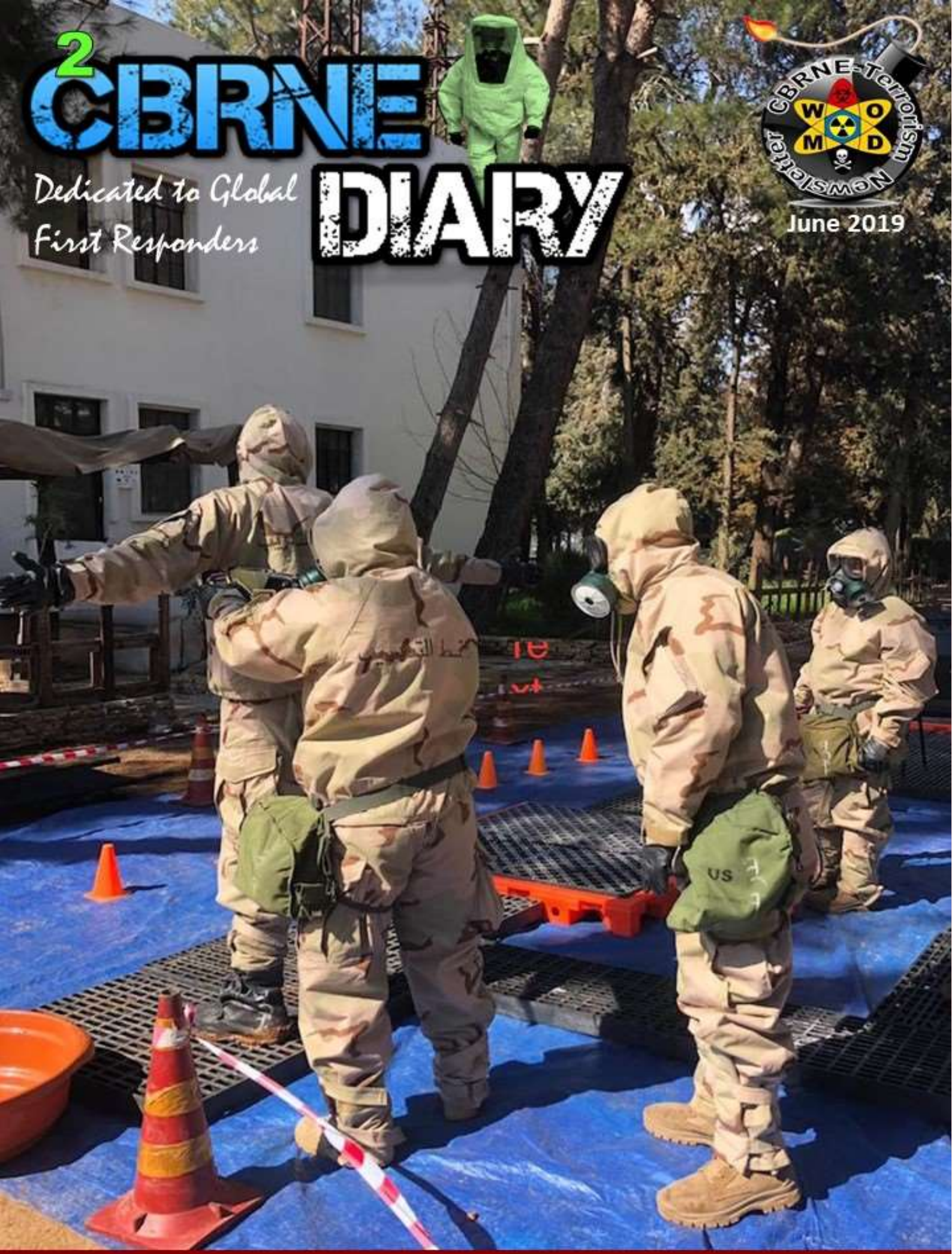
2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

June 2019



www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

DIRTY R-NEWS

Former IAEA Official Believes Iran Might Get Nuclear Weapon in 6-8 Months

Source: https://jewishjournal.com/news/world/299626/former-iaea-official-believes-iran-might-get-nuclear-weapon-in-6-8-months/

June 05 – Former International Atomic Energy Agency (IAEA) Deputy Olli Heinonen told Israeli Army Radio on Wednesday that Iran could develop nuclear weapons as soon as six-to-eight months, the Times of Israel reports.

Heinonen, a fellow at the Foundation of Defense Democracies think-tank, argued that Iran hadn't been following to its end of the bargain in the 2015 Iran nuclear deal because they have been "actually weaponizing uranium enrichment without making a weapon."

However, Heinonen criticized President Donald Trump's decision to exit from the Iran nuclear deal in May 2018, arguing that Iran could "withstand a lot of sanctions" while ramping up its enrichment.

Heinonen's prediction comes after the Jerusalem Post reported on June 4 that two German state intelligence agencies concluded that Iran has been making efforts to illicitly obtain weapons of mass destruction.

Before Trump announced the United States' exit from the Iran deal, Israeli Prime Minister Benjamin Netanyahu revealed in a televised announcement that Iran had been concealing nuclear facilities from the IAEA. Iran's Atomic Energy Organization head Ali Akbar Salehi admitted to Iranian television in January that Iran pretended to close its Arak reactor as stipulated under the deal, but kept the reactor operational in secret.

Trump told Britain's ITV channel on Wednesday that "there's always a chance" that war with Iran could happen, but he prefers to hold a dialogue with the regime instead. However, Iranian Supreme Leader Ayatollah Ali Khamenei said in a June 4 speech in Tehran that the regime is not interested in negotiating with the Trump administration.

"They want us to be losers and put our hands up as a sign of surrender, and because we don't do that, they threaten us," Khamenei said. "Resistance has a cost, but the cost of surrendering to the enemy is higher."

Recently declassified U.S. intelligence reportedly determined that Iranian terror proxies like Hamas and Hezbollah have seen a shortfall in funding from Tehran due to the re-imposition of U.S. sanctions.

America Never Had a Chernobyl. But It Came Close.

Source: https://www.popularmechanics.com/military/weapons/a27729387/chernobyl-broken-arrows/

June 05 – HBO's *Chernobyl* is over, but if you've seen the series, you'll remember it for a long time.

Coming on the heels of the mega-hyped *Game of Thrones* series finale, the five-part miniseries—created and written by Craig Mazin, and directed by Johan Renck—quickly overtook the fantasy story with its astonishing performances and commitment to its immersion in a world that Americans never really understood.

The focus in the discussion around *Chernobyl* lies where the miniseries has gone: nuclear reactors meant for peaceful energy. The safety of nuclear plants is of upmost importance, but that's not the only place nuclear energy is located. According to the *Bulletin of Atomic Scientists*, the Department of Defense maintains an estimated stockpile of approximately 4,000 warheads. Mishaps with these weapons of mass destruction are referred to as "Broken Arrow" accidents.

The United States has officially had approximately 32 of these incidents, often involving the transport of weapons from one location to another. None of these incidents caused a major disaster, let

alone a Chernobyl-like event. Two nuclear weapons were dropped on Goldsboro North Carolina in 1961 and are now commemorated with an historical marker. But there's no such memorial for the 1980 accident in which a Titan II missile carrying a thermonuclear reactor exploded near Damascus, Arkansas.

Chernobyl offers a new chance to examine these Broken Arrows. Fortunately, both the stories of Goldsboro, the Damascus Incident, and other Broken Arrows have already been documented in the film *Command and Control*, directed by Robert Kenner and based on a book by Eric Schlosser.

Available on PBS, Netflix, and other streaming services, the documentary shows that the story of lies and of nuclear mismanagement is not limited to Soviet borders.

On September 18, 1980, routine maintenance on an Titan II went awry. A Propellant Transfer System (PTS) team was working on the missile under the authority of the Air Force. A ratchet was used instead of a torque wrench, and that was all it took for a socket from the missile's oxidizer tank to fall 80 feet down, where a freak bump allowed it to puncture the missile's first-stage fuel tank.

Efforts to stabilize the missile failed, and late into the night, it exploded. Two men sent in to vent the gas were presumed dead. One of them, Senior Airman David Livingston, died 12 hours later. The nuclear warhead was later found in a field.

Who Saved Europe? The Three Unsung Heroes of Chernobyl
From the right - Alexei Ananenko and Valeri Bezpalov
https://www.chernobylwel.com/blog-detail/113/who-saved-europe-the-three-unsung-heroes-of-chernobyl

There are many differences between Damascus and Chernobyl, of course. Honesty was maintained within the chain of command, although the man who dropped the socket had trouble articulating the truth of the situation for half an hour afterward. And while safety protocols couldn't keep the 7-story missile from exploding, they did keep the warhead in check.

But when it comes to nuclear incidents, *Command and Control* makes it clear that the U.S. shares more with the scientists of Chernobyl than many feel comfortable to admit.

There may not be a deeply embedded culture of lying stateside, but the U.S. was as willing to cover up the truth of Damascus, as well as thousands of other nuclear accidents, for decades. And when it came down to the final decision making in Damascus, the documentary paints a picture of an out-of-touch Strategic Air Command that issued commands without any understanding of the situation on the ground—decisions that resulted in Livingston's death.

Mazin has made it clear that his *Chernobyl* is not primarily focused on nuclear power. It's a complex subject, as Valery Legasov, played masterfully by Jared Harris, makes clear in the final episode. But perhaps the greatest similarity between Damascus and Chernobyl was the confident belief that nuclear power could be safely managed at all.

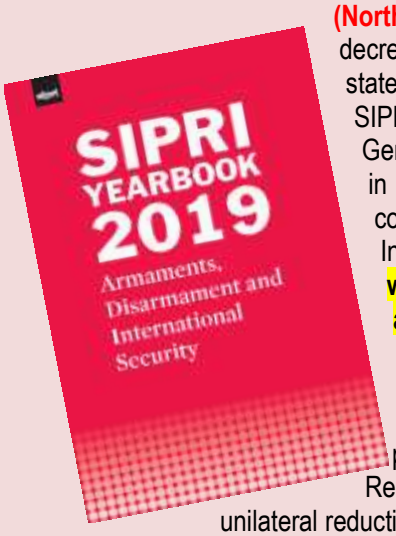
Explaining how nuclear power works in a Soviet court, Legasov describes a dance that can generate tremendous energy. But as Adam Higginbottom shows in *Midnight in Chernobyl*, it's a dance that people have been trying to get right for many years.

The Soviet system might have set up the scientists at V.I. Lenin Nuclear Power Plant for failure. But even with the best dancers in the world, there's eventually a missed step.

Overall number of nuclear warheads decreases, but modernization of world nuclear forces continues

Source: http://www.homelandsecuritynewswire.com/dr20190617-overall-number-of-nuclear-warheads-decreases-but-modernization-of-world-nuclear-forces-continues

June 17 – The modernization of nuclear forces continues, even as the overall number of nuclear warheads continues to decline. **At the start of 2019, nine states—the United States, Russia, the United Kingdom, France, China, India, Pakistan, Israel and the Democratic People's Republic of Korea (North Korea)—possessed approximately 13,865 nuclear weapons.** This marked a decrease from the approximately 14,465 nuclear weapons that SIPRI estimated these states possessed at the beginning of 2018.



SIPRI Governing Board Chair Ambassador Jan Eliasson, former Deputy Secretary-General of the United Nations, says: "A key finding is that despite an overall decrease in the number of nuclear warheads in 2018, all nuclear weapon-possessing states continue to modernize their nuclear arsenals."

Information gathered in SIPRI Yearbook 2019 shows **that of these 13,865 nuclear weapons, 3,750 are deployed with operational forces and nearly 2,000 of these are kept in a state of high operational alert.**

SIPRI says that the decrease in the overall number of nuclear weapons in the world is due mainly to Russia and the United States—which together still account for over 90 percent of all nuclear weapons—further reducing their strategic nuclear forces pursuant to the implementation of the 2010 Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START) while also making unilateral reductions. In 2018, Russia and the USA announced that they had achieved the final New START force reduction limits by the specified deadline.

New START will expire in 2021 unless both parties agree to extend it. There are currently no discussions about extending New START or negotiating a follow-on treaty. "The prospects for a continuing negotiated reduction of Russian and US nuclear forces appears increasingly unlikely given the political and military differences between the two countries," says Shannon Kile, Director of SIPRI's Nuclear Disarmament, Arms Control and Non-proliferation Program.

Both Russia and the United States have extensive and expensive programs under way to replace and modernize their nuclear warheads, missile and aircraft delivery systems, and nuclear weapon production facilities. In 2018, the U.S. Department of Defense set out plans to develop new nuclear weapons and modify others to give them expanded military roles and missions.

The nuclear arsenals of the other nuclear-armed states are considerably smaller, but all are either developing or deploying new weapon systems or have announced their intention to do so. China, India and Pakistan are increasing the size of their nuclear arsenals. "India and Pakistan are expanding their military fissile material production capabilities on a scale that may lead to significant increases in the size of their nuclear weapon inventories over the next decade," says Kile.

North Korea continues to prioritize its military nuclear program as a central element of its national security strategy, although in 2018 it announced a moratorium on the testing of nuclear weapons as well as medium- and long-range ballistic missile delivery systems.

SIPRI notes that the availability of reliable information on the status of the nuclear arsenals and capabilities of the nuclear-armed states varies considerably.

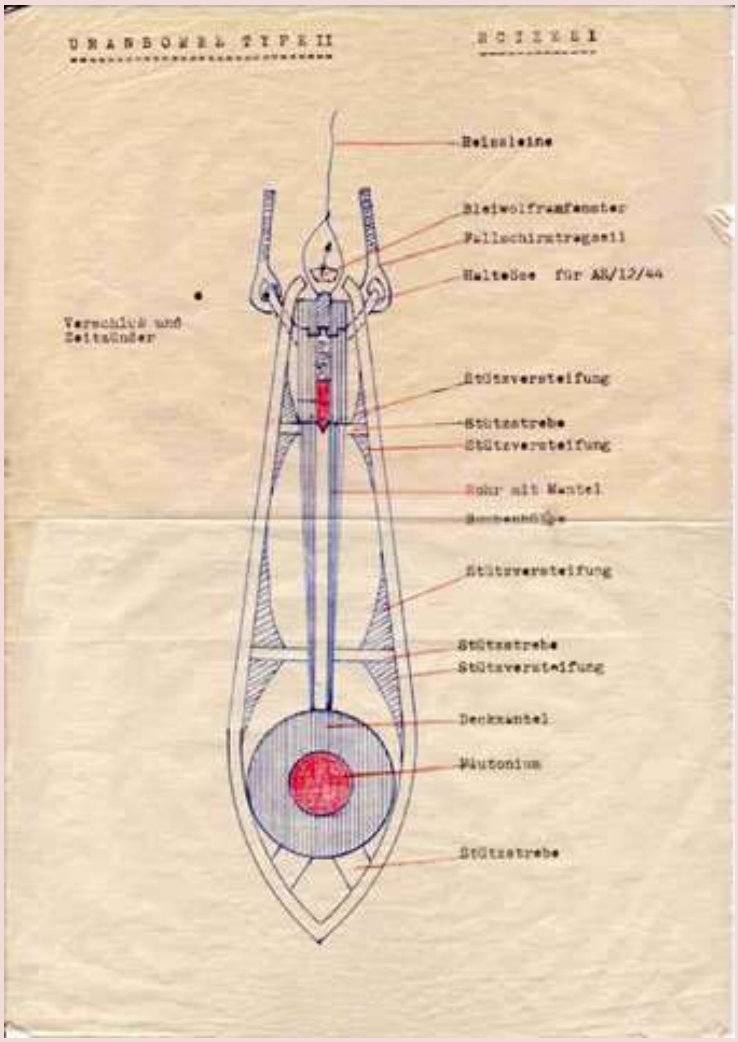
The United States and the United Kingdom have disclosed important information about their stockpile and nuclear capabilities, and France has also declared some information. Russia does not make publicly available a detailed breakdown of its forces counted under New START, even though it shares this information with the United States.

The governments of India and Pakistan make statements about some of their missile tests but provide little information about the status or size of their arsenals. At present, North Korea has acknowledged conducting nuclear weapon and missile tests but provides no information about its nuclear weapon capabilities. Israel has a long-standing policy of not commenting on its nuclear arsenal.

How close was Nazi Germany to the bomb?

Source: http://www.homelandsecuritynewswire.com/dr20190620-how-close-was-nazi-germany-to-the-bomb

June 20 – Back in 2013, Timothy Koeth, an associate research professor at the University of



Maryland, received a rather extraordinary birthday gift: a little cloth lunch pouch containing a small object wrapped in brown paper towels. As Koeth peeled back the layers, his eyes grew wide with astonishment. He immediately asked, "Where did you get that?"

Inside he found a heavy metal cube and a crumpled message, a provocative note wrapped around a stone that came crashing through the window of history. It read, "Taken from Germany, from the nuclear reactor Hitler tried to build. Gift of Ninninger."

Koeth's friend grinned, picked up the 5-pound block of uranium metal and handed it to him. Though modest in size, the cube was heavy, dense and steeped in lost history. Koeth accepted the cube and its note as an invitation to the adventure of a lifetime.

In the May 2019 issue of *Physics Today*, Koeth and Miriam Hiebert, a doctoral candidate working with him on this project at UMD's A. James Clark School of Engineering, describe what they've discovered while exploring the German quest and failure to build a working nuclear reactor during the Second World War.

Uranium is weakly radioactive, and this particular cube measures about 2 inches on each side. "It's surprisingly heavy, given its size, and it's always a lot of fun to watch people's reaction when they pick it up for the first time," said Hiebert.

A chandelier of nuclear elements

AIP notes that this cube represents one of 664 uranium metal components that were strung together in a form reminiscent of a chandelier to comprise the core of a nuclear reactor experiment that a team of German scientists attempted to build toward the end of the World War II, including Werner Heisenberg — a theoretical physicist and one of the key visionaries of quantum mechanics. The chandelier was submerged in heavy water to regulate the rate of fission.

The Germans' experimental lab was small and located underground in the town of Haigerloch — it's now the Atomkeller Museum, which the public can visit. "This experiment was their final and closest attempt to create a self-sustaining nuclear reactor, but there wasn't enough uranium present in the core to achieve this goal," said Koeth.

One of the most surprising things Koeth and Hiebert have discovered so far is that while the 664 uranium cubes at Haigerloch weren't enough to build a self-sustaining reactor, an additional 400 cubes were located within Germany at the time.

"If the Germans had pooled their resources, rather than keeping them divided among separate, rival experiments, they may have been able to build a working nuclear reactor," said Hiebert. "This highlights perhaps the biggest difference between the German and American nuclear research programs. The German program was divided and competitive; whereas, under the leadership of General Leslie Groves, the American Manhattan Project was centralized and collaborative."

How close did the Germans get?

How close did the Germans get to a working nuclear reactor? This is difficult to answer, but "it's been calculated that the reactor experiment in Haigerloch would have needed about 50 percent more uranium to run," said Koeth. "Even if the 400 additional cubes had been brought to Haigerloch to use within that reactor experiment, the German scientists would have still needed more heavy water to make the reactor work. Despite being the birthplace of nuclear physics and having nearly a two-year head start on American efforts, there was no imminent threat of a nuclear Germany by the end of the war."

Another important aspect of Koeth and Hiebert's work is an effort to track down the cubes recovered from Haigerloch that ended up being shipped to the U.S."Cubes were distributed to various individuals around the country," Hiebert explained. "We don't know how many were handed out or what happened to the rest, but there are likely more cubes hiding in basements and offices around the country, and we'd like to find them!"

Many questions remain unanswered, and chief among them are: How many of these cubes still exist, and what has happened to them? Physics Today helped track down a few.

"We hope to speak to as many people as possible who've had contact with these cubes," said Hiebert. "As much as we've learned about our cube and others like it, we still don't have an answer about how exactly it ended up in Maryland 70 years after being captured by Allied forces in southern Germany."

Koeth and Hiebert are also trying to learn more about the fate of the other 400 cubes that ended up on the black market in Europe after the war.

Koeth and Hiebert said that anyone with any information about one of these uranium cubes, can contact them via email at uraniumcubes@gmail.com.

— Read more in Timothy Koeth and Miriam Hiebert, "Tracking the journey of a uranium cube," Physics Today 72, no. 5 (1 May 2019).

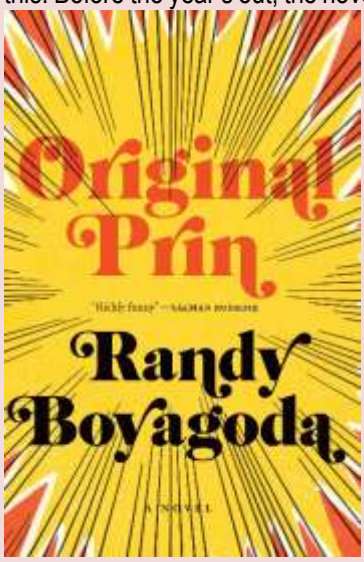

ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EXPLOSIVE
NEWS

His Novel's Hero Is a Middle-Aged Canadian Catholic Professor. And a Suicide Bomber

By Tom Barbash

Source: https://www.nytimes.com/2019/05/30/books/review/original-prin-randy-boyagoda-novel.html

May 30 – Pity poor Prin. The college where he teaches is failing. His area of study, marine references in Canadian literature (post-"English Patient" seahorses), is in the midst of a dry patch. His marriage to Molly feels increasingly unglamorous, and even a trip to the Toronto Zoo ends in the death of one of his daughters' favorite primates, prompting Prin to come clean to his kids about his cancer diagnosis. Then this: Before the year's out, the novel's first line reveals, Prin, a self-doubting, bike-riding, practicing Roman Catholic, will become a full-fledged suicide bomber.



"**Original Prin**," Randy Boyagoda's third novel, is an original animal, a comedy of literary and cultural references, with wordplay involving unfunny matters like cancer, a crisis of faith and Islamic terrorism, as well as easier comedic subjects like juice-box fatherhood and academic power plays.

Spotted early, Prin's prostate cancer is excised along with his prostate. Mortality postponed, he turns his attention toward the fate of his college — the University of the Family Universal, or U.F.U. (the old name, Holy Family College, sounded "too Catholic," Boyagoda writes) — and then a problematic attraction to his predatory ex-girlfriend, Wende, a consultant hired to save the college by (a) turning it into an elder-care assisted living facility and (b) partnering with an academic group in a fictional war-torn Middle Eastern country called Dragomans.

The story takes us then to Molly's family's home in Milwaukee, where Prin witnesses two near-death moments that end up being elaborate pranks: the first staged by one of Prin's nephews to win the attention of a pretty lifeguard, the second the shooting of his nephews' favorite right-wing shock jock by what turns out to be a group of antiwar paintball marksmen.

What to make of all these high jinks? Boyagoda finds dark absurdities in all corners: A self-promoting colleague promises to share her personal mindfulness space with Prin until he recovers; during confession, a priest talks about "Star Wars"; Wende's stated seat designation, 34C, for her flight to Dragomans, leaves Prin wondering if it might be "information meant to remind him of something." A young Dragomans man wears a T-shirt that reads "We Found the Weapons of Mass Destruction," with arrows pointed at his biceps.

There are references throughout to those who were likely Boyagoda's influences: Kingsley Amis (Prin's comically domineering father is named Kingsley), Evelyn Waugh, Vladimir Nabokov, Thomas Pynchon and David Foster Wallace. Most of this is clever, often ingenious, but the frequency of one-liners works against the novel's trajectory. The comedic exit ramps feel like authorial escapes, as if we can't go more than a page or two before the next absurdity, and so we're less involved in Prin's journey, and more aware of Boyagoda's restless intellect.

Once arrived in Dragomans, Prin endures a cab trip with a driver who loves "the Taylor Swift" and a Steve Jobs-style presentation by the country's newest minister of education and strategic realignment initiatives, a Silicon Valley exile who wears wire-rimmed glasses and a black mock-turtleneck T-shirt and introduces his cheering audience to Dragomans 2.0, then segues to Prin's lecture on Kafka by saying the writer "absolutely crushed a story about metamorphosis."

In discussions that night on the dismantling of U.F.U., Wende, "the ice queen bitch-goddess of the wordplay universe," presses her knee against Prin under the table and lures him into a kiss that throws him into a panic. Prin then bungles a phone conversation with his family that leaves him feeling adrift. Without revealing how suicide bombing figures into the final act of the book, it's enough to say that it fits into Boyagoda's absurdist design and raises, albeit

late, some of the book's most fascinating questions about fanaticism and the state of the modern world. Prin evolves in surprising ways, and tensions spike. For readers feeling confounded at the end, fear not. It's the first in a planned trilogy.

Innovations in CBRNe and EOD: Meeting the Needs of Responders

By Cpt. Christian Resch

Research and Development Manager CBRN Defence and C-IED, Federal Ministry of Defence Austria

Source: http://nct-magazine.com/nct-magazine-june-2019/innovations-in-cbrne-and-eod-meeting-the-needs-of-responders/

The technological change of the last decades not only has a fundamental social Led change, but also the armed forces face new challenges. New forms of conflict and "hybrid" threat images require comprehensive solutions and make new demands on capability development of armed forces to continue in the future as a "strategic action reserve".

Defense research follows the requirements of military capability as a function of military and security competence. It establishes new forms of cooperation for innovation and technology development, both at European and national level. To ensure military innovation capability of the Austrian Armed Forces the defense research program "FORTE" has been established.

Defense Research in Austria – CBRN & C-IED a top priority

FORTE will support EUR 5 million worth of scientific and technological military research to develop capabilities for future threat scenarios and to enhance the capacity of the armed forces to innovate. The Austrian Armed Forces are responsible as a user and expert for the content and thematic design of the funding program. Key research areas are "Cyber Defense", "Information Management Systems", "CBRN Defense", "Counter IED", "Critical Infrastructure Protection against UAVs" and "Military Robotics", which follows the strategic direction and necessary skills of modern, innovative and future-oriented armed forces.

However, FORTE does not only make a significant contribution to the military capability development, but also positions the Federal Ministry of Defense and the Armed Forces as partners of the economy and industry for research, innovation and technology development. As a research funding program, FORTE therefore also aims to set new priorities in Austria's research landscape and, subsequently, to strengthen its national competencies in such a way that national research institutions and companies are also competitive in an international environment.

▶▶ You can read the rest of this article at source's URL.

Captain Christian Resch *is a CBRN Defense Officer and working as the Research and Development Manager in the Austrian Federal Ministry of Defense. In the Science, Research and Development Division he is responsible for all activities related to CBRN and C-IED. He has been working for over ten years in operational service of the Austrian Armed Forces as a Commander. Captain Resch holds a Master's degree in military leadership and in process and plant safety, where he is currently writing his PhD on critical chemical infrastructures. He is also Managing Director of DCNA (Disaster Competence Network Austria), a science and research cluster in the field of security and disaster research.*

Flying 'drone grenade' is the future of airborne weaponry

Source: https://metro.co.uk/2019/06/12/flying-drone-grenade-future-airborne-weaponry-9919673/

The military has embraced drone technology in a big way, using it to avoid sending soldiers to their deaths. Now there's a new type of weaponized drone that was shown off at an arms conference in Florida last month. It's called the Drone-40 and it's a low-cost 40mm munition

that can be flown remotely into enemy territory and detonated. Basically, it's a drone grenade. The weapon

is fired from a conventional grenade launcher before four, helicopter-style rotors deploy in order to keep it aloft. It can fly for 12 minutes or hover for 20 minutes. It is cruising speed is 20m/s and it has a range of 10km.

It doesn't just have to be loaded with explosives. It can be used to deploy cameras or smoke bombs or just as a countermeasure to other UAVs. Soldier Systems explains: 'With these mixed of payload types, Drone-40 can be used individually, paired, or as a swarm, to a variety of effects. For example, a team could launch one or more ISR configured munitions along with a swarm of anti-armor payloads and loiter over an ambush spot, waiting for a vehicle column. 'With Multi-Round Simultaneous Impact mode, multiple effects can be achieved at once, depending on the types of payloads delivered.'

London terrorists linked to Iran had secret bomb factory with stockpile of TONS of explosives before plot smashed by MI5

Source: https://www.thesun.co.uk/news/9257721/london-terrorists-bomb-factory-hezbollah/

June 09 – Terrorists with links to the Iran-backed militant group Hezbollah have reportedly been caught stashing tons of explosive materials in London.

It's claimed radicals stockpiled thousands of ice packs containing ammonium nitrate at a secret bomb factory on the outskirts of the capital.

The Daily Telegraph reveals officers from MI5 and the Metropolitan Police uncovered the terrifying plot in the autumn of 2015.
Three metric tonnes of ammonium nitrate - a common ingredient in homemade bombs - was said to have been discovered.
The paper reports that is more than the amount used to in the horrific Oklahoma City bombing that killed 168 people and devastated hundreds of buildings.
Four properties were raided in North West London and a man in his forties was arrested on suspicion of plotting terrorism before being released without charge.
One source said the plot was "proper organised terrorism". Another added that enough explosive materials were stored to do "a lot of damage".

Tip off

The covert operation was reportedly launched after a tip off- which the Telegraph understands came from a foreign government.
MI5's intelligence investigation is understood to have lasted months was part of an effort to disrupt the plot and also get an insight into what Hezbollah was plotting.
However, there was no evidence that the UK was to be target of any bomb attacks, it's reported.
A UK intelligence source said: "MI5 worked independently and closely with international partners to disrupt the threat of malign intent from Iran and its proxies in the UK."
The news comes amid mounting tensions between Iran and the west and after Home Secretary Sajid Javid announced a blanket ban on those with links to Hezbollah.
In February, he ruled all UK supporters of the Iran-backed group will face up to 10 years in prison.
Hezbollah - or the Party of God - is a Shia Muslim movement which emerged during the early 1980s with financial backing from Iran.
In 2001, ministers banned its external security organisation. Seven years later, the proscription was extended to Hezbollah's military wing.
A listing in the official register of banned groups says Hezbollah is "committed to armed resistance to the state of Israel, and aims to seize all Palestinian territories and Jerusalem from Israel".

'Balloon bomb' launched from Gaza explodes in Israel, report says

Source: https://www.foxnews.com/world/balloon-bomb-from-gaza-explodes-in-israel-report

June 12 – A "balloon bomb" launched from the Gaza Strip reportedly exploded over a community in southern Israel on Wednesday, as tensions along the border escalated.

The explosion, which did not cause any injuries or damage, came as Gazans have stepped up launches of balloon-born incendiary devices into Israel, The Times of Israel reported, citing government officials.
A local government spokesperson told the outlet that the device detonated "near a community in the Eshkol region" and "residents reported a loud blast heard in the community."
The explosion marked the first explosive attack of its kind from the Gaza Strip since an Egyptian-brokered cease-fire was reached following two days of intense fighting in early May, which killed 25 militants and civilians in Gaza as well as four Israeli civilians.
As part of the agreement, Gaza's Hamas rulers were reportedly obligated to stop the launching of incendiary balloons at Israel. In addition to the danger they pose to people, the devices have been blamed for wildfires.

While violence has subsided since the cease-fire agreement, fire departments in southern Israel reported an increase in "arson attacks," including six fires on Wednesday, which fire officials believe is a result of the devices, The Times of Israel reported.

On Tuesday, seven fires in southern Israel were reportedly sparked by "balloon bombs," which prompted Israel to announce that it will further scale back the Gaza fishing zone from 11.5 miles to about 7.

Israeli officials have said they hold Hamas responsible for all attacks from the coastal territory. The sides have engaged in several rounds of cross-border fighting over the past year.

Security Union: The EU strengthens rules on home-made explosives and fight against terrorist financing

Source: http://europa.eu/rapid/press-release_IP-19-3003_en.htm

June 14 – Today, the Council adopted two important priority files under the Security Union which strengthen EU rules on explosives precursors and facilitate law-enforcement access to financial information. The reinforced rules on explosives precursors will ensure stronger safeguards and controls, including online, on the sale and marketing of the dangerous chemicals, which have been used to produce "home-made" explosives in a number of terror attacks in Europe. The new measures on access to financial information will allow law enforcement to obtain important financial information across borders quickly, helping them fight serious crime and terrorism more effectively.

Commissioner for Migration, Home Affairs and Citizenship Dimitris **Avramopoulos** said: *"Terrorists and criminals will find it much harder to get their hands-on dangerous chemicals to produce home-made bombs or money to fuel their crimes. I am glad to see that the Security Union we have been building over the past 5 years is progressing steadily and that we are closing the most pertinent security loopholes."*

Commissioner for Justice, Consumers and Gender Equality Věra **Jourová** said: "*Following the money is one of the most effective ways to fight organised crime and terrorism. Our law enforcement authorities gain an important tool to get financial information quickly to improve security of our citizens and serve justice."*

Commissioner for the Security Union Julian **King** said: *"The adoption of these two measures marks an important step forward in closing down the space in which terrorists operate - making it harder for them to obtain the chemicals needed to make home-made explosives, while making it easier for law enforcement to tackle terrorist financing. It is important that Member States now fully implement these measures as quickly as possible."*

The EU already has strict rules in place on access to chemical substances that can be used to produce homemade explosives, however the new Regulation will:

- **Ban additional substances**: two additional chemicals will be banned: sulphuric acid, which is a central ingredient for the production of the highly explosive TATP (tri-acetone tri-peroxide); as well as ammonium nitrate, a chemical predominantly used as a fertiliser.
- **Strengthen licensing and screening**: national authorities will be required to carry out a more in-depth check on members of the public applying for a license to purchase restricted substances. In particular, they will need to check the legitimacy of such a request and perform a careful security screening, including a criminal background check on the applicant.

The new measures for cross-border access to financial information by law enforcement authorities will complement the EU Anti-Money Laundering framework while ensuring:

- **Timely access to information:** law enforcement authorities, Asset Recovery Offices (AROs) and anti-corruption authorities to have direct access to bank account information contained in the national centralised bank account registries. All Member States have to set up these registries under new EU Anti-Money Laundering rules.
- **Better cooperation**: the new rules will also ensure greater cooperation between national law enforcement, Europol and Financial Intelligence Units (FIUs) and will further facilitate the exchange of information between the national FIUs.
- **Stronger data protection safeguards**: the new Directive provides for strong procedural and data protection guarantees in line with the Charter of Fundamental Rights.

Next Steps

Both texts will now need to be signed by the President of the European Parliament and the rotating Presidency of the Council after which they will be published in the Official Journal of the European Union. The new rules will enter into force 20 days later and as regards explosives precursors, they will start applying across the EU in 18 months´ time. Member States will have 2 years to transpose the new measures facilitating access to financial information into their national laws.

Background

The Juncker Commission has prioritised security from day one. The European Agenda on Security guides the Commission's work in this area, setting out the main actions to ensure an effective EU response to terrorism and security threats. Since the adoption of the Agenda, significant progress has been made in its implementation, paving the way towards an effective and genuine Security Union.

In 2013, the EU put in place rules to restrict access to explosive precursors that could be used to make home-made explosives. However, the security threat has been constantly evolving with terrorists using new tactics, and developing new recipes and bomb-making techniques. This is why the Commission proposed to tighten those rules further in April 2018, as part of a wider set of security measures to deny terrorists the means to act. The European Parliament and the Council reached a provisional agreement on the Commission's proposal on 4 February.

Criminal groups and terrorists are increasingly operating across borders with their assets located both within and beyond EU territory. While the EU has a strong EU Anti-Money Laundering framework, the current rules do not set out the precise conditions under which national authorities can use financial information for the prevention, detection, investigation or prosecution of certain criminal offences.

Following up on the Action Plan set out in February 2016, in April 2018 the Commission proposed to facilitate the use of financial and other information to prevent and combat serious crimes, such as terrorist financing, more effectively. The measures, agreed by the European Parliament and the Council on 12 February, will strengthen the existing EU anti-money laundering framework as well as Member States' capacity to combat serious crime.

FBI releases image of teddy bear pipe bomb from serial Anderson County bomber

Source: https://www.greenvilleonline.com/story/news/2019/06/17/fbi-releases-image-teddy-bear-pipe-bomb-anderson-county-bomber/1480122001/

June 17 – The FBI released additional details Monday about a convicted Anderson County bomber, including never-before seen images of a teddy bear pipe bomb left in a local road.

An Anderson County man was convicted in October 2018 and sentenced in March after leaving six bombs, three of them were hoaxes and three with explosives, according to court records and the FBI.

The devices were discovered between Jan. 24, 2018, and Feb. 24, 2018, according to the FBI's timeline, which adds details about the timing and type of device used.

The FBI released the statement Monday morning, recounting the case and adding details of the bureau's role and the evidence against the man, some of which have not been previously reported.

The convicted bomber is described by the FBI as a "terrorist sympathizer" who was radicalized by reading propaganda from propaganda from Anwar al-Awlaki, Osama bin Laden and others.

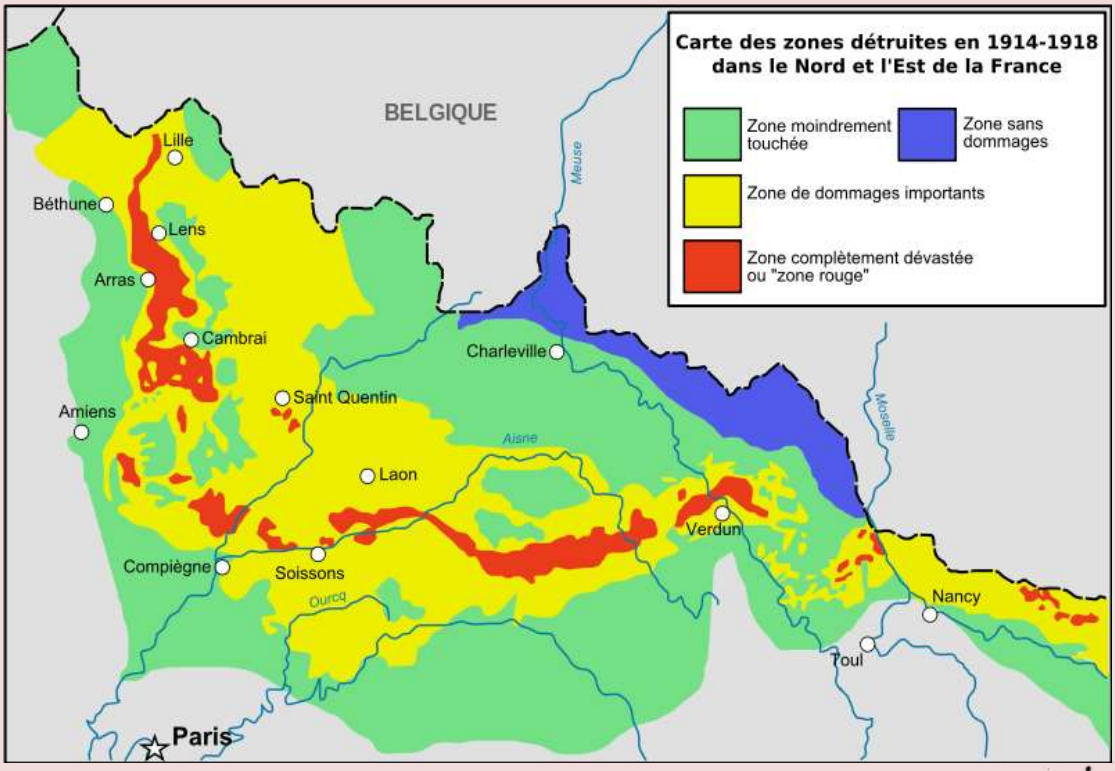
Wesley "Dallas" Ayers, 28, was sentenced in March to more than 30 years in federal prison and another 5 years of supervision after release. He pleaded guilty to using, attempting to use, and threatening to use weapons of mass destruction; possession and discharge of a firearm in furtherance of a violent crime; and to the use of an explosive device during the commission of a felony.

Ayers is being held at a federal detention center in Illinois with an anticipated release date in 2044, according to online records.

The Independent Mail and The Greenville News has previously reported many of the details of the case, including that one device was a teddy bear pipe bomb and that the investigation began after an Anderson County man was injured by a small explosive device found in a basket in a roadway.

Zone Rouge (France)

Source: Wikipedia



Map showing condition immediately following the war: totally destroyed areas in red, areas of major damage in yellow and moderately damaged areas in green

The *Zone Rouge* (English: Red Zone) is a chain of non-contiguous areas throughout northeastern France that the French government isolated after the First World War. The land, which originally covered more than 1,200 square km (460 sq mi), was deemed too physically and environmentally damaged by conflict for human habitation. Rather than attempt to immediately clean up the former battlefields, the land was allowed to return to nature. Restrictions within the *zone rouge* still exist today although the control areas

have been greatly reduced.

The *zone rouge* was defined just after the war as "Completely devastated. Damage to properties: 100%. Damage to Agriculture: 100%. Impossible to clean. Human life impossible".

Under French law, activities such as housing, farming or forestry were temporarily or permanently forbidden in the *zone rouge*. This was because of the vast amounts of human and animal remains and millions of items of unexploded ordnance contaminating the land. Some towns and villages were never permitted to be rebuilt after the war.

Main dangers

The area is saturated with unexploded shells (including many gas shells), grenades, and rusty ammunition. Soils were heavily polluted by lead, mercury, chlorine, arsenic, various dangerous gases, acids, and human and animal remains. The area was also littered with ammunition depots and chemical plants.

Each year dozens of tons of unexploded shells are recovered. According to the Sécurité Civile agency in charge, at the current rate 300 to 700 more years will be needed to clean the area completely. Some experiments conducted in 2005–06 discovered up to 300 shells/10,000 m^2 in the top 15 cm of soil in the worst areas.

Some areas where 99% of all plants still die remain off limits (for example two small pieces of land close to Ypres and Woëvre), as arsenic constitutes up to 176 mg/kg of soil samples.

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

CYBER NEWS

The Growing Importance of Bio-Cybersecurity

By Ryan Riggs

Source: https://www.cpomagazine.com/cyber-security/the-growing-importance-of-bio-cybersecurity/

June 04 – In a world where more than 26 million people have taken an at-home DNA test, healthcare companies are soon going to have to face a new frontier of patient expectations for security. As patients increasingly want genetic screening to be part of preventative care, healthcare systems are responding by offering DNA sequencing—but nearly all are unprepared for the demands of bio-cybersecurity. As DNA sequencing becomes more common, healthcare providers, payers, vendors, and pharmaceutical companies need to ensure that patient genetic data is secure.

While genetic databases have been put to good use improving medicine and even tracking down serial killers, consumers are gradually becoming aware of why genetic data needs to be better protected. Stories of misuse are revealing how ill-prepared healthcare companies are for genetic sequencing. Between the national security threats of biological warfare and authoritarian states conducting massive surveillance programs (as is currently happening in northwest China), healthcare cybersecurity professionals need to think about how to protect their patients' genetic information.

Most security breaches involving DNA to date has been testing companies experiencing the garden variety theft of emails and passwords. The risks begin to multiply though when DNA data itself is taken into consideration. Healthcare systems could experience a breach of genetic data from ransomware and be forced to purchase back patient data. Hackers might also use stolen genetic data to blackmail individuals who have compromising information embedded in their DNA. As consumer's genetic identification becomes increasingly tied to standard forms of identification (e.g. driver's license, birth certificate, passport, etc.), the opportunity for identity theft using stolen genetic data could become more prevalent. These are not far-fetched futuristic prognostications. Any of these scenarios could appear in the news tomorrow.

The shift to cloud services across healthcare has been a boon to the industry in terms of improving interoperability and accessibility – but it has also opened up greater bio-cybersecurity threats. Healthcare vendors and providers cited cybersecurity, privacy and security as their top concern according to the 2019 HIMSS U.S. Leadership and Workforce Survey. And for good reason: the average healthcare organization spends $1.4 million to recover from a cyberattack, so the cost of inaction is significant.

When researchers from the University of Washington looked at the sort of open-source programs currently used by many DNA test companies, they found the DNA data process pipeline to be extremely vulnerable to hacking. This inherent vulnerability has given rise to a number of start-ups focused on offering secure genetic testing. For many, the future of protecting genetic data lies in blockchain.

The company Nebula Genomics created by George Church, a professor of genetics at Harvard, utilizes blockchain technology and multi-party access control to encrypt data with multiple keys and ensure data is anonymized. The anonymization methods currently used by DNA testing companies like 23 and Me do not protect against genomic re-identification and rely entirely on the company's discretion regarding the dispersal of that data (if the consumers opts in). Whereas, blockchain is encrypted, resilient to hacking and can be shared out on a time-limited basis with the ability to choose what parts of your genome to provide. It also enables patients to securely sell their DNA to researchers.

Blockchain technology has the potential to not only upend the DNA testing market estimated to be worth over $22 billion in five years, but also creates an imperative for healthcare systems to ensure electronic health records and other patient information are secure.

And some healthcare companies are already experimenting with the technology. Humana, Optum and others have formed an alliance to pilot the use of blockchain to managing provider directories, while healthcare start-ups are using the technology to reinvent how patient data is disseminated. Doc.ai, for example, enables patients to securely sell their medical data to researchers using blockchain and smart contracts.

The trend towards patients owning their genetic and medical data marks a major shift in technology and will also change the economic model of how patient data is sourced. While there's a long history of paying test subjects, medical researchers paying patients directly for their genetic and medical data will transform the value of those records, turning them into

a currency. Having genetic data and medical records hacked may not seem so terrible now, but when it leads to a loss of income for the end-consumer, healthcare doesn't have long to adopt a more secure technology like blockchain.

Ryan Riggs *is VP of Cloud Services at ProKarma, where he develops and delivers cloud and cybersecurity solutions that help companies reduce risk and run the future. He is a former VP of Operations at IP Services and Yesmail, and specializes in using information technology to drive growth while improving customer experience.*

Entering the Third Decade of Cyber Threats: Toward Greater Clarity in Cyberspace

By Dan Efrony

Source: https://www.lawfareblog.com/entering-third-decade-cyber-threats-toward-greater-clarity-cyberspace

June 13 – Over the course of just a few decades, the world has entered into a digital age in which powerful evolving cyber capabilities provide access to everyone connected online from any place on the planet. Those capabilities could be harnessed for the benefit of humanity; they might also be abused, leading to enormous harms and posing serious risks to the safety and stability of the entire world.

A strategy of international cooperation is crucial to mitigate the threats of abuse of cyberspace, primarily by clarifying the "red lines" in the field of cybersecurity and determining how to verify and enforce states' compliance with their legal obligations in the field. The five permanent members of the U.N. Security Council (the P5) should have a decisive role in meeting this challenge. Yet while the P5 have had some success when mitigating the risks posed by weapons of mass destruction, the group is unlikely to be able to duplicate this pattern of action in cyberspace considering the rising tensions among the P5 and the geopolitical divisions in cyberspace. These divisions manifested in the 2017 failure of the United Nations Group of Governmental Experts on Information Security (UN-GGE) to produce a consensus report after two decades and five sessions of governmental groups of experts. Nevertheless, given the significance and seriousness of the risks that cyber operations pose to the safety and stability of states, giving up on collective action altogether is also unacceptable.

Currently, states have used three main modes of action to meet the challenge, which I will briefly review below. Recent developments have highlighted the mode embraced and

implemented by the U.S. and its close allies: a deterrence-based approach combined with a high degree of ambiguity regarding questions of law and policy in cyberspace. However, this ambiguity undermines attempts to develop clear rules for the conduct of states in cyberspace and thereby adversely affects both the effectiveness of deterrence and the legitimacy of cyber operations conducted to compel compliance with general nonbinding norms and principles. This approach should be reconsidered in favor of a clearer and more balanced strategy that can gain at least the international acceptance of like-minded states.

Current Modes of Action

Since the failure of the UN-GGE in June 2017, key states active in cyberspace have mainly taken three separate modes of action to mitigate the threats posed in or through cyberspace. First, states have *resumed international cooperation* through two new parallel groups of governmental experts, instead of the one that collapsed. Both new groups act in accordance with two bidirectional resolutions, which the U.N. General Assembly adopted in December 2018. One resolution, led by the United States, established the GGE (Group of Governmental Experts) and the other, led by Russia and China, established the OEWG (Open-Ended Working Group). The two groups' mandates have significant overlap, as both are authorized to discuss, inter alia, the development of rules and norms in the field of cybersecurity and how international law applies to the use of information and communications technologies. Importantly, the new (i.e., sixth) UN-GGE comprises 25 experts representing 25 states, including the P5, whereas the new OEWG is open to all U.N. member states. Since both groups act on the basis of consensus, we will have to wait and see whether either or both will succeed in overcoming the difficulties that caused the failure of the UN-GGE's fifth round.

Second, states have engaged in *voluntary international initiatives* such as the Paris Call, the Cybersecurity Tech Accord, the Charter of Trust and the Global Commission on the Stability of Cyberspace (GCSC). These efforts were initiated by major tech corporations in cooperation with states, think tanks and civil society organizations. These private actors have stepped into the standard-setting arena largely because of a sense of societal responsibility, with a view to fill the void created by the influential states, whose strategy has been to adopt a policy of silence or ambiguity.

The common goal of all those initiatives is to articulate nonbinding norms for cyberspace and to ensure cybersecurity through international cooperation between all relevant stakeholders, inter alia, states, the private tech sector and civil society organizations. They seek to achieve this while preserving neutrality and credibility to reinforce trust and confidence in their processes. In principle, such initiatives should have included most concerned states, including the U.S., the U.K., Russia and China, but these states have refrained from officially becoming involved in such initiatives, ostensibly because they have embraced a policy of ambiguity regarding norms of conduct in cyberspace. This could be considered the Achilles heel of these initiatives—but it does not have to be so, as long as expectations remain modest and reasonable. By acknowledging that states and only states are entitled to determine what constitutes binding law in cyberspace (although adoption of such laws anytime soon seems unlikely), these initiatives have only limited and indirect impact on state practice in cyberspace. Still, they may softly and gradually influence such practice.

Third, states have embraced *a deterrence-based strategy*. The most powerful states in cyberspace—namely, Russia and China on one side, and the U.S. and the U.K. on the other—have funneled their efforts and resources into a vigorous cyber arms race, motivated by their own strategic considerations. The greater technological advantage gained by one side, the more intensified the mistrust and the fear in the mindset of the other. That may trigger retaliatory responses, not necessarily confined to cyberspace, to reestablish the balance of powers or to ensure mutual deterrence. Obviously, such a response is risky—but if managed cautiously, U.S. deterrence may be more successful. Still, it will probably not be enough to meet the long-term challenge of ensuring security and stability in cyberspace.

The U.S. has implemented a three-layer deterrence doctrine as emphasized in the National Cyber Strategy and the Defense Department's 2018 Cyber Strategy, as well as by the U.K. minister of foreign affairs, who depicted it as a new deterrence doctrine endorsed by the U.K.

The first layer is *identification and attribution*, when the evidence is sufficient and public attribution may not jeopardize strategic interests. Second is *naming, shaming and indicting*, when the amount of evidence gathered allows it. Finally, there is *lawful retaliation,* mostly by

retorsions such as diplomatic or economic sanctions, which are lawful acts though unfriendly within interstate relations. Although these layers of operation could be implemented consecutively or separately by any concerned state considering its self-interests in any given scenario, they were tailor-made for the U.S. and its national security interests. Unsurprisingly, the U.S. is the only state that has implemented a doctrine involving all three layers.

A short review of recent developments indicates a change in the U.S. policy in cyberspace toward more a proactive and deterrent approach to ensure compliance of states with nonbinding norms that reflect responsible state behavior.

1. ***Setting the Norms***
   The new National Cyber Strategy encourages "universal adherence to cyber norms: [i]nternational law and voluntary non-binding norms of responsible state behavior in cyberspace provide stabilizing, security-enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace …." Eventually, it refers to the 2017 G7- Declaration of Responsible State Behavior, including the norms, rules and principles of responsible behavior of states consensually endorsed in the UN.-GGE third (2013) and fourth (2015) rounds, and the U.N. Charter.
2. ***Collective Attribution***
   This involves formalizing cooperation with like-minded states to jointly and publicly attribute responsibility for cyber attacks. Attributing the May 2017 WannaCry cyber operation and the June 2017 NotPetya operation at the outset of 2018 (see here, here and here) was a precursor to such enhanced cooperation. In October and December 2018, the U.S and its close allies, mainly its Five Eyes partners (Australia, Canada, New Zealand, and the U.K.), jointly attributed responsibility to Russia and China, respectively, for a series of cyber operations conducted by the GRU (including disruptive and destructive operations) and the group known as APT10 (including economic espionage) against numerous states (see here, here, here, here and here).
3. ***Coordinated Retaliation and Imposing Consequences***
   The updated National Cyber Strategy calls for the deterrence of irresponsible state behavior by imposing consequences for breaching nonbinding norms, such as those endorsed by the UN-GGE and mentioned above. This combines with the launching of an International Cyber Deterrence Initiative by a coalition of like-minded states to coordinate and support each partner's response to significant malicious cyber incidents. The U.S. implemented this strategy by indicting Russian and Chinese governmental operatives for the GRU and APT10 operations (see here and here), in addition to personal sanctions imposed against the Russian and Chinese defendants. However, the U.S. allies had little ability to impose additional costs, especially because the targeted states are superpower states, such as China and Russia. Nevertheless, the U.K., the U.S. and the Netherlands coordinated unprecedented exposure of intelligence about GRU's operatives, methods and cyber operations to harm its operational capabilities (here and here). The U.K. and the U.S. coordinated exposure of intelligence also against China's APT10 (here and here).
   Furthermore, at the national level, Congress has adopted active defense principles toward specific states (Russia, China, North Korea and Iran). This involves removing bureaucratic restrictions and authorizing offensive-defensive actions "to disrupt, defeat, and deter" should any of the four countries conduct malicious activity in cyberspace against the U.S. and the American people, including attempting to influence American elections and democratic political processes. In the same vein, the Defense Department's 2018 Cyber Strategy includes "defense forward" as a deterrent measure, defining it as "disrupt[ing] or halt[ing] malicious cyber activity at its source, including activity that falls below the level of armed conflict." In other words, the policy tackles emerging threats immediately at the source and may include cyber activities below the threshold of "use of force" within the adversary's network or territory, by virtue of the relevant authorities delegated down to the appropriate level in U.S. Cyber Command.
   In the time since the power to approve specific offensive cyber operations has been delegated down, it has been used much more frequently and effectively, including in a preventive manner during the U.S. midterm elections in November 2018 (see

also here). In a recent statement, U.S. National Security Adviser John Bolton emphasized the United States's improved "capabilities across the board to engage in more offensive cyber activities" and told Russia and any other state engaged in cyber operations against the U.S. that they "will pay the price … we will impose costs on you until you get the point."

It is worth noting that the active defense approach has been endorsed publicly by senior officials such as the British minister of foreign affairs and even the French minister of defense, who suggested France's approval of the approach while presenting the new French national cyber strategy. Still, from the perspective of international law, the legality of this proactive approach—which may include "hack-back" actions and other intrusion operations—is questionable. It depends on the way legal terms such as "sovereignty" and "countermeasures" would be interpreted and consensually applied in cyberspace.

Ambiguity and Deterrence

In a recent article for the American Journal of International law, Yuval Shany and I present an investigation of 11 cyber operations that occurred from 2013 to summer 2018, including, inter alia, the hack of the Democratic National Committee, the hack of Sony, the Office of Personnel Management hack, and the WannaCry and NotPetya cyber operations. All these operations were deemed to be executed by states or state-sponsored groups or individuals. Our findings indicated that victim states and attackers as well have endorsed a policy of ambiguity and silence. The goal of such approach is to maintain as much leeway as possible under the legal, technological and political uncertainties of cyberspace—thus, we wrote, "[E]ven when [states] acknowledge that they were victims of cyber operations directed against them, the rhetoric they use to describe the operation and their planned reaction thereto tends not to include legal arguments or references to specific norms of international law."

When operating under conditions of significant normative uncertainty, Shany and I argue, states employ three interrelated strategies: "optionality," regarding international law as an optional legal framework, which states may or may not invoke and apply; "parallel tracks," the development through state practice of formal rules backed by *opinio juris* and informal set of rules shaped by practice without the sense of a legal obligation, both of which can presumably limit state power; and "gradations in law enforcement," distinguishing between violations that are likely to lead to some form of response and those unlikely to do so.

It is worth noting that states did not reference any violation of an international obligation regarding the cyber operations that were collectively attributed (WannaCry, NotPetya, and the APT10 and GRU operations). This is consistent with the strategy of optionality: Treating the applicable international law framework as optional allows states to choose whether or not to invoke the legal discourse of international rights and obligations regarding their mutual interactions in cyberspace.

Undertaking retorsions and criminal indictments coincides with the strategies of "parallel tracks" and "gradations in law enforcement." This is seemingly a reasonable compromise between the deterrence and ambiguity considerations. Hence, despite strong rhetoric about imposing consequences as a deterring retaliation, the U.S. and its close allies have so far applied only retorsions, which are lawful acts, though unfriendly—in lieu of countermeasures, unlawful acts in response to the violation of an international obligation. Countermeasures carry the risk of qualifying as a violation of international law by itself, if undertaken mistakenly.

The U.S. determination to implement a deterrence-based approach in cyberspace in tandem with its policy of ambiguity and silence may weaken deterrence and harm U.S. credibility. It also blurs the message of adherence to the rule of law in cyberspace, which is particularly concerning at a time when the question of how international law should be applied is still open ended and the law unclear and underdeveloped.

Attributing responsibility for violating nonbinding norms and undertaking punitive or retributive measures might be legally problematic, to say the least. Moreover, any attribution claim should refer to a violation of an international obligation, which should be clear and unequivocal. Enforcing nonbinding norms or principles with no clear contents is unacceptable and contradicts basic requirements of the principle of legality, which demands strict articulation of any legal prohibition. A state that deliberately ignores nonbinding norms is not in violation of its international obligations and

therefore cannot be legally subjected to countermeasures, nor can it face consequences according to the deterrence-based approach.

Obviously, the policy of ambiguity is legitimate and premised on a common objective of maintaining operational latitude that remains as wide as possible, both defensively and offensively. However, this policy may result in a vicious cycle. While it serves states' interest in maintaining latitude, it creates a significant obstacle in establishing accountability, which requires a clear binding legal framework and an efficient enforcement mechanism—both of which have not yet been formulated and cannot be shaped under conditions of uncertainty.

Ultimately, the tit-for-tat imposition of consequences provides the U.S. and its close allies with a prominent deterrence tool to deploy against their adversaries. That might be useful against a nonstate actor or less powerful state. But when the adversary is, for instance, Russia or China, the risk of escalation is much more serious.

Bearing in mind the uncertainties regarding the rising tensions among powerful states in cyberspace, along with evolving technological capabilities, ambiguity and deterrence are not a zero-sum game. They can and should be rebalanced.

Increasing Legitimacy

The recent collective attribution claims rely mainly on close cooperation among intelligence communities, primarily the Five Eyes and several additional Western allies. The content and amount of evidence remain classified, and the standard of proof is enunciated by short sentences or phrases such as "highly likely," "high confidence," "almost certainly responsible" and "highest level of probability." That lack of transparency reinforces the adverse effect on the process's credibility, which, in turn, may affect the legitimacy of any act taken in retaliation.

Nevertheless, there are some options that should be considered to increase legitimacy and credibility while implementing limited transparency. A priority should be reinforcing cooperation among an increasing number of like-minded states; collective attribution should involve more than a select group of states. Even more so, substantiating attribution claims also requires permanent cooperation with private cybersecurity and tech firms such as GAFAM (Google, Apple, Facebook, Amazon and Microsoft). Establishing parallel cooperation between states on the one hand and private companies on the other while maintaining national security will be a challenge. But as insurmountable as it may appear, it will be a worthy challenge to tackle.

Gradual Clarification

Exactly a year ago, U.K. Attorney General Jeremy Wright made a significant step toward setting *opinio juris* regarding the application of international law to cyberspace. Most relevant were his comments on the principle of sovereignty in cyberspace: The U.K. does not recognize the existence of a cyber-specific rule on violations of territorial sovereignty. Furthermore, the speech negated the applicability of two traditional obligations: the obligation to provide advance notification prior to executing countermeasures and the obligation to disclose evidence justifying attribution. Moreover, the attorney general emphasized the importance of international law in cyberspace despite the restrictions this places on states' freedom of action: "[B]ecause we believe that a rules-based international order makes the world a safer place … it must also follow that a rules-based international order can only prevail when the rules can be clearly understood and that where they are unclear we seek to bring clarity."

Considering the recent developments in cyberspace, it is time for the U.S.—as a leading superpower in the international community, and primarily in cyberspace—to take the lead in clarifying its legal and political stances regarding the application of international law in cyberspace, particularly on essential issues such as sovereignty, nonintervention, due diligence, countermeasures, the evidentiary standard and even the boundaries of legitimate espionage. Although this will reduce the level of ambiguity, it should not necessarily remove it totally—a gradual reduction in the level of ambiguity might be even better.

The U.S. should also prioritize reinforcing international cooperation to ascertain that the International Cyber Deterrence Initiative (ICDI) does not just focus on deterrence through joint imposition of consequences. Instead, the initiative should attempt to establish accountability in cyberspace by relying on a defined legal framework that includes binding

rules and clear attribution and enforcement mechanisms. This could be done in parallel or in combination with the other modes of action described at the outset. Determining how to do this will be the responsibility of the ICDI, or, more accurately, the International Cyber Accountability Initiative (ICAI) to decide.

Conclusion

Two decades have passed since the UN-GGE was established with the mandate to examine and recommend how to meet the challenges and close the increasing gap between international law and evolving technology in cyberspace. Time is running out. International achievements in standards setting are limited, and cyber threats are increasing exponentially. The international community, particularly democracies led by Western major powers, should enter the third decade of the digital age equipped with broadly accepted tools and strong willingness to establish accountability in cyberspace based on clear, binding rules and enforcement mechanisms.

Maj. Gen. Dan Efrony *was the Military Advocate General of the Israel Defense Force from 2011–2015. He served for 15 years in the IDF intelligence corps, rising to the rank of lieutenant colonel. He is an associate researcher at the Hebrew University's CyberLaw Program.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

Small drones and the use of chemical weapons as a terrorist threat

By Professor David Hastings Dunn
Department of Political Science
University of Birmingham
Source: https://www.birmingham.ac.uk/research/perspective/small-drones-chemical-weapons-terrorist-threat.aspx

Inventive and spectacular ways of killing people has long been a hallmark of Islamic State's modus operandi and recent intelligence reports suggest that the group are becoming even more ambitious in their planning. With the return to the UK from Syria and Iraq of between 400-500 Jihadists counter terrorism experts are now concerned that IS are planning a "technology transfer" of techniques, substances and tactics learned abroad for use in Europe.

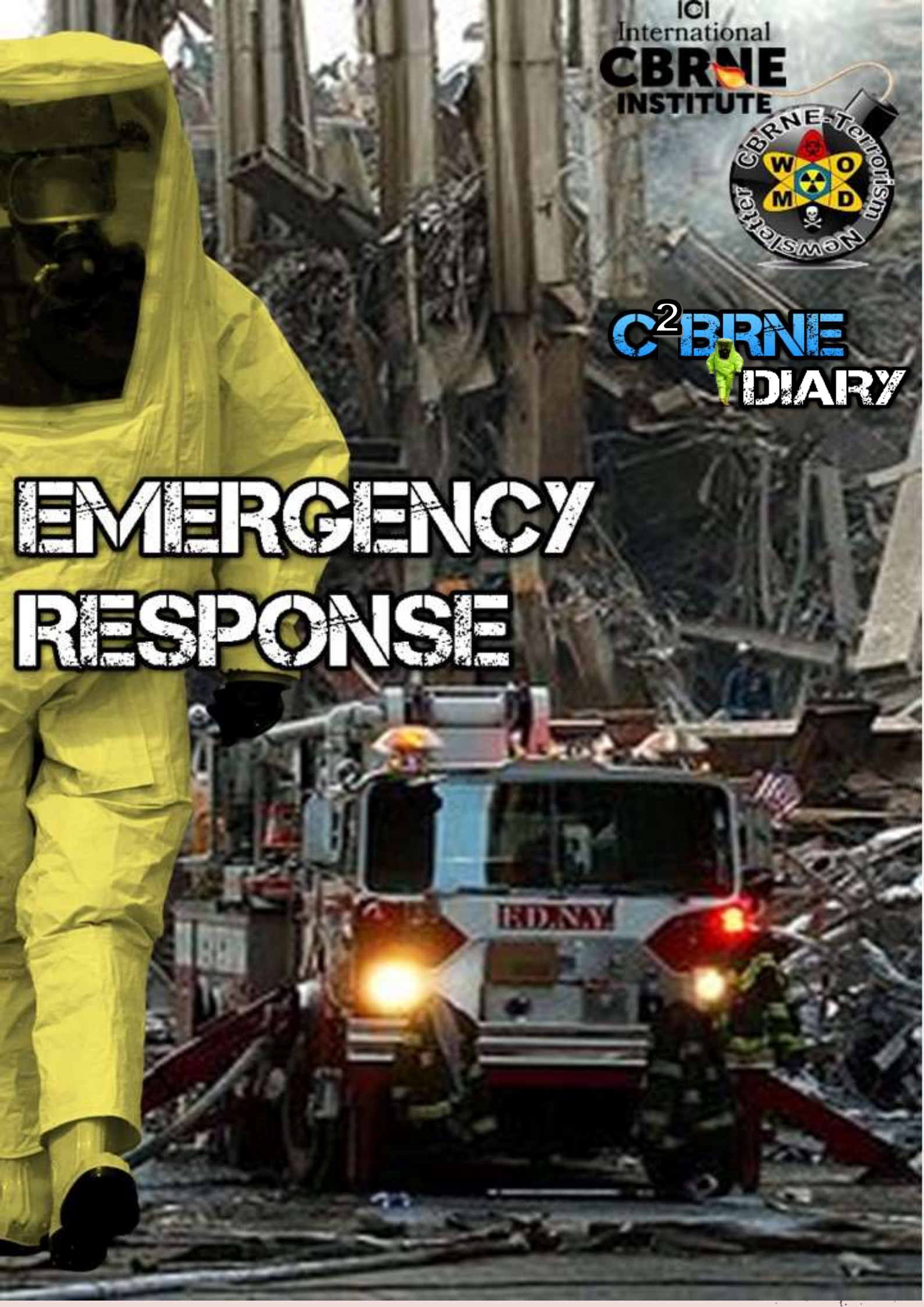
Use of mustard gas and chlorine against Kurdish Peshmerga fighters is well documented, as is research by IS to develop radiological dispersion devices. It is these technologies that are of particular concern to the security services but their concern does not stop there. IS has used drones for propaganda filming and intelligence gathering for years and last October it used a homemade drone to attack and kill Pashmerga fighters. Then in November a secret bomb factory was discovered in Mosel, Northern Iraq. The fear is that IS are planning to marry together two technologies, drones as a dispersal device and chemical, biological or radiological material as the dispersant.

Small drones are cheap, easy to buy and operate and can provide distance and anonymity to their operators. As the first iteration of the robotics revolution they have proliferated on a massive scale with estimates of over five million drones having been sold worldwide. The same technology that enabled the smart phone revolution has now provided unprecedented access to the air. Improvements in battery technology give drones greater power, lift and endurance; cameras are now tiny and highly capable allowing distant operation through live streaming, and fast chips and sensors allow automatic stability and easy operation.

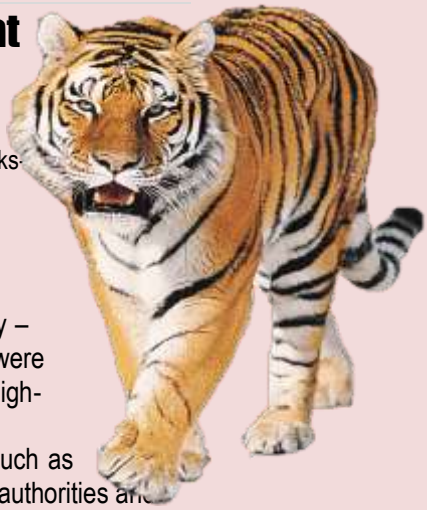
However, the same technology that facilitates the fantastic photography on *Planet Earth II* could also be put to malign or nefarious use. The ability to attach an improvised explosive device (IED) to a drone has already been demonstrated, and the task of weaponising a drone to carry a chemical agent is technically possible, as seen in crop dusting use. What is more, the terrorists don't even need to acquire chemical weapons in order to create weapons. Even gasoline spread as a vapour when ignited has 15 times the explosive energy of the equivalent weight of TNT. Moreover, even if the gasoline was simply ignited its effect on a crowd would be devastating.

How serious the small drone threat should be taken is hotly contested in the counter terrorist community. A Paris style marauding attack or a rucksack filled with ammonium nitrate would technically be an easier terrorist operation to mount and could cause more carnage than the payload of a small drone. But a drone attack would be psychologically unnerving and terror inducing.

Given the use of drones in Afghanistan and Iraq by Britain and the US it also has symbolical appeal to IS and its affiliates. To guard against the small drone threat would also require a rethink of some established notions. Traditionally a building is secured by perimeter defence and entry point control. In November 2015 this prevented terrorists entering the Stad Du France in Paris. If the jihadists had put their devices on drones, however, they could have flown into the stadium with potentially devastating effect. Similarly, defending aircraft in flight or on the ground from a swarm attack by drones is also a concern for police and security services. The British Airline Pilots Association has called for studies of the effect of a drone strike on a jet engine. The concern is that their lithium batteries alone could cause an engine fire. Multiple drones flown at these engines for deliberate effect could cause a mass casualty event. Clearly the misapplication of "dual use" chemicals or recreational drones poses new challenges for security in the age of terrorist attack. How to assess these threats and how to deal with them accordingly is also the job of academics interested in security studies.


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

Earthquakes or tiger attacks: understanding what people fear most can help prevent disasters



By Hanna Ruszczyk

Source: http://www.homelandsecuritynewswire.com/dr20190523-earthquakes-or-tiger-attacks-understanding-what-people-fear-most-can-help-prevent-disasters

May 23 - It's been more than four years since a magnitude 7.8 earthquake devastated Nepalese cities, claiming thousands of lives. Since then, there have been thousands of aftershocks. Yet when I spoke with residents of Bharatpur – Nepal's fourth largest city – as part of my ongoing research, beginning in 2014, I was surprised to discover they were more concerned about wild animal attacks than the prospect of another high-magnitude quake.

Understanding what people worry about is crucial to preparing for natural hazards such as earthquakes and mitigating their effects. To prevent disasters, local people, municipal authorities and national governments all need to pull in the same direction – especially when budgets are low for disaster planning. But if residents feel that their everyday fears are ignored by those in power, they may disengage, leaving authorities unable to influence their behavior in a time of crisis.

Throughout my research into the way cities are governed, I have investigated what people worry about, how they cope, how they raise their concerns and what role local authorities play in addressing them. I have consistently found that people tend not to worry about things they cannot prevent or control. And so far, local and national governments haven't done a good job of recognizing this.

A world of worries

Residents of Bharatpur (which has a population of 300,000) did not worry about earthquakes. The fact is, their everyday experiences and relationships are difficult and filled with tension – so they're more concerned with immediate dangers and changes than with the indistinct threat of a natural hazard.

For example, the residents I spoke to were worried about wild animals – specifically tigers and rhinos – attacking people in the forest as they gathered firewood for their homes. This is a real threat: when I visited Bharatpur in 2017, I discovered that earlier in the year there had been a deadly tiger attack in broad daylight on the same dirt road where I had interviewed participants for my PhD research in 2014/15.

Residents also worried about changes to municipal boundaries that will affect their access to government services. Administrative changes in the city have led to a reallocation of funding from rapidly urbanising areas to the rural parts of the city, which lack the most basic infrastructure (electricity and paved roads).

What's more, the local authority is raising taxes in 2019, which leaves those with very little money struggling to pay for services that were free before, on top of feeding their families and paying for school uniforms.

Yet policy makers and government officials at all levels ignore or discount residents' fears about wild animal attacks, reallocation of municipal funding and the prospect of increasing taxes, when deciding what risks to address in their cities. Local authorities are more focused on paving roads throughout the city – a visible improvement which shows they are "doing something" – rather than addressing the full continuum of urban risk.

It's important to note that there is nothing natural about disasters. Natural hazards such as earthquakes, tsunamis and volcanic eruptions happen frequently around the world. But disasters only occur when people are left exposed and vulnerable to natural hazards – which should be mitigated through safer building, better planning and preparation.

By ignoring residents' everyday fears, governments risk losing their trust, which could increase the risk of disaster as residents disengage from government initiatives aimed at mitigating natural hazards.

Listen and learn

In a new paper, due to be published as part of the 2019 United Nations' global assessment report for disaster risk reduction, I explain why it's crucial to listen and include the views of

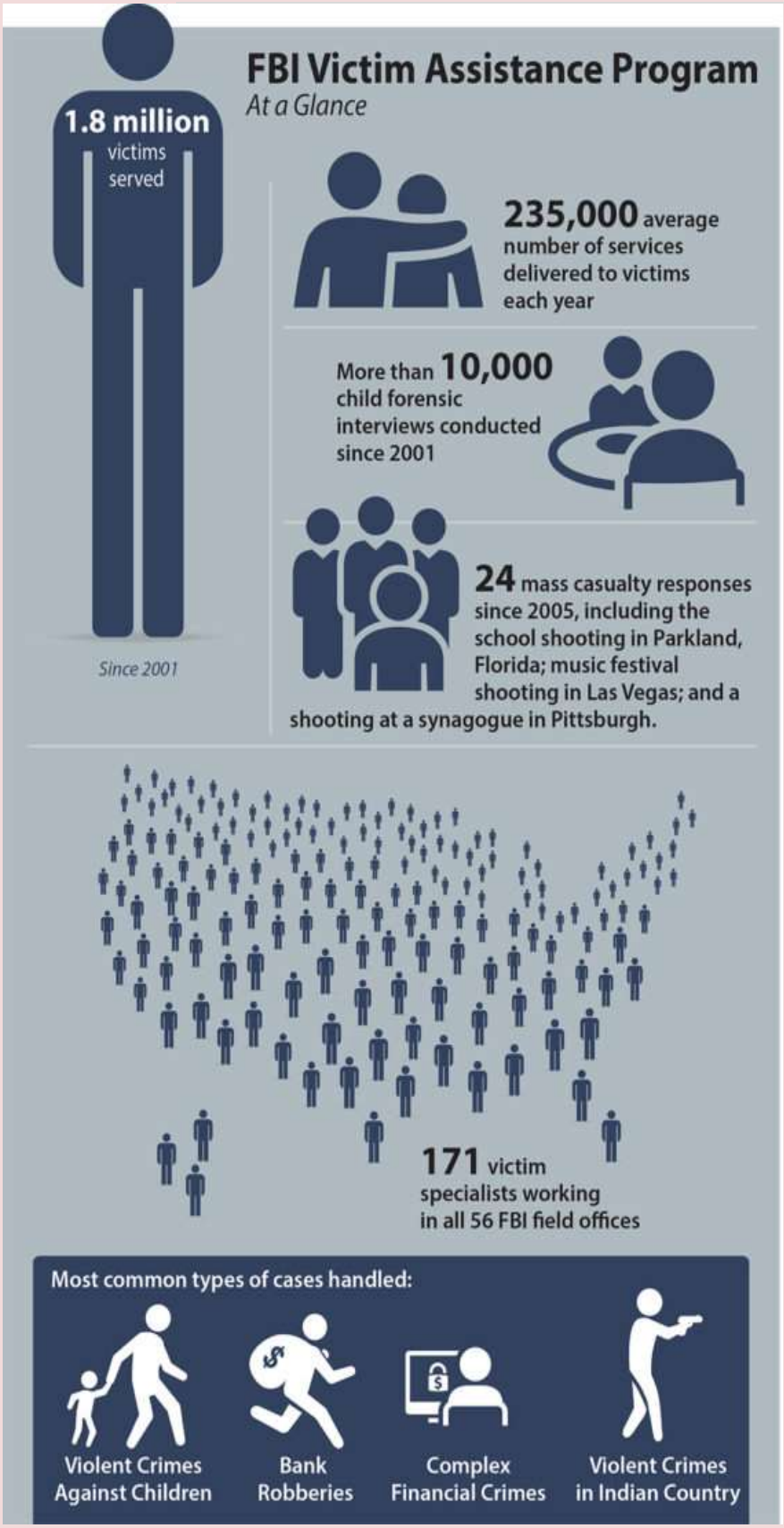
residents and local authorities when national governments, donors and United Nations agencies think about how to manage risk in cities.
Local authorities are on the front line and are increasingly responsible for managing the full range of urban risks and hazards – from the economic precarity that forces young Nepali men to work abroad, to environmental degradation including lack of sewage treatment and rapid urbanization which leads to fertile agricultural land being built on. And the list continues.
Recognizing this wider range of risks is important for global conversations taking place between national governments and United Nations organizations. How these leaders define risk can decide how governments act on an international, national and even municipal level.
What's more, if local people's perceptions of risk are not included in national policy decisions, this shape and actually limits what risks are actually managed locally. This leads to people's worries being left ignored and unaddressed – and they become disenchanted and disengaged.
According to the United Nations, we are now living in an urban world, so we should all make the effort to better understand the complexity of challenges facing cities, and the continuum of risks in Nepal and all the other fast-urbanizing places in the world. This includes listening to cities' residents.

***Hanna Ruszczyk** is Assistant Professor, Durham University.*

A Rapid Deployment Team for Mass Casualty Victims

Source: https://cbrnecentral.com/a-rapid-deployment-team-for-victims/18149/

Apr 09 – When the special agent leading the FBI's response to a church shooting in Sutherland Springs, Texas, arrived on the scene in 2017 to join local police in assessing the crisis—in which a gunman killed 26 people before being shot dead—he made quick determinations about which FBI assets to deploy.
Special agent bomb technicians and evidence response teams from the FBI's San Antonio Field Office were already on scene supporting the Texas Rangers, the state law enforcement agency leading the investigation. Their job was to secure the crime scene, determine what happened, and collect evidence to support the investigation. And victim specialists from the nearest FBI office were already beginning to coordinate with local agencies in the rural area to support the victims and their families.
But it was quickly evident after the November 5, 2017, shooting that the sheer magnitude of the incident would require a surge of resources to assist survivors, witnesses, and the families of the injured and deceased. So Christopher Combs, the special agent in charge of the San Antonio FBI, called up what he described as one of the Bureau's key "crisis assets"—the Victim Services Response Team (VSRT), a specially trained cadre of FBI personnel whose primary function is to address the needs of victims in mass casualty events.
The FBI's VSRT, which includes victim specialists, agents, and analysts from around the country, was established in 2005 to provide support for victims in large-scale events. Team members generally work their regular jobs within the Bureau but are on call.
Once on the ground for a deployment, the team engages with victims and families to assess their immediate needs and provides crisis intervention and other forms of emergency assistance. They work with local agencies to staff family assistance centers and support victims during investigative interviews. VSRT members also work closely with the Bureau's Evidence Response Teams (ERTs) to collect, manage, clean, and return personal effects—items not considered evidence—collected from crime scenes.
"They're as important to the active shooter response for the Bureau as the ERTs," said Combs. He said the VSRT presence in Sutherland Springs meant his trained agents could focus all their attention on investigating the crime scene while a similarly trained team attended entirely to the victims. "To have a team that's so specialized, I knew that they had just taken that entire piece off the table and were going to handle that for me," Combs said.
The FBI's Victim Services Division (VSD) manages the VSRT program and provides specialized training for team members, who serve three-year terms and are on call for a month at a time. Each deployment team includes a mix of victim specialists, agents, and analysts; the size of the team depends on the scope of the mass casualty event. The mass



shooting in Las Vegas in October 2017, for example, required an unprecedented response because of the large number of victims, including 59 killed and more than 850 injured. Additionally, VSRT works with local agencies to reach out to people who were present but not injured at mass casualty events. They may be eligible to receive services, including counseling, and might also have information that can assist an investigation.

Since its inception in 2005 as the Victim Assistance Rapid Deployment Team, VSRT has responded to 24 mass casualty events, including the Boston Marathon bombing in 2013, the Pulse nightclub shooting in 2016, and the San Bernardino shooting in California in 2015. The team's most recent response was last November, when 13 people were killed at the Borderline Bar and Grill in Thousand Oaks, California.

Aaron Rouse, special agent in charge of the FBI's Las Vegas Field Office, said having an experienced team focused on serving victims—and all the logistics that entails—is a valuable component to an FBI response. The shooting on the Las Vegas strip occurred during a crowded outdoor concert, which led not only to a large number of casualties but also an enormous collection of personal effects that were left behind when people scrambled for safety. VSRT members worked with evidence collection teams to identify thousands of hats, phones, boots, chairs, and other personal items and match them with their owners.

"They understand better than most departments what's going to have to be laid out in order for the victims to get the proper assistance," Rouse said. "What they learned from Las Vegas was an evolution from the Pulse nightclub, from the Boston bombing, from San Bernardino. And in each one of these cases, we're pushing envelopes that we didn't push before. And we're getting a better understanding of what is it going to take to get a large group of people through this event."

No Paw Left Behind: Include Pets' Needs in Your Disaster Plan

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/no-paw-left-behind-include-pets-needs-in-your-disaster-plan/

June 14 – Planning for hurricane season means planning for all members of your family, including those who can't plan for themselves. Don't put yourself in a bad situation by forgetting to prepare for your pets' needs.

Make sure you're ready for natural disasters by following these steps:

1. **Build an emergency kit.** Include at least a three-day supply of food and water as well as medications, medical records, registration papers, a pet first aid kit (include a pet first aid book), collar or harness with ID tag, leash, crate or pet carrier, picture of you and your pet together, and sanitation items like litter, paper towels and garbage bags. Your pet will also appreciate familiar items to reduce stress, like treats, toys, bedding and a calming shirt. Use the checklist at https://go.usa.gov/xmFDP to help build your emergency kit.
2. **Identify shelters.** Many emergency shelters will not accept pets. Consider whether family or friends can take in your pets in an emergency instead. Also look for hotels that allow pets and find kennels or other boarding facilities near your likely shelter.
3. **Use the buddy system.** In case you're not home when disaster strikes, arrange for a trusted neighbor to care for your pets.
4. **Know how to find them.** In case you lose track of a pet, write down the phone numbers for the local humane society and animal welfare organizations, your county animal response team and the National Animal Rescue and Sheltering Coalition. You may also want to consider a permanent identification method such as microchipping.

If you must leave your pets behind in an emergency, never leave them chained outside.

To learn more about preparing for natural disasters with pets, visit www.ready.gov/caring-animals or www.listo.gov/es/cuidado-de-los-animales for Spanish.

The First Hour: Social Media in Crisis Communication

By Vivian Marinelli

DRJ Fall 2019

Source: https://www.drj.com/fall2019/index.php/blog-footer/149-speaker-spotlight-vivian-marinelli?source=F19-Crisis

Dr. Vivian Marinelli's passion comes from experiencing the resiliency of people, organizations and communities when they are provided the basic support necessary to recover and restore their own support systems. This support begins with basic information about who was or was not involved in a particular situation.

"The impact of the crisis on family members, friends and colleagues is the next information needed," she says. "This two-way communication and sharing of information are paramount

during a crisis both at the organizational and individual levels to help to decrease the level of anxiety and distress that is experienced."

According to Marinelli, disaster recovery for the organization also relies on their ability to communicate information and updates to their stakeholders as the response evolves.

Marinelli is senior director of Crisis Management Services, FEI Behavioral Health. She has been in her current position for 11 years and in the business continuity and disaster recovery profession for 20 years. She presents "The First Hour: Social Media in Crisis Communications" at DRJ Fall 2019 in Phoenix.

As a psychologist, Marinelli's focus is on the effects of trauma and the recovery of individuals, families and communities. She initially began consulting with FEI because of their work supporting mass casualty events. The first situation involved an all-fatal aviation crash with 217 passengers. The consultation involved support of the families of the victims as well as the airline staff and operations. Since that initial response, Marinelli has been involved in numerous mass casualty events including the terrorist attacks of 9/11.

During her presentation, Marinelli will discuss about what happens when a crisis occurs. Individuals who need information extends beyond those directly impacted. However, emergency response teams may be so focused on managing the situation that they fail to effectively communicate with internal and external audiences and track public relations.

"A lack of communication from an organization during a crisis can lead to both potential brand reputation damage, and safety concerns," says Marinelli. "Effective social media management is vital to controlling the validity of information being shared as well as any potential fallout."

Marinelli will include a question-and-answer session in her presentation and share information with real-life examples.

One "insider tip" she plans to share with attendees is how a crisis communication plan needs to include guidance on postings for personal social media accounts for employees and staff.

"Your crisis communications plan needs an annual checkup and stress test to be in the best shape possible and ready to respond."

Marinelli also says a crisis communications plan should include social media monitoring or listening well past the initial crisis response. "I will share a crisis response situation which appeared to be resolved successfully. However, social media monitoring revealed otherwise."

In her position as senior director of crisis management services, Marinelli is responsible for leading and directing a full complement of emergency support services for her clients which include universities, government agencies, airlines, hospitality, entertainment, and corporate entities. The services include review of existing emergency response and family assistance plans to ensure operational feasibility as well as consultation on emergency preparedness, crisis response, family assistance, and crisis communication in accordance with industry requirements, company policies and procedures, and best practices from lessons learned from previous responses.

In addition, Marinelli oversees the internal and external FEI Crisis Support Team and has been the principal architect in designing, developing, and training a highly successful team of specialists focused on supporting the critical needs of individuals, families, and communities during disasters.

Marinelli is recognized as a subject matter expert in academic, corporate, and government emergency response and has traveled the world to deliver trainings to her clients and communities Working with people and effective communication are vital as her role as a consultant and crisis responder. She has responded to multiple mass casualty events of both natural and man-made in nature. She has provided support to the families and individuals directly impacted by multiple aviation disasters, terrorist attacks of 9/11, hotel bombings in Islamabad and Jakarta, Boston Marathon bombings, and the attack in Nice. Her responses to natural disaster incidents include Hurricanes Katrina, Rita, Irma, Maria, and Superstorm Sandy. More recently, she has been providing support on crisis communication response including development of press releases and media response during a crisis.

Marinelli has presented at numerous conferences including the National Center for Spectator Sport Safety and Security, Campus Safety Conference, NFL Security Conference, and Inaugural Conference for College and University Safety and Security. She has been a panelist at the McKenna Long & Aldridge LLP Airline Symposium and the Regional Aviation Association. She holds a doctoral degree in clinical psychology.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
ASYMMETRIC
THREATS

As global temperatures climb, risk of armed conflict likely to increase substantially

Source: http://www.homelandsecuritynewswire.com/dr20190620-as-global-temperatures-climb-risk-of-armed-conflict-likely-to-increase-substantially

June 20 – As global temperatures climb, the risk of armed conflict is expected to increase substantially, according to experts across several fields. Synthesizing views across experts, the study estimates climate has influenced between 3 percent and 20 percent of armed conflict risk over the last century and that the influence will likely increase dramatically.

Intensifying climate change will increase the future risk of violent armed conflict within countries, according to a study published today in the journal *Nature*. Synthesizing views across experts, the study estimates climate has influenced between 3 percent and 20 percent of armed conflict risk over the last century and that the influence will likely increase dramatically.

In a scenario with 4 degrees Celsius of warming (approximately the path we're on if societies do not substantially reduce emissions of heat-trapping gases), the influence of climate on conflicts would increase more than five times, leaping to a 2 percent chance of a substantial increase in conflict risk, according to the study. Even in a scenario of 2 degrees Celsius of warming beyond preindustrial levels – the stated goal of the Paris Climate Agreement – the influence of climate on conflicts would more than double, rising to a 13 percent chance.

"Appreciating the role of climate change and its security impacts is important not only for understanding the social costs of our continuing heat-trapping emissions, but for prioritizing responses, which could include aid and cooperation," said Katharine Mach, director of the Stanford Environment Assessment Facilityand the study's lead author. Mach is also a senior research scientist in Earth system science.

Climate change-driven extreme weather and related disasters can damage economies, lower farming and livestock production and intensify inequality among social groups. These factors, when combined with other drivers of conflict, may increase risks of violence.

"Knowing whether environmental or climatic changes are important for explaining conflict has implications for what we can do to reduce the likelihood of future conflict, as well as for how to make well-informed decisions about how aggressively we should mitigate future climate change," said Marshall Burke, assistant professor of Earth system science and a co-author on the study.Burke is also a center fellow at the Freeman Spogli Institute for International Studies.

Finding consensus

Stanford notes that researchers disagree intensely as to whether climate plays a role in triggering civil wars and other armed conflicts. To better understand the impact of climate, the analysis involved interviews with and debates among experts in political science, environmental science, economics and other fields who have come to different conclusions on climate's influence on conflict in the past.

The experts, who also served as co-authors on the study, agree that climate has affected organized armed conflict in recent decades. However, they make clear that other factors, such as low socioeconomic development, the strength of government, inequalities in societies, and a recent history of violent conflict have a much heavier impact on conflict within countries.

The researchers don't fully understand how climate affects conflict and under what conditions. The consequences of future climate change will likely be different from historical climate disruptions because societies will be forced to grapple with unprecedented conditions that go beyond known experience and what they may be capable of adapting to.

"Historically, levels of armed conflict over time have been heavily influenced by shocks to, and changes in, international relations among states and in their domestic political systems," said James Fearon, professor of political science and co-author on the study. "It is quite likely that over this century, unprecedented climate change is going to have significant impacts on both, but it is extremely hard to anticipate whether the political changes related to climate change will have big effects on armed conflict in turn. So I think putting nontrivial weight on significant climate effects on conflict is reasonable."

Planning ahead

Reducing conflict risk and preparing for a changing climate can be a win–win approach. The study explains that adaptation strategies, such as crop insurance, post-harvest storage, training services and other measures, can increase food security and diversify economic opportunities, thereby reducing potential climate–conflict linkages. Peacekeeping, conflict mediation and post-conflict aid operations could incorporate climate into their risk reduction strategies by looking at ways climatic hazards may exacerbate violent conflict in the future.

However, the researchers make clear there is a need to increase understanding of these strategies' effectiveness and potential for adverse side effects. For example, food export bans following crop failures can increase instability elsewhere.

"Understanding the multifaceted ways that climate may interact with known drivers of conflict is really critical for putting investments in the right place, "Mach said.

— Read more in Katharine J. Mach et al., "Climate as a risk factor for armed conflict," Nature *(12 June 2019).*