishani ten days ago, there are now 12 new cases from almost all municipalities in Skopje, out of which six are officially laboratory confirmed and six have a clear clinical picture and are awaiting official laboratory confirmation.

The outbreak gas affected both children and adults, all of which are unvaccinated.

"We inform that unfortunately in the territory of the City of Skopje there are 12 new cases, 6 are definitely confirmed by the relevant analyzes, for the remaining 6 we expect the next day. Of the 15,000 unvaccinated children with vaccine calls, only 310 were vaccinated, which is a small figure. It is a good circumstance that schools do not work because of the holidays.

"But, of course, we have the situation under control. This is an extremely serious disease that, unfortunately, is sometimes fatal to the lives of children. Any disregard for the recommendations is an additional risk for the health of the whole population, "said Minister Filipche (computer translated).

Posible public exposure to ricin (USA)

Source: https://www.kiro7.com/news/local/ricin-scare-at-olympia-hospital/898723538

Jan 04 – The Thurston County Sheriff's Office said a patient admitted to taking the poison ricin inside Providence St. Peter Hospital [Olympia, WA] Wednesday [2 Jan 2019] evening, potentially putting dozens of people at risk. "This is a public safety concern. When you go to the [emergency room] you might expect to catch the flu, you don't expect to be exposed to ricin," said a man who was inside the hospital at the time of the incident. The man asked to keep his name private because he's worried about his family member, who's still hospitalized."[Hospital workers] said there was potentially an exposure in the [emergency room] to ricin," he said. "They told us to watch out for difficulty breathing, nausea, vomiting, fever."

The sheriff's office said the incident began around 8 PM Wednesday [2 Jan 2019]. An 18-year-old Olympia man called medics because he wasn't feeling well. When medics responded to his home, they had no idea the man was making ricin. Neighbors on the block

were also in the dark. "It's a scary situation. You don't know if he's going to leave it in the mailbox or anything, or if any of us could be exposed to that," said Dave Conn.

Ricin is a highly toxic compound found in castor beans.

"It's scary, it's really scary, there's a lot of younger kids in the area," said Stephanie Conn.

Deputies said the man admitted to hospital workers he started feeling sick while making ricin at his house and that he brought some with him to the emergency room.

The Federal Bureau of Investigation (FBI) is now handling the investigation. Officials sent KIRO 7 a statement regarding the incident: "The FBI responded shortly before 11 PM to Providence St. Peter Hospital in Olympia, WA, to learn more about the contact of an individual with a possibly suspicious material. The FBI transported the material to the Washington Department of Health's public health lab for testing."

Hospital workers said there is not an immediate concern for people who were inside the hospital at the time. They plan to follow up with people who were in the emergency room.

Ricin [comment]

The article does not tell us if the ricin was brought to the hospital in a powered form (presumably) or how fine the powder was. *Likely most hospitalized people don't have a worry. If the container were opened and even small amounts aerosolized, those nearby, including the patient/perpetrator, would be at most risk of exposure.*

Why was this individual making, presumably powdered, ricin? One has to wonder what nefarious plans or activity this individual had in mind to be making this product. Why did he bring this to the hospital? Was he trying to test the effectiveness of his product? It seems he may have at least one test subject: himself.

It is hoped the authorities will figure out the answers to these and other questions associated with this individual, his activities, and his intentions.

Ricin is a poison found naturally in castor beans. If castor beans are chewed and swallowed, the released ricin can cause injury. Ricin can be made from the waste material left over from processing castor beans. It is a potent protein derived from the beans of the castor plant (Ricinus communis). Castor beans are used in the production of castor oil, a brake and hydraulic fluid constituent. The aqueous phase of the process, termed the "waste mash," is 5% to 10% ricin.

Castor oil does not contain ricin. *Ricin has been used experimentally in medicine to kill cancer cells. Ricin works by getting inside the cells of a person's body and preventing the cells from making the proteins they need; hence, it is often called a*

toxalbumin. Without the proteins, cells die. Eventually this is harmful to the whole body, and death may occur.

Ricin can be in the form of a powder, a mist, or a pellet, or it can be dissolved in water or weak acid. It is a stable substance under normal conditions, but can be inactived by heat above 80^{0}C.

Effects of ricin poisoning depend on whether ricin was inhaled, ingested, or injected. The major symptoms of ricin poisoning depend on the route of exposure and the dose received, although many organs may be affected in severe cases. Initial symptoms of ricin poisoning by inhalation may occur within 8 hours of exposure. Following ingestion of ricin, initial symptoms typically occur in less than 6 hours.

Inhalation: *Within a few hours of inhaling significant amounts of ricin, the likely symptoms would be respiratory distress (difficulty breathing), fever, cough, nausea, and tightness in the chest. Heavy sweating may follow as well as fluid building up in the lungs (pulmonary edema). This would make breathing even more difficult, and the skin might turn blue. Excess fluid in the lungs would be diagnosed by x-ray or by listening to the chest with a stethoscope. Finally, low blood pressure and respiratory failure may occur, leading to death. In cases of known exposure to ricin, people having respiratory symptoms that start within 12 hours of inhaling ricin should seek medical care.*

Ingestion: *If someone swallows a significant amount of ricin, he or she would develop vomiting and diarrhea that may become bloody. Severe dehydration may be the result, followed by low blood pressure. Other signs or symptoms may include hallucinations, seizures, and blood in the urine. Within several days, the person's liver, spleen, and kidneys might stop working, and the person could die.*

Skin and eye exposure: *Ricin is unlikely to be absorbed through normal skin. Contact with ricin powders or products may cause redness and pain of the skin and the eyes.*

Death from ricin poisoning [may] take place within 36 to 72 hours of exposure, depending on the route of exposure (inhalation, ingestion, or injection) and the dose received. If in suspected situations where ricin may have been disseminated, preliminary environmental testing by public health or law enforcement authorities may detect ricin in powders or materials released into the immediate environment. Persons occupying such areas may initially be observed for signs of ricin poisoning.

No widely available, reliable medical test exists to confirm a person has been exposed to ricin. Because ***no antidote exists*** *for ricin, the most important factor is to avoid ricin exposure in the 1st place. If exposure cannot be avoided, the most important factor is then getting the ricin off or out of the body as quickly as possible.*

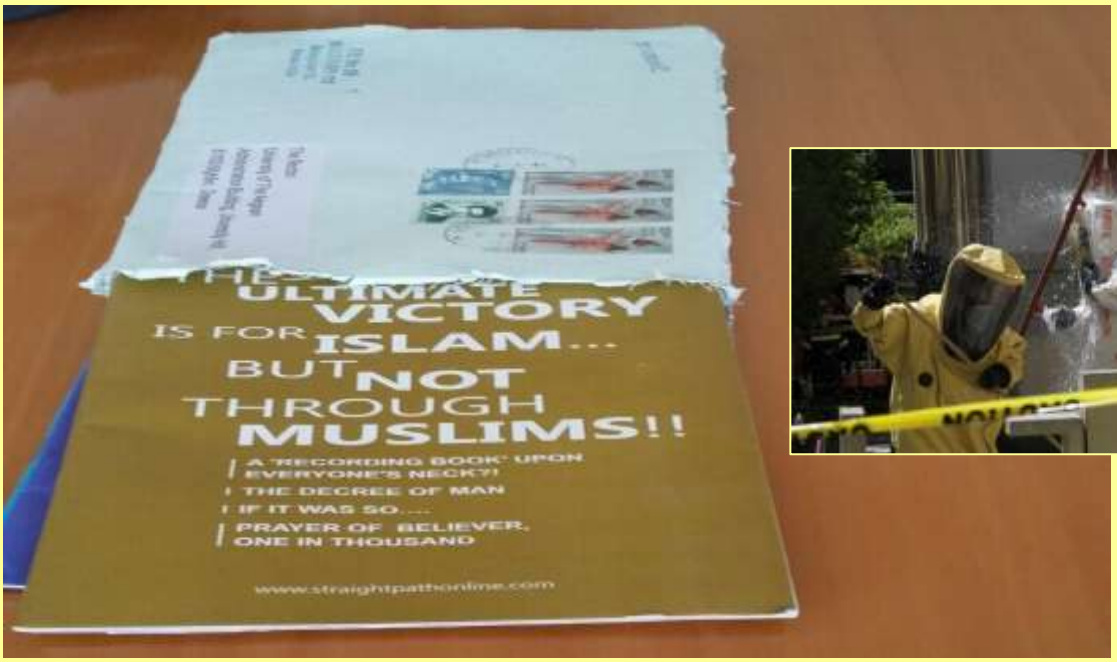
Symptomatic ricin poisoning is treated by giving victims supportive medical care to minimize the effects of the poisoning. The types of supportive medical care would depend on several factors, such as the route by which victims were poisoned (that is, whether poisoning was by inhalation, ingestion, or skin or eye exposure). Care could include such measures as helping victims breathe, giving them intravenous fluids (fluids given through a needle inserted into a vein), giving them medications to treat conditions such as seizures and low blood pressure, flushing their stomachs with activated charcoal (if the ricin has been very recently ingested), or washing out their eyes with water if their eyes are irritated.

▶▶ **Portions of this comment were extracted from** https://emergency.cdc.gov/agent/ricin/facts.asp

Greece: Suspicious envelopes mailed to universities

Jan 10 – An envelope containing a chemical was mailed to the Dean of the University of Aegean in capital city Mitylini, Lesvos Isalnd. The envelope was mailed fron India. Five employees exposed were admitted to local hospital some complaining for mucus

membranes irritation that soon resolved. Special Police CBRN Unit from Athens arrived with a military aircraft to further investigate the incident. THIRTY similar envelopes were mailed to various educational



facilities (polytechnic schools, universities, technological institutes) all over Greece.

EDITOR'S COMMENTS: (1) Envelopes and content were soaked with irritating chemical (not powder) used in glue industry and printing inks (does the latter ring a bell?); (2) Are these incidents somehow connected with the recent 38 asbestos Australian suspicious packages mailed to national and international diplomatic authorities? (3) Were they part of an exploitation plan to validate CBRN preparedness? (4) Envelopes were mailed from India or from Greece – is not that difficult to find Indian stamps or counterfit a post office stamp; (5) Was the Greek response the right one? By studying publiced photos and some videos, training problems identified again in all special units involved mainly because fire fighters insist to follow certain norms not compliant with international standard operational procedures.

After 14 years of deep involvement in efforts to promote an effective CBRN training, I feel I failed to inspire changes and make colleagues in high places to expel the attitude that it will not happen to them and therefore spending money to modernize training and build a CBRN culture is an unnecessary luxury not worthing further investment or attention.

Is Kenya at Risk of a Bioterrorism Attack?

Source: https://sokodirectory.com/2019/01/is-kenya-at-risk-of-a-bioterrorism-attack/

Jan 07 – **The United States (US) has cautioned Kenya of a possible terror attack from unsecured biological agents stored in health facilities and Kenya Medical Research Institute (KEMRI).**

The warning document was released in December 2018 and reveals undercover efforts to secure pathogens at Kenya's KEMRI.

The Defence Threat Reduction Agency (DTRA), under instructions from the US Government, is monitoring the ongoing construction of a secure storage facility at Kemri. The US is financing the

construction of a sample storage facility at Kemri which is es timated to be at 607 million shillings and is 90 percent of the total cost.

The Government is then expected to finance the remaining 10 percent which will include CCTV installations expected to cost 50 million shillings with another 40 million shillings to enable maintenance of the security software for five years.

The warning document creates focus onto the dangers brought about by the pathogens in the health facilities and terms them as a serious threat to the Country's national stability.

In May 2016, police were reported to have foiled a massive biological attack using anthrax by a terror group believed to have had links to the Islamic State (IS), a couple and a woman were arrested in the operation.

Kenya has experienced the horror of terrorist attacks in form of grenades and gunmen but is yet to be exposed to a biological attack commonly termed as Bioterrorism.

The naivety that comes with not having been faced by bioterrorism should be of concern to our Government which needs to propel it to step up on its bioterrorism surveillance.

Where will the world's next Zika, West Nile or dengue virus come from?

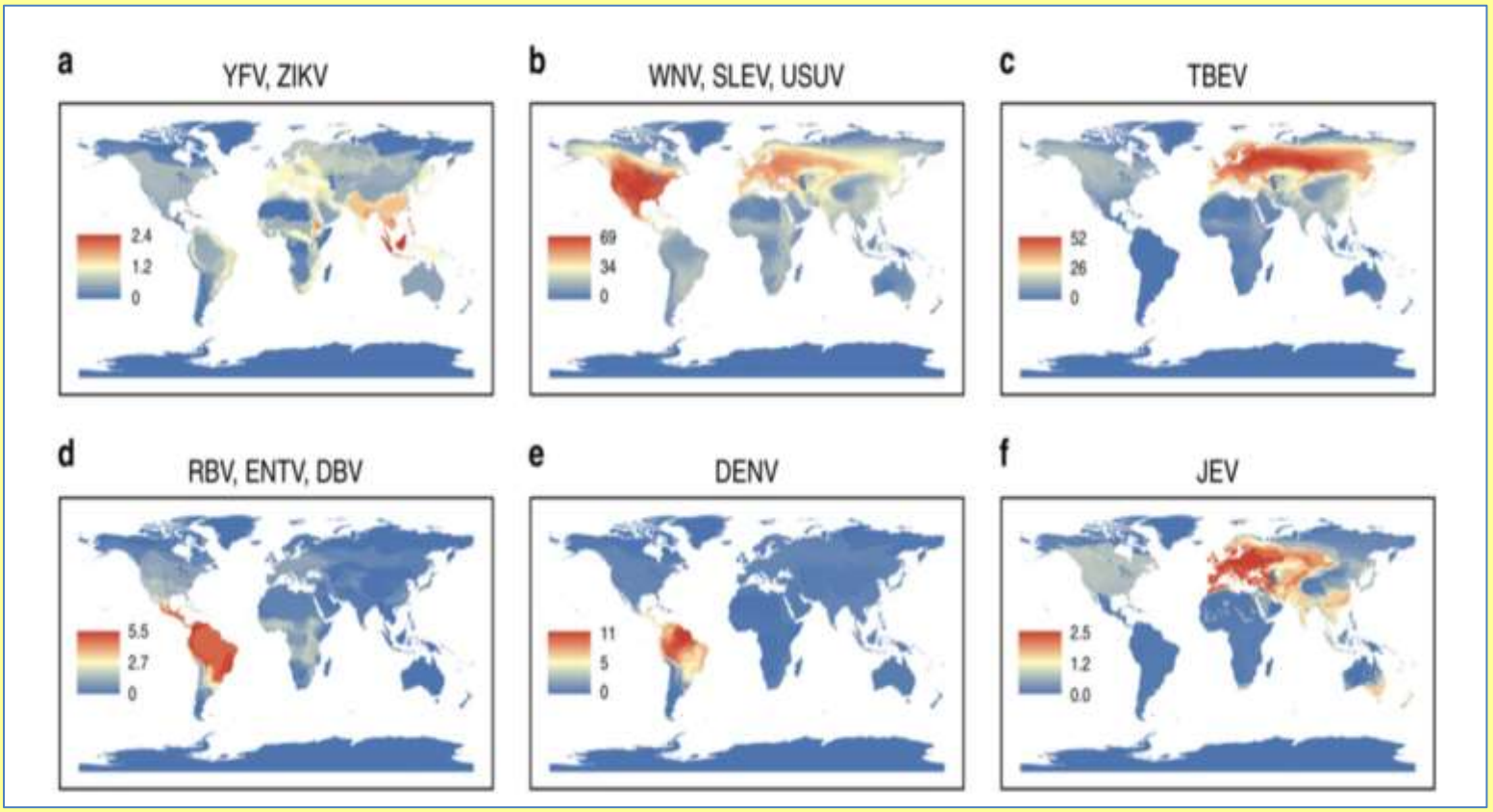
Source: https://medicalxpress.com/news/2019-01-world-zika-west-nile-dengue.html

Jan 04 – After collecting data and comparing it with every known mammal and bird species on Earth, scientists from the University of California, Davis, have identified wildlife species that are the most likely to host flaviviruses such as Zika, West Nile, dengue and yellow fever. Flaviviruses are known to cause major epidemics and widespread illness and death throughout the world.

The resulting "hot spot" maps show regions of the world with high diversity of potential wildlife hosts of flaviviruses—viruses mostly spread by mosquitoes and ticks. These include regions

where flaviviruses have not been detected but that have wildlife species with the potential to harbor them. The information provides scientists and health authorities with a road map for disease detection and surveillance efforts.

"Tomorrow, if there's an outbreak anywhere in the world, we now know which wildlife species are most likely to be infected in addition to humans," said lead author Pranav Pandit, a postdoctoral scholar with the UC Davis One Health Institute's EpiCenter for Disease Dynamics in the School of Veterinary Medicine.



This map, Fig. 4 in the study in *Nature Communications*, shows the geographical distribution of predicted flaviviral host richness. A) Yellow fever virus (YFV) and Zika virus (ZIKV). B) West Nile virus (WNV), St. Louis encephalitis virus (SLEV) and Usutu virus (USUV). C) Tickborne encephalitis virus (TBEV). D) Rio Bravo virus (RBV), Entebbe bat virus (ENTV) and Dakar bat virus (DBV). E) Dengue virus (DENV). F) Japanese encephalitis virus (JEV). Maps were generated using data from International Union for Conservation of Nature, BirdLife International and NatureServe. Credit: UC Davis

Predicting potential hosts

The findings are reported in a recent study published in the journal *Nature Communications*. Recently Zika virus emerged and continues to circulate in South America and Southeast Asia. The study predicts potential wildlife hosts in these regions with the ability to maintain Zika virus transmission in nature.

There is also rising concern that Japanese encephalitis virus will emerge and establish in Europe. The study identifies Europe as one of the regions with a high richness of potential Japanese encephalitis hosts, including many common bird species.
For the study, researchers collected all the published data on wildlife species that have tested positive for flaviviruses. They identified important host traits, such as environmental and physiological features. Then they used a machine-learning model that considered the roughly 10,400 avian and 5,400 mammal species in order to identify the most likely species to host viruses.
The model predicted hundreds of previously unobserved host species. For example, it predicted 173 host species for dengue virus, of which 139 have not been previously recognized.

Helping humans and other primates
Co-leading author and UC Davis professor Christine Kreuder Johnson said the modeling work can help researchers identify which primate species could be potential virus hosts. For example, the model indicated that primates are the main hosts of Zika and yellow fever, but only nine of the 21 primate species predicted to be hosts have been detected with either of those viruses due to limited surveillance activities among these species to date.
UC Davis One Health Institute scientists have established noninvasive sampling techniques for primates, such as collecting saliva from sticks and plants chewed by primates or from ropes coated with strawberry jam. But flaviviruses can be difficult to detect, especially in wildlife.
"We needed this modeling technique to help us understand the most likely hosts for these viruses in their natural habitat," said Johnson, director of the EpiCenter for Disease Dynamics. "That's important for both global health and wildlife conservation. Many of these primates are already endangered, and these diseases burden an already strained population."

Death in the Air: Revisiting the 2001 Anthrax Mailings and the Amerithrax Investigation

By Glenn Cross
Source: https://warontherocks.com/2019/01/death-in-the-air-revisiting-the-2001-anthrax-mailings-and-the-amerithrax-investigation/

Jan 16 – Time may have diminished the memory of the 2001 anthrax attacks and the sense of urgency surrounding the efforts to identify the attacker. The attacks, which involved ailings of five anthrax-laced letters to prominent senators and media outlets, killed five individuals and made 17 others ill. The anthrax mailings played a profound role in raising concerns over possible terrorist use of biological agents in attacks against the homeland. As a result of the anthrax scare, Americans' perceptions of terrorism came to include an existential fear of biological terrorism (aka "bio-doom"). Though this sense of dread has since diminished in the absence of another biological attack, it persists today because of the recent revolution in biotechnology: a revolution capable of resulting in enormous benefit for humanity as well as catastrophic dangers.
These concerns have fueled enormous growth in federal government spending on biodefense measures, and a cottage industry has arisen to lobby for further resources to combat the bioterror threat. Investments in biodefense have ranged from exponential spending increases and the expansion in the numbers of Bio-Safety Level 3 and 4 laboratories nationwide to the passage of the Bioshield Act in 2004 and the creation of the Biomedical Advanced Research and Development Authority and Federal Select Agent and Biowatch programs. However, as time passed without a biological attack, concerns about bioterror have diminished and biodefense has arguably become passé, its advocates shifting their attention to health security and pandemic preparedness.
The FBI's investigation into the 2001 mailings, labeled Amerithrax, remains a salient fixture on the post-9/11 landscape. Amerithrax was one of the largest and most complex in American history. It involved more

than 10,000 witness interviews worldwide, 80 separate searches, and the recovery of more than 6,000 items of potential evidence, including 5,730 environmental samples from 60 site locations. The lessons of the investigation are crucial to understanding not only the U.S. government's response to the first deadly bioterror attack on American soil, but also the role scientific evidence does — and does not — play in efforts to attribute bioterror attacks to an individual or group. Today, notwithstanding significant advances in bioforensics, the debates that continue to surround the Amerithrax investigation findings, the Syrian regime's chemical weapons attacks, or the Russian involvement in the Skripal poisonings are all examples of the doubts confronting even the most earnest attribution efforts.

Hurdles Facing Bioterrorism Attribution

The investigation ran from late 2001 through to its eventual closing in February 2010, nearly two years after its principal subject, Dr. Bruce Ivins, committed suicide. The investigation found that Ivins was responsible for mailing the anthrax-laced letters in 2001 based on a combination of factors, including motive, opportunity, history of mental health struggles, access to the anthrax spore source, proximity of the source to the envelopes used to mail the spores, and a consciousness of guilt.

One key lesson of Amerithrax was that the United States lacked the means for accurate attribution of bioterror attacks. Attribution of a biological attack is the result of a process that combines the results of traditional forensics (fingerprints, tool marks, fiber, trace element analysis, etc.), bioforensics (genomic signatures and analytical chemistry), and investigative techniques (interviews, polygraphs, surveillances, telephone taps, etc.), which are particularly relevant in cases involving foreign actors, intelligence methods (human intelligence and signal intelligence collection and analysis).

Bioforensics, as a component of attribution, was born out of the Amerithrax investigation. But bioforensics, also commonly referred to as microbial forensics, is only one element of attribution. Because of the "CSI effect" (i.e., a perception resulting from popular television crime shows that laboratory tests can decisively determine guilt), laboratory tests almost certainly have eclipsed other forms of evidence in their influence over juries. In reality, scientific results take a long time to bear fruit and often are not as unambiguous as portrayed in television fiction.

As the Amerithrax investigation began, microbial forensics was in its infancy, and the capabilities were rudimentary compared to current tools. As Dr. Vahid Majidi,

former Assistant Director of the FBI's WMD Directorate, pointed out in his self-published book on Amerithrax, the goal of the investigation was to meet the legal standards, not necessarily the higher standard of scientific proof. Scientific certainty would have been too time-consuming and expensive. The scientific goal of Amerithrax, to paraphrase Majidi, was the good-enough. Dr. Randy Murch, who was involved in establishing the FBI's microbial forensics efforts in 1996, stated that science will never get all the way to providing attribution, and that's the way it will always be. Microbial forensics can exclude some possible perpetrators and include a few.

Thus, for all the progress made in the life sciences since 1996, attribution efforts still have a long way to go. No one size fits all the possible universes of possible threat scenarios. Methods remain largely untested in terms of validation and legal acceptance in federal courts. Having not been tested it the courts, questions remain as to whether the methods would meet the Daubert standard, the rule of evidence governing the admissibility of expert witnesses' testimony in federal courts. Given that microbial forensics alone is unable to answer the attribution question, attribution must incorporate all the available tools. Majidi stressed that to assign attribution, it was prudent to look at the information from each element independently and, once all the information had been gathered, to bring together the most diagnostic information to arrive at a conclusion. In the end, any attribution effort will be complex, and the results almost certainly will be controversial.

A Useful Insider Account

Scott Decker's book on Amerithrax is the first and, so far, only insider account of the science involved in the investigation. Decker served as an FBI special agent, one of very few in the bureau with a PhD in the life sciences. His strong academic background and experience in the FBI's then-fledgling bioforensics effort ensured his rise to a prominent role in the Amerithrax investigation. In time, Decker became the supervisory special agent overseeing Amerithrax's Squad 2, which was responsible for the scientific and forensics work of the task force.

Thus, Decker is perhaps one of only a handful of people capable of providing comprehensive insight into the inner workings of Amerithrax's bioforensics effort. His book likely will be the only one to offer such a detailed and unique perspective into the U.S. government's response to the first deadly bioterrorism attack on American soil in peacetime.

(A disclaimer: For much of the time Amerithrax was active, I was working as a supervisor in the FBI's Weapons of Mass Destruction Directorate, an entity created after 9/11 to counter the threat from terrorist use of improvised nuclear weapons as well as biological and chemical agents. There I came to know many of the players in Decker's book, although my role was tangential to what came to be the major thrust of the investigation. I focused on supporting Amerithrax's effort to identify possible international terrorist involvement in the anthrax mailings. I did work with several of the investigation's special agents and knew of Decker and his work. I certainly cannot claim any insider insight into the scientific work or the efforts as they centered on Bruce Ivins.)

The book is Decker's first-person account of his role in the case. This perspective is both the book's major strength and its major weakness. Decker's focus was on developing and refining the scientific approach to the investigation, so he deftly weaves a compelling account of the scientific aspects of Amerithrax. At the same time, although he certainly was aware of other aspects of Amerithrax, Decker's book offers no insight into the efforts to examine possible international terrorist involvement in the mailings, an early concern that continued late into the case. I also take issue with Decker on several minor issues in the book, but these all fall into the category of nitpicking and in no way detract from the import of his work.

The Path to Bruce Ivins: An Inadvertent Discovery

Much of the book explores the groundbreaking genetics work that was crucial to identifying Ivins as the lead person of interest in the case. As Decker aptly describes, the bioforensics work of Amerithrax and its collaborators outside of government led to the development of new scientific capabilities of attribution of biological attacks. Yet the crucial scientific lead came by accident.

Relatively early in the investigation, a researcher unintentionally let cultures of the *B. anthracis* used in the mailings incubate longer than planned. These cultures exhibited several unusual physical characteristics (i.e., morphologies) pointing researchers to possible genetic mutations that could be used as identifying signatures.

A technician at the Army's biomedical research lab in Ft. Detrick, Md., opens an envelope containing anthrax. CreditFederal Bureau of Investigation, via Associated Press

Absent this accidental discovery and lacking today's sequencing power, Amerithrax might have been unable to home in on the unique signatures that led them to the RMR-1029 flask in Ivins' laboratory. Very early in the investigation, investigators learned that the spores in the letters belonged to the Ames strain of *B. anthracis*, yet early efforts to identify a unique genetic signature eluded them. The accidental discovery of the unique morphologies pointed to a way forward. By focusing on the genetic mutations responsible for the morphologies, researchers uncovered genetic signatures that linked the letter spores to spores originating from the RMR-1029 flask. Given his research at the U.S. Army Medical Research Institute of Infectious Diseases, Ivins had access to that flask. The envelopes used in the attacks also were sourced to several locations in or relatively near Ivins in Frederick, Maryland. But this scientific evidence did not point to Ivins alone. Others working in the same laboratory had access to the same flask, and Ivins had shared samples of spores from RMR-1029 with researchers at other laboratories.

The investigative focus on Ivins was based on both the science that narrowed the source of the *B. anthracis* in the mailings to that particular spore flask and on Ivins' own suspicious behaviors. Decker's book deftly describes the path that led investigators to RMR-1029. In parallel, he paints a compelling picture of Ivins' mental health demons. Investigators emphasized Ivins' "consciousness of guilt," a term of art describing behavior or actions of a guilty individual. In Ivins' case, the consciousness of guilt involved his deceit when questioned about several material facts related to the case, destruction of incriminating evidence, his deteriorating mental health, and ultimately his suicide. Supposedly Ivins perpetrated the attacks out of an anxiety that his supervisors planned to end Ivins' anthrax research and reassign him to work on another pathogen. According

to this explanation, Ivins mailed the letters to ensure anthrax research remained a priority at the U.S. Army Medical Research Institute. In the end, the weight of the evidence pointing to Ivins, as well as the scientific work that identified RMR-1029 as the parent source of the anthrax spores, compelled the Department of Justice to conclude Ivins was the sole perpetrator of the anthrax letter attacks.

Although many of Ivins' associates have told me that they cannot believe Ivins would have perpetrated the attacks, Decker makes a strong case for Ivins' role. His case is supported by the findings of the Expert Behavioral Analysis Panel and the Amerithrax Investigative Report. Still, Ivins' motive remains a matter of debate. Absent the investigation's identification of RMR-1029 as the source of the anthrax spores in the letters, one has to wonder whether Ivins' mental health would have ever become an issue. Ivins' case highlights the difficulty of attributing biological attacks, particularly the inadequacy of scientific evidence to, on its own, point to a perpetrator.

With the suicide of Bruce Ivins, the Amerithrax investigation closed and the scientific methods developed in the case were never tested or proven in court. Questions about the viability of the scientific findings remained. In response, the FBI requested the National Academies of Science's National Research Council independently review the bureau's scientific work as it related to Amerithrax. Highlighting the limitations of microbial forensics, the council concluded "it is not possible to reach a definitive conclusion about the origins of the *B. anthracis* in the mailings based on the available scientific evidence alone." Although the results of the FBI's microbial forensics were consistent with RMR-1029 or its descendants as the source material for the anthrax mailings, the science itself was not definitive and was insufficient to cast the shadow of guilt on Ivins.

How Far Have Attribution Efforts Come?

The ongoing revolution in biotechnology would have had a profound effect on Amerithrax had those capabilities been available back in 2002. If the investigation were to take place today, advances in genetic sequencing likely would mean that the case would not have rested on an accidental discovery of unique morphologies to point to signature mutations. The timeframe for the genomic analysis of Amerithrax's *B. anthracis* repository also would have been sped up significantly. Decker marvels at the tremendous advances in bioforensics given the exponential increase in sequencing speed and capacity along with a corresponding decrease in cost that took place during Amerithrax and in its aftermath. Decker stated that in 2002 he estimated that sequencing the 1981 Ames strain of *B. anthracis* would cost close to $500 million and that it would take six months to find an accurate genomic sequence. Today the cost has fallen to tens of thousands of dollars and the time required to complete the sequencing shortened to weeks rather than months.

However, even with the advances of the biotechnology revolution, it is unlikely that bioforensics today can, on its own, put a smoking gun in the hands of any one individual or group. Absent a claim of responsibility, reliable attribution of attacks — whether for use in a court case or to justify military or diplomatic responses to chemical or biological weapon use overseas — must combine sound science with investigative techniques and/or intelligence sources and methods. A 2018 exercise, CladeX, conducted by the Johns Hopkins University Center for Health Security, demonstrated the critical importance of a claim of responsibility for attribution and highlighted the lack of relevant scientific expertise in American investigative and intelligence agencies.

Given the serious consequences of error, decision-makers almost certainly will set a very high bar for attribution in terms of accuracy, reliability, and credibility. Ambiguities in interpreting scientific findings, as well as the limitations and nuances inherent in intelligence reporting, make it difficult for attribution efforts to meet that high bar. Faulty science combined with incomplete investigative work likely would result in a miscarriage of justice. Likewise, reliance on faulty science in the absence of solid intelligence about chemical or biological weapons use overseas would be disastrous diplomatically and militarily. Attribution, whether before a jury or before the court of international opinion, must be convincing and any action must be defensible.

Although advances in the life sciences are improving the tools available for bioforensics,

Amerithrax also demonstrates the limitations of such innovations. Admittedly, bioforensics was in its infancy at the outset of the investigation. A 2017 Government Accounting Office report cites experts as stating that bioforensics at the time of Amerithrax was incapable of detailed characterization and comparative analyses, and whether the scientific findings would have withstood critical scrutiny in the courts is uncertain. Decker points out the scientific challenges facing Amerithrax at its outset, admitting that his job would have been much easier had he possessed today's tools. He does not address what direction the case would have taken had the unique morphologies in the anthrax letter spores not been identified. Without that discovery of its link to RMR-1029, investigators may not have focused their attention on Ivins until much later, if ever. In that alternate universe, Amerithrax could have plausibly remained centered on its initial person of interest without ever casting serious suspicion on Ivins.

Neither a sterile official history nor a journalistic exercise, Decker's book fills the gap in the history of the Amerithrax investigation. His book is an exemplary insider account of one of the most challenging investigations ever conducted by the FBI, and it raises important questions about the proper place of science in criminal probes. Decker's story is all the more important given that few, if any, retellings are likely to come forth from individuals with his level of access and dedication to the truth.

***Dr. Glenn Cross** currently works for the Federal Bureau of Investigation and is a former deputy national intelligence officer for weapons of mass destruction, specializing in biological weapons. He also is the author of "Dirty War: Rhodesia and Chemical Biological Warfare, 1975 to 1980."*

North Korea's Less-Known Military Threat: Biological Weapons

By William J. Broad

Source: https://www.nytimes.com/2019/01/15/science/north-korea-biological-weapons.html

Jan 15 — Pound for pound, the deadliest arms of all time are not nuclear but biological. A single gallon of anthrax, if suitably distributed, could end human life on Earth.

Even so, the Trump administration has given scant attention to North Korea's pursuit of living weapons — a threat that analysts describe as more immediate than its nuclear arms, which Pyongyang and Washington have been discussing for more than six months.

According to an analysis issued by the Middlebury Institute of International Studies at Monterey last month, North Korea is collaborating with foreign researchers to learn biotechnology skills and build machinery. As a result, the country's capabilities are increasing rapidly.

"North Korea is far more likely to use biological weapons than nuclear ones," said Andrew C. Weber, a Pentagon official in charge of nuclear, chemical and biological defense programs under President Obama. "The program is advanced, underestimated and highly lethal."

The North may want to threaten a devastating germ counterattack as a way of warding off aggressors. If so, its bioweapons would act as a potent deterrent.

But experts also worry about offensive strikes and agents of unusual lethality, especially the smallpox virus, which spreads person-to-person and kills a third of its victims. Experts have long suspected that the North harbors the germ, which in 1980 was declared eradicated from human populations.

Worse, analysts say, satellite images and internet scrutiny of the North suggest that Pyongyang is newly interested in biotechnology and germ advances. In 2015, state media showed Kim Jong-un, the nation's leader, touring a biological plant, echoing his nuclear propaganda.

But compared to traditional weapons, biological threats have a host of unsettling distinctions: Germ production is small-scale and far less expensive than creating nuclear arms. Deadly

microbes can look like harmless components of vaccine and agricultural work. And living weapons are hard to detect, trace and contain.

The North's great secrecy makes it hard to assess the threat and the country's degree of sophistication. Today, the North might well have no bioweapons at all — just research, prototypes, human testing, and the ability to rush into industrial production.

Still, Anthony H. Cordesman, a former Pentagon intelligence official now at the Center for Strategic and International Studies, said the North "has made major strides" in all technical areas needed for the production of a major germ arsenal.

In unclassified reports, the Trump administration has alluded to the North's bioweapons program in vague terms. President Trump did not broach the subject of biological weapons during his meeting with Mr. Kim in Singapore, according to American officials.

The lack of detail and urgency is all the more surprising given that John R. Bolton, Mr. Trump's national security adviser, has long described it as a regional and even a global threat.

In 2002, as under secretary of state for arms control and international security in the George W. Bush administration, Mr. Bolton declared that "North Korea has one of the most robust offensive bioweapons programs on Earth."

Last century, most nations that made biological arms gave them up as impractical. Capricious winds could carry deadly agents back on users, infecting troops and citizens. The United States renounced its arsenal in 1969.

But today, analysts say, the gene revolution could be making germ weapons more attractive. They see the possibility of designer pathogens that spread faster, infect more people, resist treatment, and offer better targeting and containment. If so, North Korea may be in the forefront.

South Korean military white papers have identified at least ten facilities in the North that could be involved in the research and production of more than a dozen biological agents, including those that cause the plague and hemorrhagic fevers.

United States intelligence officials have not publicly endorsed those findings. But many experts say the technological hurdles to such advances have collapsed. The North, for instance, has received advanced microbiology training from institutions in Asia and Europe.

Bruce Bennett, a defense researcher at the RAND Corporation, said defectors from the North have described witnessing the testing of biological agents on political prisoners.

Several North Korean military defectors have tested positive for smallpox antibodies, suggesting they were either exposed to the deadly virus or vaccinated against it, according to a report by Harvard Kennedy School's Belfer Center for Science and International Affairs.

Smallpox claimed up to a half billion lives before it was declared eradicated. Today, few populations are vaccinated against the defunct virus.

Starting three years ago, Amplyfi, a strategic intelligence firm, detected a dramatic increase in North Korean web searches for "antibiotic resistance," "microbial dark matter," "cas protein" and similar esoteric terms, hinting at a growing interest in advanced gene and germ research.

According to the Middlebury Institute analysis, at least 100 research publications that were jointly written by North Korean and foreign scientists have implications for military purposes, such as developing weapons of mass destruction. The collaborations may violate international sanctions.

Joseph S. Bermudez, Jr., a North Korean military analyst, said it is entirely likely that the North has already experimented with gene editing that could enhance bacteria and viruses.

"These are scientists, and scientists love to tinker," he said.

Western concerns about the North's program jumped in June 2015, after Mr. Kim posed in a white lab coat alongside military officers and scientists in a modern-looking pesticide facility called the Bio-Technical Institute, his arms outspread toward shiny lab equipment.

The plant allegedly produced pesticides. The photos showed enormous fermenters for growing microbes, as well as spray dryers that can turn bacterial spores into a powder fine enough to be inhaled. Mr. Kim was beaming.

Melissa Hanham, a scholar who first identified the site's threatening potential, said equipment model numbers showed that the North had obtained the machinery by evading sanctions — laundering money, creating front companies or bribing people to buy it on the black market.
She said the evidence suggests the North succeeded in building a seemingly harmless agricultural plant that could be repurposed within weeks to produce dried anthrax spores.
Arms-control analysts say intrusive inspections are needed to see whether a facility is intended for peaceful aims or something else.
"A nuclear weapons facility has very visible signals to the outside world," Mr. Bermudez said. "We can look at it and immediately say, 'Ugh, that's a nuclear reactor.' But the technology for conducting biological weapons research is essentially the same as what keeps a population healthy."
Americans felt the sting of bioweapons in 2001 when a teaspoon of anthrax powder, dispatched in a handful of envelopes, killed five people, sickened 17 more and set off a nationwide panic. The spores shut down Congressional offices, the Supreme Court and much of the postal system, and cost about $320 million to clean up.
Federal budgets for biodefense soared after the attacks but have declined in recent years.
"The level of resources going against this is pitiful," said Mr. Weber, the former Pentagon official. "We are back into complacency."
Dr. Robert Kadlec, the assistant secretary for preparedness and response at the Department of Health and Human Services, said, "We don't spend half of an aircraft carrier on our preparedness for deliberate or natural events."
The National Security Council's top health security position was eliminated last year, so biological threats now come under the more general heading of weapons of mass destruction.
Still, on the Korean Peninsula, troops gird for a North Korean attack. According to the Belfer report, American forces in Korea since 2004 have been vaccinated against smallpox and anthrax.
Recently, Army engineers sped up the detection of biological agents from days to hours through Project Jupitr, or the Joint United States Forces Korea Portal and Integrated Threat Recognition, a Department of Defense spokeswoman said.
The comptroller general of the United States, after a request from the House Armed Services Committee, is currently conducting an evaluation of military preparedness for germ attacks.
"If you're a country that feels generally outclassed in conventional weapons," Ms. Hanham said, a lethal microbe such as anthrax might seem like a good way "to create an outsized amount of damage."
Such an attack would maximize casualties, she said, while terrorizing the uninfected population. For North Korea, Ms. Hanham added, "That would be the twofold goal."

***William J. Broad** is a science journalist and senior writer. He joined The Times in 1983, and has shared two Pulitzer Prizes with his colleagues, as well as an Emmy Award and a DuPont Award.*

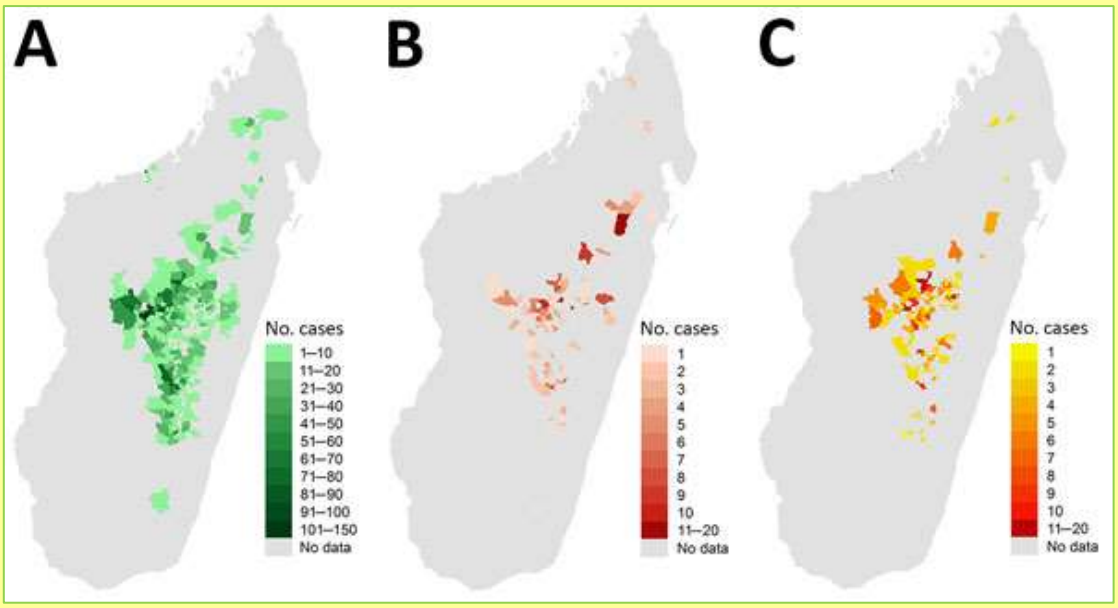
Trends of Human Plague, Madagascar, 1998–2016

Emerging Infectious Diseases. Volume 25, Number 2—February 2019
By Voahangy Andrianaivoarimanana, Patrice Piola, David M. Wagner, et al.
Source: https://wwwnc.cdc.gov/eid/article/25/2/17-1974_article

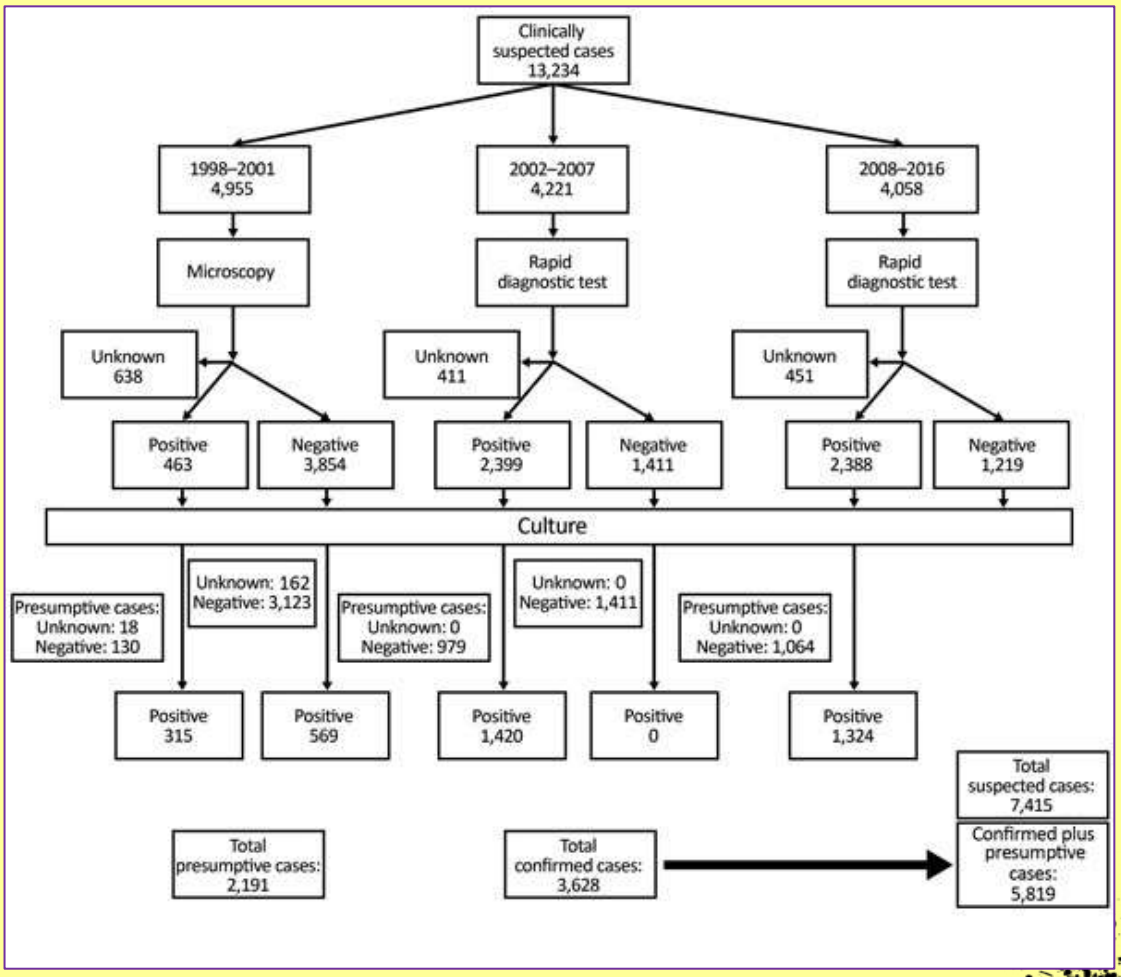
Abstract

Madagascar is more seriously affected by plague, a zoonosis caused by *Yersinia pestis*, than any other country. The Plague National Control Program was established in 1993 and includes human surveillance. During 1998–2016, a total of 13,234 suspected cases were recorded, mainly from the central highlands; 27% were confirmed cases, and 17% were presumptive cases. Patients with bubonic plague (median age 13 years) represented 93% of confirmed and presumptive cases, and patients with pneumonic plague (median age 29 years) represented 7%. Deaths were associated with delay of consultation, pneumonic form, contact with other cases,

occurrence after 2009, and not reporting dead rats. A seasonal pattern was observed with recrudescence during September–March. Annual cases peaked in 2004 and decreased to the lowest incidence in 2016.



Geographic distributions of bubonic plague (A), pneumonic plague (B), and infection clusters (C), Madagascar, 1998–2016.



Diagnostic flowchart for suspected cases of plague, Madagascar, 1998–2016.

This overall reduction occurred primarily for suspected cases and might be caused by improved adherence to case criteria during widespread implementation of the F1 rapid diagnostic test in 2002.

Producing vaccines without the use of chemicals

Source: http://www.homelandsecuritynewswire.com/dr20190116-producing-vaccines-without-the-use-of-chemicals

Jan 16 – Vaccinations against polio, diphtheria, whooping cough and tetanus have been on the list of standard infant vaccinations for decades now. Many vaccines are inactivated vaccines - that is to say, the pathogens they contain have been killed so that they can no longer harm the patient. Despite this, the vaccine provokes an immune response: The body detects a foreign intruder and begins to produce antibodies to ward off infection.

To produce these vaccines, pathogens are cultivated in large quantities and then killed using toxic chemicals. The most common of these is formaldehyde - heavily diluted so it doesn't harm the patient when the vaccination is administered. Nevertheless, there are downsides to even this minimal concentration: The toxin must remain in contact with the pathogen for days or even weeks to take effect, which has a negative impact both on the structure of the pathogen and the reproducibility of the vaccine. And in cases that call for speed – flu vaccines for instance – drug manufacturers are obliged to use higher dosages of formaldehyde. The product must then undergo a time-consuming process of filtration to avoid traces of the toxic chemical being left behind in the vaccine.

Electron beams kill harmful pathogens

Fraunhofer says that now, pharmaceutical companies will be able to produce inactivated vaccines without the slightest trace of toxic chemicals – quickly and reproducibly. The scientists who developed this process see its greatest potential in the production of vaccines that until now were not amenable to the method of chemical inactivation. The technique was developed jointly by researchers at the Fraunhofer Institutes for Cell Therapy and Immunology IZI, Manufacturing Engineering and Automation IPA, Organic Electronics, Electron Beam and Plasma Technology FEP and Interfacial Engineering and Biotechnology IGB. **"Instead of using chemicals to inactivate the pathogens, we employ low-energy electron beams"** explains Fraunhofer IPA team leader Martin Thoma. The accelerated electrons break down the DNA of the pathogens either via direct collisions or through the generation of secondary electrons, which subsequently result in single or double strand breaks. In a nutshell, the electrons fragment the pathogens' DNA while maintaining their external structure. This is important to trigger an effective immune response.

The challenge arises from the fact that the electrons cannot penetrate very deeply into the suspension containing the pathogens - in fact, for an even dose distribution, liquid levels should not exceed 200 micrometers. Because there were no existing technologies capable of meeting these requirements, Fraunhofer IPA developed two new methods from scratch. In the **first method,** a cylinder is continuously wetted with the pathogen suspension, irradiated, and the inactivated liquid transferred into a sterile vessel. In other words, there are two reservoirs of liquid: one containing the active and one containing the inactive pathogens - connected to one another via a constantly turning cylindrical vessel or tumbler. "It's a continuous process that can easily be scaled up for the mass production of vaccines," says Thoma. The **second method** is more suited to lab-scale applications, in which small quantities of vaccine are produced for research or drug development purposes. In this instance, the solution containing the pathogens is placed in bags, which are then passed through the electron beam using a patented process.

A collaborative undertaking

This kind of project calls for a range of expertise that is perfectly covered by the four Fraunhofer Institutes involved in the initiative. Researchers at Fraunhofer IZI took responsibility

for cultivating the various pathogens – including one for avian flu and one for equine influenza. "Following the irradiation, we also worked with our colleagues at Fraunhofer IGB to determine whether the pathogens had been fully inactivated, thus providing effective vaccine protection," says Dr. Sebastian Ulbert, head of department at Fraunhofer IZI and the initiator of the project. The expertise in electron beam technology came from researchers at Fraunhofer FEP, who developed a system capable of delivering the low-energy electron beams at precise doses – this is necessary because, while the aim is to reliably inactivate the pathogen, care must also be taken to preserve the pathogen structure so that patients' immune systems can produce the corresponding antibodies.

The new technology has already been implemented, and not only on the laboratory scale: "In the fall of 2018, a research and pilot facility entered into service here at Fraunhofer IZI. Using our continuous module – the wetted tumbler – we are currently able to produce **four liters of vaccine per hour,**" says Ulbert. That is not far off industrial scale, given that, for certain vaccines, **15 liters of pathogen suspension can yield a million doses of vaccine.**

Discussions are already underway with partners in industry. However, it will be another two to four years before vaccines produced using electron beams can be tested in clinical trials.

Potential biotech and health applications with new knowledge on bacteria and viruses

Source: https://www.sciencedaily.com/releases/2019/01/190118095941.htm

Jan 18 – University of Otago research to better understand how bacteria and their viruses interact and evolve will enable future studies to exploit the use of bacteria and their viruses for potential biotechnology and health applications.

Research led by Dr Simon Jackson and Associate Professor Peter Fineran, from the Department of Microbiology and Immunology, investigating the function of bacteria immune systems and what impact they have on the coevolution of bacteria and viruses was published today in a top tier scientific journal, *Cell Host and Microbe*.

Viruses infecting bacteria are called bacteriophages ("phages" for short) and are the most abundant biological entities on the planet influencing many aspects of our lives and the global ecosystem.

Dr Jackson says the war between phages and bacteria is ever-present and many bacteria protect themselves using immune defences known as CRISPR-Cas systems.

"Research to understand more about the interactions between phages and bacteria, particularly how bacterial CRISPR-Cas immunity functions, is being exploited internationally in many ground-breaking biotechnological applications including gene editing," Dr Jackson explains.

"We think this area of research holds a lot of promise for biotechnology applications and might also be an important consideration for the use of phages to treat infectious diseases.

"For example, because phages kill specific bacteria, they can be used as alternatives to antibiotics to treat some infectious diseases and can even kill antibiotic resistant bacteria."

Bacterial adaptive immunity is similar in concept to human adaptive immunity. Bacteria must first become "vaccinated" against specific phages, which involves the bacteria storing a short snippet of viral DNA, termed a "spacer," used to recognise and defend against future infections.

In a previous study examining how CRISPR-Cas systems acquire spacers, the Otago research team found that often bacteria acquire "incorrect" spacers, known as "slipped spacers." At the time, they did not know whether the incorrect or imprecise slipped spacers were functional.

Associate Professor Fineran, a molecular microbiologist, says their initial observations were surprising and showed these slipped spacers were very efficient at boosting bacterial immunity by stimulating bacteria to acquire extra spacers targeting the same phage. This unexpected role

increases immune diversity, which is important for bacteria to protect against the rapidly evolving phages.
"Several groups had previously identified the occurrence of imprecisely acquired or slipped spacers.
However, no-one had previously considered whether they were functional or what impact they might have on immunity," Associate Professor Fineran explains.
"By showing they are functional and can provide benefit to bacteria, we have revealed an unexpected complexity to the evolutionary battle between bacteria and phages."
If in the future, researchers can determine how immunity is first gained, they may be able to either prevent or promote it for different applications, Associate Professor Fineran says.
"For example, in the dairy industry for the production of cheese and yoghurt it is beneficial for bacteria to have resistance against phages, whereas if phages are used as antimicrobials, emergence of immunity would be undesirable -- akin to antibiotic resistance."

Journal Reference

Simon A. Jackson, Nils Birkholz, Lucía M. Malone, Peter C. Fineran. ***Imprecise Spacer Acquisition Generates CRISPR-Cas Immune Diversity through Primed Adaptation***. Cell Host & Microbe, *2019; DOI: 10.1016/j.chom.2018.12.014*

In Congo, fighting a virus and a groundswell of fake news

By Laura Spinney

Science 18 Jan 2019: Vol. 363, Issue 6424, pp. 213-214. DOI: 10.1126/science.363.6424.213
Source: http://science.sciencemag.org/content/363/6424/213

Occurring in a conflict zone amid controversial presidential elections, the current Ebola epidemic in the Democratic Republic of the Congo (DRC) has proved to be fertile ground for conspiracy theories and political manipulation, which can hamper efforts to treat patients and fight the virus's spread. Public health workers have mounted an unprecedented effort to counter false rumors. For the first time in an Ebola outbreak, the United Nations International Children's Emergency Fund and other agencies have joined forces in a single response team, which answers to the DRC's Ministry of Health and includes dozens of social scientists. They use the airwaves, social media, and meetings with community and religious leaders to fight misinformation.

Laura Spinney *is a journalist based in Paris.*

New Hope with Ebola Drug Trial as Entebbe Airport Steps Up Screening

By Kylie Bull

Source: https://www.hstoday.us/public-health/new-hope-with-ebola-drug-trial-as-entebbe-airport-steps-up-screening/

Jan 15 – Since the start of the Ebola current outbreak in the Democratic Republic of the Congo (DRC) in August 2018, patients have had access to one of four investigational treatments on a compassionate basis. These drugs: **mAb 114, Remdesivir, Zmapp and REGN-EB3** were offered under an ethical framework developed by the World Health Organization (WHO) known as the Monitored Emergency Use of Unregistered Interventions (MEURI) protocol.

By 1 January, 248 patients had received one of these four drugs. While some patients seemed to improve, there was no scientific evaluation of the efficacy and safety of these drugs.
On 24 November, the DRC's Ministry of Public Health announced the start of a randomized control trial. WHO is coordinating the trial which is led and funded by the DRC's Institut National de Recherche Biomédicale (INRB)

and the National Institutes of Health, a part of the US Department of Health and Human Services. Other partners are Médecins Sans Frontières (MSF) and ALIMA.

"This is the first multi-drug trial for Ebola treatments, and the rigorous collection and analysis of data is expected to deliver clarity about which drug works best," says Dr Janet Diaz, WHO's team lead for clinical management of emerging infectious diseases and, in this current outbreak, the team lead for care of patients with Ebola. "This will ultimately save lives in future outbreaks – either in the DRC or in other countries."

For now, mAb 114 and Remdesivir are being evaluated against Zmapp, the control arm. REGN-EB3 will be added to the trial in due course. Optimal supportive care is also provided to all patients.

Mr Kambale was one of the first patients to be admitted to the trial. Fading fast, he was admitted to the Ebola Treatment Centre (ETC) by the doctors from ALIMA, the health NGO that runs the facility. After the medical staff explained to him the details of the trial, they asked if he would be willing to participate and he was quick to give his consent.

In the week since falling ill, he'd initially been misdiagnosed with malaria and typhoid, and then a traditional healer told him he'd been poisoned. The fourth health worker he consulted took one look at him and told him to go straight to the ETC.

"I didn't want to go," says Mr Kambale, 30, a secondary school mathematics teacher. "But I had no fight left in me."

He spent the night at the MSF-run transit facility, where patients stay until Ebola is confirmed or ruled out. The following afternoon he got back his result: he tested positive for Ebola.

There is no cure for Ebola and the mortality rate in this outbreak is about 60%. However, there is new cause for hope thanks to the new treatments.

"Our objective now is to discover among these treatments which is the most effective," says Dr Camara Alseny Modet, the ALIMA doctor who was in charge of running the Beni ETC and is now a trial coordinator. As of January 6, 44 patients have been enrolled in the trial at the Beni ETC. Patients at other ETCs, for example in Butembo, will soon also have the opportunity to be part of the trial.

It is unlikely that the study will reach its target enrolment number of 336 patients during this outbreak. So, under the protocol, the trial is permitted to cover multiple outbreaks in multiple countries over a period of five years.

When a patient consent to be part of the trial, the pharmacy team at the Beni ETC selects a sealed envelope telling them which drug to administer. In this way the trial is randomized.

While the trial is important, health workers nevertheless remain clear that their top priority in this outbreak is looking after sick patients and ensuring they have the best care possible.

Running a clinical trial is a complex business at the best of times. But in Beni it is being conducted during an emergency in an active conflict zone where elections are also taking place.

"Security is a big challenge," says Prof Sabue Mulangu, Ebola research coordinator at the INRB. "Sometimes we have to stop our work early because security is not good and staff have to respect curfews. We really try to minimize this but it's not easy, I can tell you."

There was a happy ending for Mr Kambale. Having come through Ebola, and well on his way to recovery, he has only good words for his doctors, praising their dedication in caring for him and their courage. As his condition improved, he was moved from intensive care to the convalescence ward. After five days there he was given the all-clear and allowed to go home.

Now he is back in the ETC – this time helping to care for other sick patients.

"People in this community helped me and now it's my turn to give back," he explains. "This is not one person's story, it affects us all. Those who don't believe that Ebola exists are mistaken."

He reflects that it's not easy being part of this trial because Ebola is not a disease that anyone would want to catch – but he is also able to strike a note of optimism.

"Maybe in this way, I can convince other people in my town that there is a treatment available for Ebola and that they can get better. And if

they feel ill, the should go straight to the ETC."
As of January 12, there were 595 confirmed and 49 probable cases of Ebola, and 343 deaths had been confirmed. Airport authorities in Uganda have been screening passengers returning on flights from DRC since the severity of the latest outbreak was known. Now, WHO has ordered the mandatory Ebola screening of all passengers entering Uganda through Entebbe International Airport.
As part of the new measures, more than 40 health workers are now located at Entebbe International where all passengers are now screened using an automatic thermal stand. An isolation center at Entebbe hospital is on stand-by to accommodate any passengers that the scanner flags up.

While the latest outbreak is a cause for concern, lessons learned from previous years have helped to increase health security in neighbouring countries and regions, as well as improve and fine-tune the treatments available.

__Kylie Bull__ has 20 years' experience in reporting and editing a wide range of security topics, covering geopolitical and policy analysis to international and country-specific trends and events. She is an editor and contributor for Jane's by IHS Markit, a columnist for security and counter-terror publications, and a former managing editor for Homeland Security Today.

Ebola epidemiological situation report, DRC Ministry of Health

Source: https://us13.campaign-archive.com/?u=89e5755d2cca4840b1af93176&id=2b3d226b45

Jan 19 – Since the beginning of the epidemic, the cumulative number of cases is 685, of which 636 are confirmed and 49 are probable. In total, there were 416 deaths (367 confirmed and 49 probable) and 244 people cured.

- 142 suspected cases under investigation.
- 5 new confirmed cases, including 4 in Katwa and 1 in Beni. The case of Beni is the 19-day-old baby of the confirmed case reported in the bulletin of 18 Jan 2019.
- 2 new deaths of confirmed cases (all community deaths) in Katwa.
- 1 new person healed out of Butembo CTE

How significant is the North Korea germ warfare threat?

Source: https://www.theweek.co.uk/99088/how-significant-is-the-north-korea-germ-warfare-threat

Jan 21 – **North Korea's biological warfare capabilities pose a more serious military threat than its nuclear programme,** according to defence analysts in Washington and Seoul.
A study conducted by California's Middlebury Institute of International Studies in December concluded that North Korea "is accessing the work of foreign researchers to develop its existing biotechnology skills and construct the equipment to produce more biological weapons", The New York Times reports.
The analysis suggests that at least 100 research papers jointly published by North Korean and foreign scientists "have implications for military purposes, such as developing weapons of mass destruction".
"We are definitely underinvested in countering North Korea's chemical and biological threats," Andrew Weber, a former head of the Pentagon's chemical-biological defence programmes, told the newspaper.
US capabilities are improving, but "we are playing catch-up, especially on the biological side", he added.
The potential for attack with viruses and bacteria "underlines the complexity of disarming the North Korean regime as President Trump gears up for a second summit with Kim Jong Un", says London's The Times.

What is in North Korea's arsenal?
The North's "great secrecy makes it hard to assess the threat and the country's degree of sophistication", says The New York Times. Today, it "might well have no bioweapons at all - just research, prototypes, human testing, and the ability to rush into industrial production", the paper adds.

However, Pyongyang is **believed to possess at least 13 different biological warfare agents** that could potentially be weaponised, including anthrax, smallpox, botulism, cholera, hemorrhagic fever, plague, typhoid and yellow fever, US officials told Capitol Hill news site Roll Call last June.
If Kim "were to unleash his suspected stockpile of smallpox, to name just one biological agent believed to be in his possession, it could bring back to the world perhaps the deadliest scourge in human history", according to the Washington DC-based news site.
In its latest assessment of Pyongyang's military capabilities, the South Korean Ministry of National Defence stated that the North "is **believed to have produced and stockpiled as much as 5,000 tonnes of chemical weapons and has the ability to produce a further 2,000 tonnes a year**", reports The Daily Telegraph.

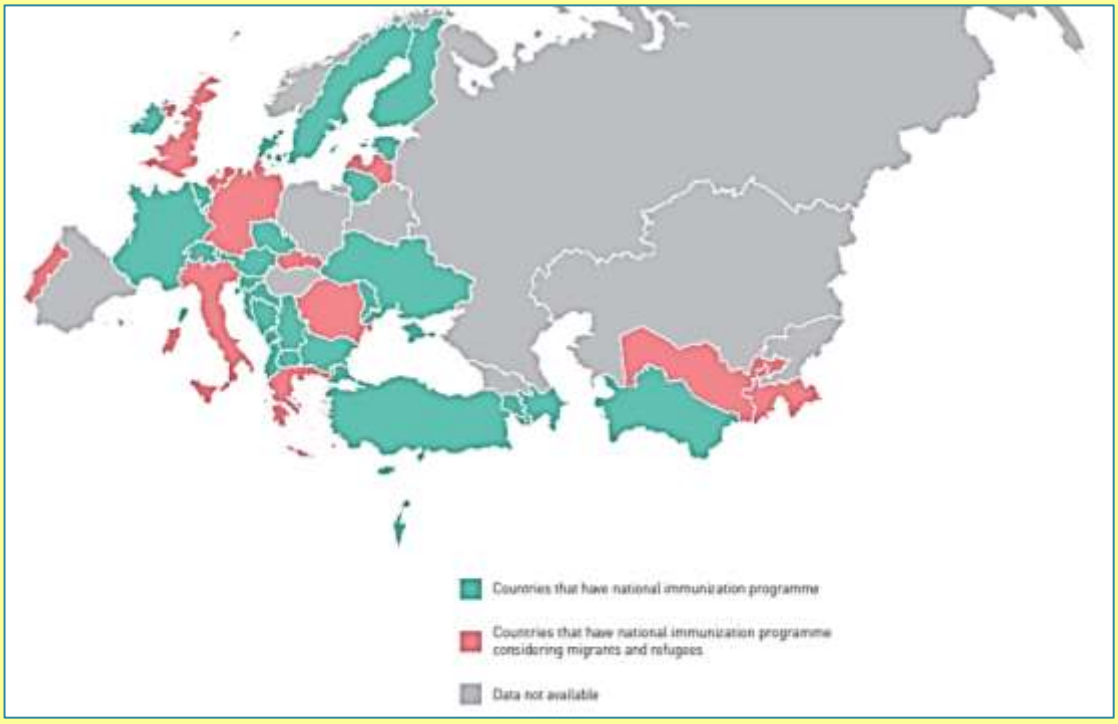
How likely is a biological weapons attack?
Analysts claim the threat of a "devastating germ counterattack" is designed to "deter the North's enemies, although biological agents can also be used as offensive weapons", says the Telegraph.
"North Korea is far more likely to use biological weapons than nuclear ones. The programme is advanced, underestimated and highly lethal," Weber told The New York Times.
The reasons are manifold. The North Korean military "views chem-bio agents as regular weapons of war, not as arms that are beyond the pale", Roll Call says.
In addition, the North Koreans may believe that the US "would see a biological as less severe than a nuclear one and therefore less likely to trigger an all-out US military response", the site adds.

WHO: Migrants do not bring diseases into Europe

Source: http://www.homelandsecuritynewswire.com/dr20190122-who-migrants-do-not-bring-diseases-into-europe

Jan 22 – A new report by the World Health Organization disputes a belief that refugees and migrants bring exotic communicable diseases into the European region.
The report is based on evidence from more than 13,000 documents. It provides a snapshot of the health of refugees and migrants who comprise about 10 percent of the nearly 1 billion population in 53 European countries.

The survey finds migrants and refugees are generally in good health, but, due to poor living conditions, they risk falling ill while in transit or while staying in receiving countries. The report says contrary to common perception, the risk of refugees and migrants transmitting communicable diseases to their host population is very low.
The WHO regional director for Europe, Zsuzsanna Jakab, tells VOA displacement itself makes refugees and migrants more vulnerable to infectious diseases.
"The refugees and migrants who come to Europe, they do not bring any exotic diseases with them, any exotic communicable diseases," said Jakab. "The diseases that they might have, they are all well-established diseases in Europe. And also, we have very good prevention and control programs for these diseases. This applies both for tuberculosis, but also HIV-AIDS."
Europe is the only one among WHO's six regions where HIV is prevalent and increasing, especially in the east. Jakab says a significant proportion of migrants and refugees who are HIV-positive acquire the infection after they arrive in Europe.
The report finds refugees and migrants seem to have fewer noncommunicable diseases on arrival than their host populations; but, it notes the longer they stay in the countries in conditions of poverty, their risk of cardiovascular diseases, stroke and cancer increases.



The report says refugees and migrants are more affected by depression and anxiety than host populations. It says unaccompanied minors are vulnerable to sexual exploitation and suffer from higher rates of depression and symptoms of post-traumatic stress disorder.

WHO considers it critically important that European countries provide quality and affordable health care for all refugees and migrants, regardless of their legal status. Providing universal health coverage, it says, would significantly improve the well-being of both the displaced and host populations.