HZS
CBRNE DIARY
Dedicated to Global First Responders
January 2021
01\21

A HOTZONE SOLUTIONS GROUP PUBLICATION


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
HOTZONE
SOLUTIONS
GROUP
C2BRNE
DIARY
DIRTY R-NEWS

Medical Management of Radiation Emergencies: REAC/TS Launches New RadMed App

Source: https://cbrnecentral.com/medical-management-of-radiation-emergencies-reac-ts-launches-new-radmed-app/25465/

Oct 2020 – The Oak Ridge Institute for Science and Education (ORISE) Radiation Emergency Assistance Center/Training Site (REAC/TS) has launched a new RadMed app, providing a wide range of resources on the medical management of radiation incidents that can be downloaded free on mobile devices and utilized while on the go.

The REAC/TS RadMed App includes:

- Updated eGuide for The Medical Aspects of Radiation Incidents, 5th edition
- Basic health physics and dose estimation (US and SI Units)
- Treatment of whole body and acute local radiological illnesses and injuries
- Assessment and treatment of internal contamination with radioactive materials
- Patient decontamination
- Delayed effects of exposure to ionizing radiation
- Risk and psychological issues
- Dicentric chromosome assay (DCA)
- State, federal and international resource database
- Assessment tools for radiation incident preparedness
- REAC/TS courses
- REAC/TS videos
- Real-Time REAC/TS news
- Links to partner resources

"The REAC/TS RadMed app offers healthcare professionals, emergency responders and planners, public health professionals and health physicists' easy access to essential medical information and resources when dealin g with a radiation incident," said REAC/TS Director Carol Iddins. "We created the RadMed app with our target audiences in mind to provide easy access to the resources they need."

Visit the RadMed page to learn more about the RadMed app, and download it for free by searching for REAC/TS RadMed in the Apple and Android app stores.

Israel Warns Iran About Uranium Enrichment Announcement

Source: http://www.homelandsecuritynewswire.com/dr20210105-israel-warns-iran-about-uranium-enrichment-announcement

Jan 05 – Israeli officials said Monday that they will not allow Iran to produce a nuclear weapon. Israel was responding to Iran's announcement that its scientists have resumed enriching uranium to 20 percent purity. The exchange is increasing tensions just two weeks before U.S. President-elect Joe Biden is set to take office.

Iran's state-run news agency quoted a government spokesman as saying that Iranian President Hassan Rouhani had given the order to resume enriching uranium to 20 percent purity at the underground Fordo facility.

The move is seen as a significant step toward achieving weapons grade levels of uranium. In the 2015 nuclear deal, Iran agreed not to go above four percent.

Israeli Prime Minister Benjamin Netanyahu said the Iranian decision shows that Iran is seeking nuclear weapons despite its denials and that Israel would not allow this to happen.

Giora Eiland, the former head of Israel's National Security Council, said the move is a significant step forward for Iran in its quest to become a nuclear power.

"As far as we know today, the beginning of 2021, they do not have a nuclear bomb although they have actually all the access and all the potential to have it, if they make a decision to try to get it in a period of less than six months or less than a year," said Eiland.

But Eiland said he saw the Iranian announcement more as a way to put pressure on the incoming Biden administration to return to the Iran nuclear deal from which the Trump administration withdrew.

"Today they accelerate very carefully this process in order to create some pressure on the United States in order to be in a better position when the dialogue begins as they believe it will in a matter of a few months," he said.

The Iranian announcement comes one year after the United States' targeted killing of senior Iranian Revolutionary Guard commander Qasem Soleimani, a move Iran has vowed to avenge.
It also comes just two months after senior Iranian nuclear scientist Mohsin Fakrisade was gunned down in Tehran, allegedly by Israel. Analysts like Reza Shayed, a journalist with France 24 based in Tehran, point to a possible link between the Iranian announcement and the killing of Soleimani.
"There's been a lot of talk in Washington in recent days that Iran plans to launch an attack on American interests to memorialize that assassination. There's no evidence that's going to happen but this could be, Iran's move today, of delivering a blow to the Trump administration saying this is the result of your maximum pressure campaign and it could be a way of honoring Qasem Suleimani," he said.
Meanwhile on Monday, Iran seized a South Korean-flagged oil tanker on its way to the United Arab Emirates, saying the ship had violated maritime laws. The move further increased tensions between Iran and Western-allied nations.

EDITOR'S COMMENT: Iran threaten to wipe out Tel Aviv and Jerusalem. I just wonder how can you threat a nuclear country with "simple" missiles? I cannot imagine that Iranian high authorities do not comprehend the day after multiple nuclear attacks in major cities and critical infrastructure including their own nuclear facilities. On the other hand, perhaps Iran is following the example of Turkey that shows the finger to nuclear France and nuclear USA. This is a situation that prevelance of logic is imperative!

Opposition MP urges scrapping Turkey's Akkuyu plant, citing crack in foundation

Source: https://ahvalnews.com/akkuyu/opposition-mp-urges-scrapping-turkeys-akkuyu-plant-citing-crack-foundation

Jan 10 – There is a crack in the cement foundation of the $20 billion nuclear power plant project in Turkey's Mediterranean coastal city of Mersin, opposition lawmaker Ali Mahir Başarır said on Sunday.

Seawater is seeping into the foundation of the plant, which is being built by Russian state nuclear energy agency Rosatom, the Republican People's Party (CHP) lawmaker said on Twitter, where he shared video footage of the alleged crack.
Başarır urged officials to scrap the project, claiming the foundation that will carry the reactor already incurred damage during its construction phase.
Officials broke ground on the Akkuyu power plant in 2018, which is set to be Turkey's first nuclear power station and is due to come online in 2023 - the 100th anniversary of the Republic of Turkey.
But engineers and workers began ringing alarm bells over a potential nuclear disaster soon after its inception, and a group of NGOs filed a lawsuit with a Turkish court demanding for construction to be halted.
"There is a tragedy being established on a foundation that has already cracked twice," Başarır said.

"Our country is being pulled into an irreversible calamity, because the Akkuyu is in an earthquake zone. The foundation is entirely (composed of) water. If there is an earthquake following the construction, the Mediterranean and Mersin will be faced with a tragedy," he added, noting officials should pull the plug on the project "while there is still time."
Turkey and Russia signed a cooperation agreement for the construction of the power plant in 2010 and officials broke ground on the project in 2018.The plant will have four units and is expected to generate around 35 billion kWh per year at full capacity and is expected to meet about 10 percent of Turkey's electricity needs.

The project is set for completion in 2023, Turkey's centennial year.

▶▶ **Watch video:** https://jurnaltr.com/chp-milletvekili-ali-mahir-basarir-akkuyu-nukleer-santralinin-zemini-catladi/

Report estimates Chinese nuclear stockpile at 350 warheads

Source: https://www.defensenews.com/global/asia-pacific/2020/12/14/report-estimateschinese-nuclear-stockpile-at-350-warheads/

Dec 14 – A paper published by the Chicago, Illinois-based Bulletin of the Atomic Scientists has estimated that China has 350 nuclear warheads, significantly more than that estimated by the US Defense Department.

Sweden builds new nuclear power plants in Estonia

Source: https://www.tellerreport.com/news/2020-12-13-%0A---vattenfall-is-building-newnuclear-power-plants-in-estonia%0A--.HkX6vRiX2v.html

Dec 13 – Sweden has decided to close the nuclear power plants on its territory, for environmental safety reasons, and to build new nuclear power plants abroad, which will be operational in ten years.

UNGA: 153 countries called on Israel to 'renounce' nuclear weapons

Source: https://www.middleeastmonitor.com/20201210-unga-153-countries-called-on-israel-to-renounce-nuclear-weapons/

Dec 10 – In a vote held on Monday, the United Nations General Assembly (UNGA) called on Israel to "renounce possession of nuclear weapons," news agencies reported.
A resolution entitled "The Risk of Nuclear Proliferation in the Middle East" had 153 supporting votes against only six who did not support it, with 25 abstentions. The US, Israel's ally, was among the six countries that did not vote for the resolution.
The resolution was part of a large package of resolutions approved by the UNGA related to nuclear disarmament, globally and in the Middle East.
Based on the resolution, the UNGA asked Israel: "Not to develop, produce, test or otherwise acquire nuclear weapons."
In addition, the UNGA called the Israeli occupation state: "To renounce possession of nuclear weapons and to place all its unsafeguarded nuclear facilities under full-scope agency safeguards as an important confidence-building measure among all states of the region and as a step towards enhancing peace and security."
Of the 193 members of the UN, 191 countries are parties of the Treaty on the Non-Proliferation of Nuclear Weapons. Israel has never signed the treaty.
This resolution passed 152-6, with 24 abstentions last year.
On Monday, the UNGA also voted 174-2, with one abstention, on a resolution that called for a nuclear-free zone in the Middle East. Only Israel and the US opposed it, with Cameroon abstaining.

EDITOR'S COMMENT: What a clever proposal! Imagine that you are a country surrounded by enemies and especially one that from time to time declares that will swap your entire nation away. Imagine that you have nuclear weapons and your neighbors do not. Now you can imagine what those in the UNGA doing in order to spend their time and excuse their salaries.

Arab world's first nuclear power plant in Abu Dhabi reaches 100% capacity

Source: https://www.straitstimes.com/world/middle-east/arab-worlds-first-nuclear-power-plant-in-abu-dhabi-reaches-100-capacity

Dec 08 – The United Arab Emirates' Barakah Nuclear Energy Plant has reached 100 per cent of the reactor power capacity for Unit 1 of the facility during testing, the Emirates Nuclear Energy Corporation (ENEC) said in a statement.
The plant in the Al Dhafrah Region of Abu Dhabi, capital of the UAE, is the first nuclear power plant in the Arab world and part of the Gulf oil producer's efforts to diversify its energy mix.
Commercial operations are expected to begin in early 2021, the statement on Monday (Dec 7) said.
Barakah's Unit 1 was connected to the national power grid in August.

"Unit 1 is generating 1,400MW of electricity from a single generator connected to the UAE grid. This milestone makes the Unit 1 generator the largest single source of electricity in the UAE," ENEC said.
When completed Barakah, which is being built by Korea Electric Power Corp, will have four reactors with 5,600 megawatts (MW) of total capacity.
Construction of Unit 3 is 93 per cent complete and Unit 4 is 87 per cent complete. Unit 2 is complete and is awaiting licensing.

Turkey-Pakistan in top-level discussion over nuclear weapon program

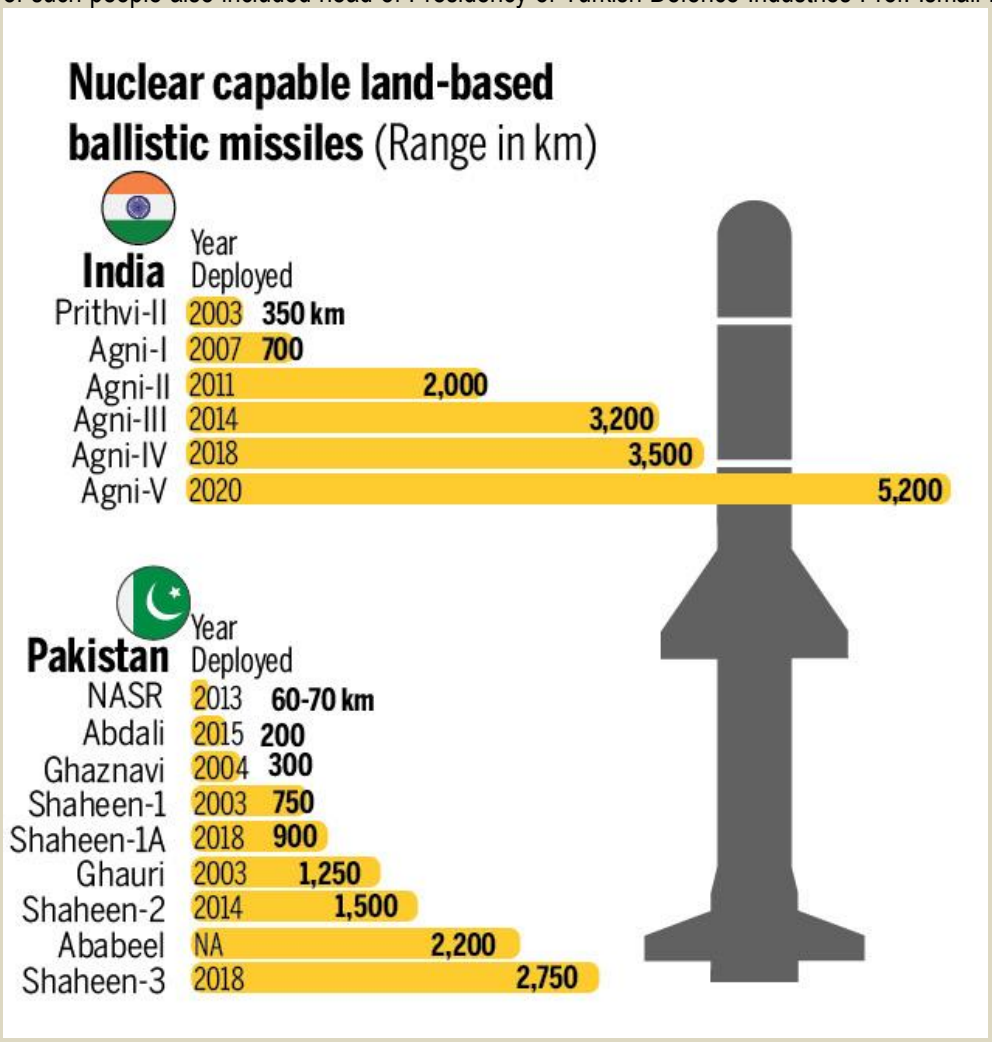
Source: https://zeenews.india.com/world/turkey-pakistan-in-top-level-discussion-over-nuclear-weapon-program-2333996.html

Jan 02 – The rapid production and proliferation of nuclear and missile technologies by Turkey have been a major concern for democratic powers across the world. It has threatened the peace and tranquillity of countries from the North Atlantic to the Middle East. A series of recent developments have attracted the eyes of the world on an emerging phenomenon wherein Turkish President Erdogan is banking on Pakistani nuclear and missile technologies to fulfil his geopolitical aspirations.

The latest development in the series is the 15" Turkey-Pakistan High-Level Military Dialogue Group (HLMDG) on 22-23 December 2020, which is the biggest institutional setup between both the countries on defence cooperation. Pakistan's Defence Secretary Lt. Gen. (Retd.) Mian Muhammad Hilal Hussain led the Pakistani delegation, while Deputy Chief of Turkish Army General Selcuk Bayraktaroglu led the Turkish delegation.
The meeting was part of a series of several meetings between top level representatives of armies of both the nations. The progress made in previous meetings between defence representatives was also reviewed and discussed. Turkish media reported that besides other things, much emphasis was laid on defence industry cooperation including joint production and procurement. Pakistani generals also met Turkish defence minister Hulusi Akar and Chief of Turkish Army General Yasar Guler.
Insiders believe that the meeting and the deliberations discussed during it were just the tip of the iceberg as it is part of a larger screenplay of sharing nuclear and missile technologies between the two countries. It is believed that Erdogan has personally requested Pakistani Army Chief General Bajwa for sharing nuclear weapon technology which Pakistan has

reportedly agreed. The meeting was organised to discuss procedural aspects of the technology transfer that could take place and covering the process at the same time.

The Pakistani defence delegation visited Turkish defence companies including Bakyar (UAV OEM), TAI,HAVELSAN and ASELSAN. It also met top Turkish Army generals and bureaucrats dealing with the production of missiles and other aerial technologies. The list of such people also included head of Presidency of Turkish Defence Industries Prof. Ismail Demir and CEO of Turkish Aerospace Limited (TAI) Dr. Temil Kotil.



The recent seizure of a Chinese autoclave — a device that is used for manufacturing motor of very long - range missiles in Kandla Port from a Hong Kong ship going to Pakistan's Port Qasim underlined the rapid transfer of missile technology from China to Pakistan. Experts argued that the type of autoclave seized is used in very long-range missiles like Shaheen-ll, capable of carrying nuclear warheads. Pakistan has accumulated a large battery of missiles from China — the conventional ones as well as those capable for carrying nuclear warheads. China is also believed to be the country responsible for the transfer of nuclear technology to Pakistan and helping the country to build its nuclear capabilities.

Pakistan is rapidly transferring the missile technologies to Turkey and Pakistani scientists are helping Turkey build its capacity in the production of missiles. Scores of Pakistani scientists are currently working with Turkey to enhance its ballistic and nuclear capabilities. By brokering the transfers of missile technologies between countries and manoeuvring the dynamics of geopolitics, Pakistan has brazenly violated the Missile Technology Control Regime (MTCR) and non-proliferation rules.

Erdogan has been blatantly expressing his nuclear desires through his speeches and comments. Articulating his nuclear aspirations very recently in September 2019, Erdogan stated, “Some countries have missiles with nuclear warheads, not one or two. I, however, am not supposed to have missiles with nuclear warheads. This, I cannot accept... And right next to us , there is Israel, right? With everything, it is frightening."

It is pertinent to note that for decades, Pakistan has been a kingpin of the ‘nuclear black market and Turkey has been contributing to Pakistan’s business. Giving a jolt to nuclear non-proliferation, the nuclear black market of Pakistan led by Abdul Qadeer Khan helped numerous countries in sharing missile technologies, especially in the production of centrifuges. According to the International Institute of Strategic Strategic Studies, Turkish companies helped the gangster of Pakistan indulge in the business of nuclear technologies to covertly import materials from Europe and export the finished products to players like Libya, Iran and North Korea . Several media reports have also highlighted that Turkey might be possessing a considerable number of centrifuges made by Pakistan.

The next meeting of HLMDG is scheduled in 2021 and insiders have revealed that both the countries have set these targets to be achieved before the next meeting: fast tracking of missile technology transfer, capacity building of Turkey in producing centrifuges, purchase of small armed Turkish drones by Pakistan, acquisition on high-range Turkish mini drones by Pakistani Army.

In another important development, Lt. Gen. Sahir Shamshad of Pakistani Army met Lt. Gen. Wali Turkchi of Turkish Army in Ankara for the Second Round of Turkish-Pakistani Military

Talks on December 21st, a day ahead of the HLMDG. Besides HLMDG, Turkish-Pakistani Army Military Talks is another important institutional arrangement between both the countries dedicated to defence cooperation and transfer of defence technologies. The transfer of missile technologies and UAVs was the central theme of this meeting as well. It is also believed that Pakistan assured Turkey of helping it to find new buyers of Turkish defence equipment after recent CAATSA (Countering America's Adversaries Through Sanctions Act) sanctions imposed by the US. Turkey is afraid of losing its defence market after these impositions and has sought Pakistan's assistance.

Scholars argue that Erdogan sees Pakistani nuclear and missile capabilities as an important weapon in achieving his caliphate aspirations. The blatant transfer of defence technologies and equipment between both countries is now increasingly threatening the peaceful world order. However, these transactions have irked the western powers along with the Saudi-led countries which now are hurriedly dissociating from Pakistan and are planning to take action against it, making Pakistan a 'pariah' in the Islamic world.

EDITOR'S COMMENT: There will be one day (soon) that Turkey will say: "Surprise! We also have nuclear weapons!" And when this happens, it would be too late to take measures or act. Turkey will automatically become a member of the nuclear club and others (in the neighborhood) will follow and this is how the WWIII will be ignited. Big powers are currently too busy with their own problems, ambitions and goals to be pro-active. Also, keep in mind that a weapon is good enough if you are willing to use it. So far, Turkey have shown that nukes do not really pose a threat to its bullying behavior in SE Mediterranean Sea. Just mark the date [Jan 25, 2021] … In addition, note the last line of this article: "… making Pakistan a pariah in the Islamic world." A nuclear pariah though!

Houses damaged in 'controlled explosion' at Akkuyu Nuclear Power Plant construction site

Source: https://www.duvarenglish.com/houses-greenhouses-damaged-in-controlled-explosion-at-akkuyu-nuclear-power-plant-construction-site-says-turkeys-mersin-governors-office-news-55927

Jan 19 – Several houses (~85) and greenhouses in the southern Mersin province have been damaged following a "controlled explosion" at the Akkuyu Nuclear Power Plant construction site, said the local governor's office in a statement on Jan. 19. The statement came after CHP MP Ali Mahir Başarır announced the explosion on social media, saying locals were in panic. A team from the police forces had been assigned to investigate the explosion. "The incident will be investigated in all aspects and the necessary procedures will be undertaken with regards to those who are responsible," a statement read.

EDITOR'S COMMENT: If this was a "controlled" explosion one can imagine what an "uncontrolled" explosion will cause. And if it was a controlled incident what is the police involvement for? Any connection with phantom explosions in Iranian industrial/nuclear sites? Because all dots are connected in this life!

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

Nashville's Big Bomb Was a Very Rare Device, Experts Think

Source: https://news.yahoo.com/nashville-big-bomb-very-rare-173704563.html

Jan 01 – Find his test sites, top bomb experts say.

Anthony Quinn Warner's device, although probably made of common over-the-counter components, is unique in the annals of mayhem, according to seasoned FBI bomb experts consulted by *SpyTalk*.

"We've never seen an **improvised thermobaric device** before in this country or any country," says Dave Williams, who conducted

the FBI's on-scene investigations of the World Trade Center, Oklahoma City, Pan Am 103 and Unabomber bombings, among other notorious incidents. Thermobaric refers to a gaseous fuel-air explosion.

"The reason is, it's very difficult to get the timing down to get an optimum mixture of air and a liquified carbonaceous fuel such as propane, methane, acetylene or natural gas," Williams told *SpyTalk*. "He couldn't have done it the first time and made it work. There had to be a test area."

Accidental thermobaric explosions are not uncommon—for example, when a house explodes because of a natural gas leak. But IED-makers haven't tried to stage them deliberately, up to now, Williams says, because too many things have to go right.

That's why investigators must be eager to locate Warner's proving ground, and also any internet sources he studied as he was building a timer and ignition mechanism that enabled him to blow up a Nashville city block, and himself, at 6:30 a.m. on Christmas Day.

As several news outlets have reported, on Aug. 21, 2019, Warner's ex-girlfriend and her lawyer alerted Nashville police that Warner was "building bombs in the RV trailer" on his property and "frequently talks about the military and bomb-making." The police referred the incident to the FBI, according to the reports, but neither agency obtained a search warrant to investigate the premises. The police report of the charges leveled by the ex-girlfriend and lawyer contains no hint of Warner's evident mastery of bomb-making and related electronics.

Williams' hypothesis, that Warner's RV bomb was likely thermobaric, also known as a fuel-air explosive, aerosol bomb or vacuum bomb, is based on videos of the yellow-orange fireball, the pattern of destruction and conversations with other experts in the tight network of bomb investigators aware of the ongoing investigation in Nashville.

Smokeless firebomb

Significantly, the videos show very little smoke from the bomb itself, which suggests the explosion was very efficient. Black smoke came later, from secondary blazes such as

burning tires. To Williams' eye, the videos and photos of wreckage indicate a slow-moving explosion and a type of rolling and heaving also consistent with a relatively slow, homemade device.
At the FBI, where he spent 27 years as a bomb technician, and now, as a consultant on bomb technology, IED countermeasures and structural vulnerabilities, Williams is known for his ability to look at a bombing scene and form a reasonable hypothesis to guide evidence collection and interviews. It's a technique not without controversy: In the 1995 Oklahoma bombing case, a Justice Department Inspector General report criticized Williams' initial assessment as unscientific because, among other things, he offered it before waiting for all the scientific data to come in.
But, as I wrote in my 1998 book, *No Heroes – Inside the FBI's Secret Counter-Terror Force* (with co-author Danny Coulson, an FBI special agent who led the evidence collection in Oklahoma City), investigators on the ground didn't have the luxury of time to compile the forensic data on explosive residues and fragments. They were racing to find the bomber and possible accomplices who might have been planning more attacks. My own investigation determined that the IG report misstated some facts and that Williams' first-look estimate—that the bomb was roughly 4,000 pounds of ammonium nitrate fertilizer and fuel oil—turned out to be uncannily accurate. FBI agents later got hold of sales records showing that Timothy McVeigh bought exactly 4,000 pounds of ammonium nitrate from a farm co-op in Kansas. McVeigh was eventually convicted of the bombing and executed.
If Williams is right now about a fuel-air bomb, he figures Warner would have exercised considerable skill and preparation. The first step would be simple enough: crack open the valves of a tank of some kind of fuel and wait for the RV to fill with an aerosolized gas-air mix.
But the mix wouldn't explode by itself. An ignition source would have to have been introduced at precisely the right moment.
A bomber determined to die inside the van might anticipate that he would likely pass out from lack of oxygen before he could detonate the gas with a cigarette lighter. He'd have to set up a device to detonate automatically. It could be as simple as a baggie of black powder, available at hobby shops, wired to an electrical component, for instance, a switch that makes a microwave or dishwasher ding when its cycle is done, or a telephone alarm.

Timing is everything

The trick would be timing the ignition with exquisite precision to detonate the aerosolized gas-air mix at its richest, when it reached maximum destructive power. That moment would depend on the type of gas and altitude.
All this argues for skill, study and hands-on practice through trial and error. The FBI playbook is straightforward: Retrace Warner's steps and build a timeline. Search highway tolls and gasoline purchase via his credit cards. Map out the towers his cellphone pinged as he moved around the countryside. Interview residents near where he stayed and ask about noise, brush fires and other indications of explosive testing. According to Nashville radio station WKRN, quoting law enforcement sources, Warner had spent time in a state park near Nashville, claiming he was hunting "lizard people." If that state park or any other rural area Warner visited has patches of burned-out foliage, the investigators will almost certainly test for residues.
As the crime scene investigators recover components, they should be running a computer search of big box stores, looking for items that were purchased in specific combinations. They should be checking Warner's credit card purchases for such items. If Warner used gas tanks, shards will still be there. At the scene of the World Trade Center bombing in 1993, Williams and his team found the remains of all three hydrogen tanks used to enhance the explosion. (The IED itself was not thermobaric; its explosive core was urea nitrate or nitrourea, apparently homemade.) The FBI will need to interview gas-supply houses for unusual purchases, if it hasn't already.
Other, as yet unidentified substances may have been incorporated into the RV bomb, to trigger or enhance it.
"Unfortunately, it is only too easy to build an explosive," says a retired senior FBI agent and bomb expert who asked not to be named because he prefers to stay out of the media spotlight. He spent three decades working on the 1998 U.S. embassy bombings by Al Qaeda in Africa, multiple bombing scenes in the Middle East, the attacks of Sept. 11, 2001, the anthrax attacks and many other cases.
"You need either nitrates or peroxide for the majority of homemade explosives. Both are readily available. Nitrates from fertilizer or even from those instant ice packs you can buy at any pharmacy," he tells *SpyTalk*. "Those white prills [pellets] inside the packs contain the nitrates. The U.S. government watches suspicious purchases, but if you keep your purchases under certain amounts, no one notices. Also if you have a business (or letterhead!) that purportedly uses that ingredient, then it's easy to escape notice."
"The trick isn't finding something that will go boom," he adds. "It's setting it off. The detonator—a person with electrical skills could easily build one with a little help from the internet. You used to have to find paper manuals, but today it's right online—most with a 'how to' video showing step-by-step guidelines."
This former FBI official finds Williams' theory positing an unprecedented fuel-air IED "very plausible."

Tinker tailored

"We know he 'tinkered' on his RV for a long time so he would be able to easily seal it tight to allow any gas to accumulate," he says. "He had more than enough electrical expertise to construct a timer and initiator that would function when he passed out."

"I think the only way to prove it for sure will be through chemical analysis of any charred remains in the pieces of the RV they recover," he added. "Most RV campers have propane-fueled stoves and heaters, so the mere presence of a propane tank or some trace of propane wouldn't be definitive for a fuel-air device. However, any other type of gas or multiple tanks would be one of the things they are looking for. The visual of the explosion sounds like a fuel-air device, but to confirm it, they will have to do a frame-by-frame examination of all video and a gas chromatography—mass spectrometry analysis of any of the residues."

In the aftermath of the 9/11 attacks, FBI bomb techs played out scenarios that involved fuel-air explosive devices.

"We always worried that someone would attack a hospital with a large truck bomb parked immediately adjacent to a hospital oxygen tank farm," the ex-FBI bomb tech tells *SpyTalk*.

"Most hospitals have very, very large tank containers of oxygen under pressure stored outside. Most are near the back side of these buildings adjacent to loading dock facilities. Perfect for a large truck bomb to easily access. Most of these tanks are only secured by a chain-link fence and $2 padlock," he says. "When we first began looking into this problem, the majority of these sites didn't even have CCTV coverage and no alarms. A real nightmare scenario."

With all the potentially explosive material on the open market, it's surprising to the bomb tech community that more bombings haven't been attempted.

"We have hundreds, if not thousands of people in this country, who could easily build bombs and have a strong enough grudge, hatred or instability to actually carry out a crime, act of terror or revenge," the former FBI agent says.

"Quite frankly, I am surprised that we don't have more acts of violence like this. I honestly believe that because guns are so readily available, they are the method of choice. Explosives take work, effort and precision. Guns don't, so we have mass shootings instead," he adds. "And let's face it, you can buy guns at Wal-Mart and flea markets and out of newspaper want-ads. There is no problem getting them."

Still, there are some individuals with time on their hands and the necessary obsession, compulsion and talent for precision bomb-making.

Tony Warner, it seems, was one of them.

ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Researchers Developed AI That Tells Apart True Conspiracies from Conspiracy Theories

By Timothy R. Tangherlini

Source: https://www.sciencealert.com/an-ai-tool-can-distinguish-between-a-conspiracy-theory-and-a-true-conspiracy

Jan 07 – The audio on the otherwise shaky body camera footage is unusually clear. As police officers search a handcuffed man who moments before had fired a shot inside a pizza parlor, an officer asks him why he was there.

The man says to investigate a pedophile ring. Incredulous, the officer asks again. Another officer chimes in, "Pizzagate. He's talking about Pizzagate."

In that brief, chilling interaction in 2016, it becomes clear that conspiracy theories, long relegated to the fringes of society, had moved into the real world in a very dangerous way.

Conspiracy theories, which have the potential to cause significant harm, have found a welcome home on social media, where forums free from moderation allow like-minded individuals to converse. There they can develop their theories and propose actions to counteract the threats they "uncover."

But how can you tell if an emerging narrative on social media is an unfounded conspiracy theory? It turns out that it's possible to distinguish between conspiracy theories and true conspiracies by using machine learning tools to graph the elements and connections of a narrative. These tools could form the basis of an early warning system to alert authorities to online narratives that pose a threat in the real world.

The culture analytics group at the University of California, which I and Vwani Roychowdhury lead, has developed an automated approach to determining when conversations on social media reflect the telltale signs of conspiracy theorizing.

We have applied these methods successfully to the study of Pizzagate, the COVID-19 pandemic and anti-vaccination movements. We're currently using these methods to study QAnon.

Collaboratively constructed, fast to form

Actual conspiracies are deliberately hidden, real-life actions of people working together for their own malign purposes. In contrast, conspiracy theories are collaboratively constructed and develop in the open.

Conspiracy theories are deliberately complex and reflect an all-encompassing worldview. Instead of trying to explain one thing, a conspiracy theory tries to explain everything, discovering connections across domains of human interaction that are otherwise hidden – mostly because they do not exist.

While the popular image of the conspiracy theorist is of a lone wolf piecing together puzzling connections with photographs and red string, that image no longer applies in the age of social media. Conspiracy theorizing has moved online and is now the end-product of a collective storytelling. The participants work out the parameters of a narrative framework: the people, places and things of a story and their relationships.

The online nature of conspiracy theorizing provides an opportunity for researchers to trace the development of these theories from their origins as a series of often disjointed rumors and story pieces to a comprehensive narrative. For our work, Pizzagate presented the perfect subject.

Pizzagate began to develop in late October 2016 during the runup to the presidential election. Within a month, it was fully formed, with a complete cast of characters drawn from a series of otherwise unlinked domains: Democratic politics, the private lives of the Podesta brothers, casual family dining and satanic pedophilic trafficking.

The connecting narrative thread among these otherwise disparate domains was the fanciful interpretation of the leaked emails of the Democratic National Committee dumped by WikiLeaks in the final week of October 2016.

AI narrative analysis

We developed a model – a set of machine learning tools – that can identify narratives based on sets of people, places and things and their relationships. Machine learning algorithms process large amounts of data to determine the categories of things in the data and then identify which categories particular things belong to.

We analyzed 17,498 posts from April 2016 through February 2018 on the Reddit and 4chan forums where Pizzagate was discussed. The model treats each post as a fragment of a hidden story and sets about to uncover the narrative. The software identifies the people, places and things in the posts and determines which are major elements, which are minor elements and how they're all connected.

The model determines the main layers of the narrative – in the case of Pizzagate, Democratic politics, the Podesta brothers, casual dining, satanism and WikiLeaks – and how the layers come together to form the narrative as a whole.

To ensure that our methods produced accurate output, we compared the narrative framework graph produced by our model with illustrations published in *The New York Times*. Our graph aligned with those illustrations, and also offered finer levels of detail about the people, places and things and their relationships.

Sturdy truth, fragile fiction

To see if we could distinguish between a conspiracy theory and an actual conspiracy, we examined Bridgegate, a political payback operation launched by staff members of Republican Gov. Chris Christie's administration against the Democratic mayor of Fort Lee, New Jersey.

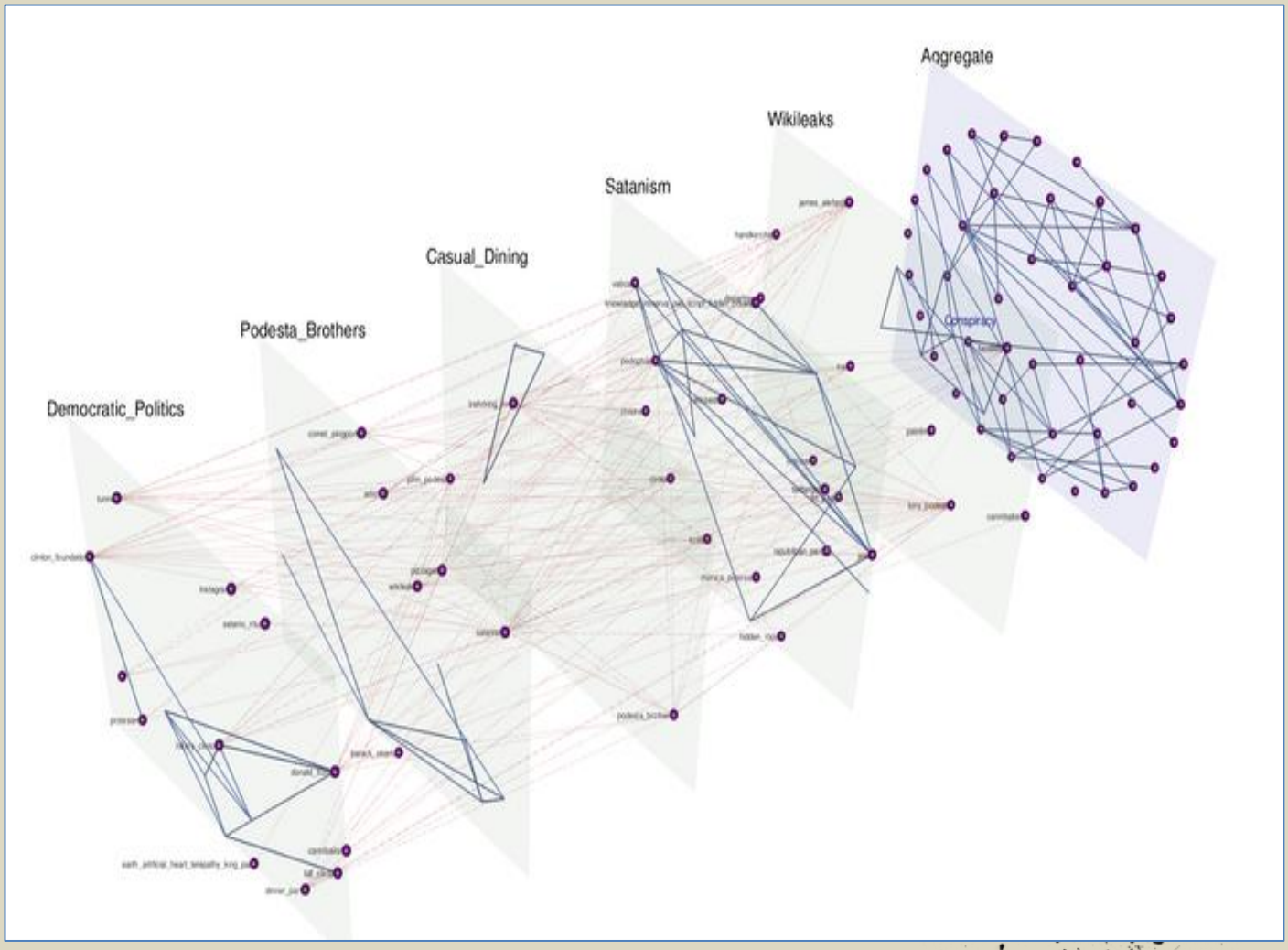
As we compared the results of our machine learning system using the two separate collections, two distinguishing features of a conspiracy theory's narrative framework stood out.

First, while the narrative graph for Bridgegate took from 2013 to 2020 to develop, Pizzagate's graph was fully formed and stable within a month. Second, Bridgegate's graph survived having elements removed, implying that New Jersey politics would continue as a single, connected network even if key figures and relationships from the scandal were deleted.

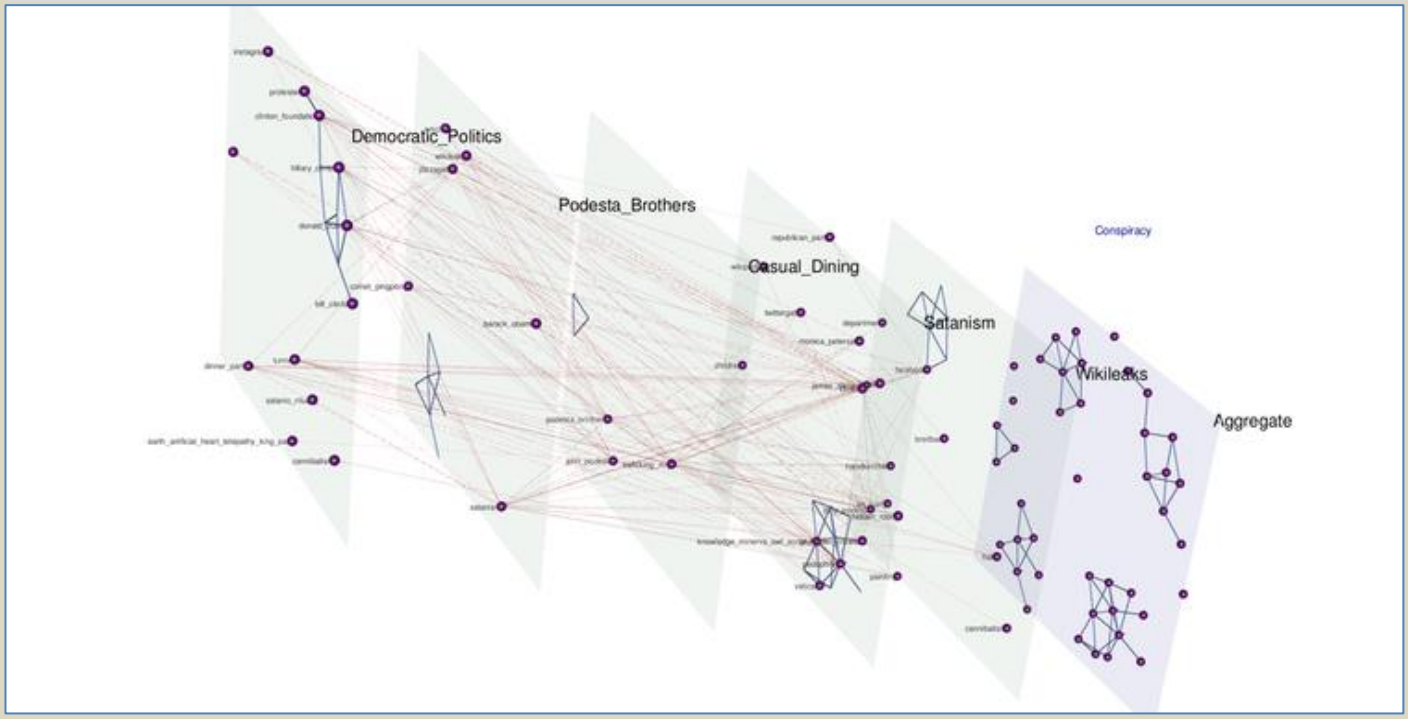
The Pizzagate graph, in contrast, was easily fractured into smaller subgraphs. When we removed the people, places, things and relationships that came directly from the interpretations of the WikiLeaks emails, the graph fell apart into what in reality were the unconnected domains of politics, casual dining, the private lives of the Podestas and the odd world of satanism.

In the illustration below, the green planes are the major layers of the narrative, the dots are the major elements of the narrative, the blue lines are connections among elements within a layer and the red lines are connections among elements across the layers.

The purple plane shows all the layers combined, showing how the dots are all connected. Removing the WikiLeaks plane yields a purple plane with dots connected only in small groups.



Above& below: The layers of the Pizzagate conspiracy theory combine to form a narrative, top right. Remove one layer, the fanciful interpretations of emails released by WikiLeaks, and the whole story falls apart, bottom right.(Tangherlini et al., CC BY 4.0)



Early warning system?

There are clear ethical challenges that our work raises. Our methods, for instance, could be used to generate additional posts to a conspiracy theory discussion that fit the narrative framework at the root of the discussion. Similarly, given any set of domains, someone could use the tool to develop an entirely new conspiracy theory.

However, this weaponization of storytelling is already occurring without automatic methods, as our study of social media forums makes clear. There is a role for the research community to help others understand how that weaponization occurs and to develop tools for people and organizations who protect public safety and democratic institutions.

Developing an early warning system that tracks the emergence and alignment of conspiracy theory narratives could alert researchers – and authorities – to real-world actions people might take based on these narratives.

Perhaps with such a system in place, the arresting officer in the Pizzagate case would not have been baffled by the gunman's response when asked why he'd shown up at a pizza parlor armed with an AR-15 rifle.

Timothy R. Tangherlini *is Professor of Danish Literature and Culture @ University of California, Berkeley.*

Cybersecurity and the Occupation of the Capitol

Source: http://www.homelandsecuritynewswire.com/dr20210107-cybersecurity-and-the-occupation-of-the-capitol

On 6 January, a large number of pro-Trump rioters occupied portions of the U.S. Capitol building to protest and disrupt the counting and certification of electoral votes from the November 2020 election. Herb Lin writes in *Lawfare* that the significance of this event for American democracy, the rule of law, and the depths of extremism in the U.S. populace will be addressed by others, "but I am compelled to point out this siege has created potentially serious cyber risks for Congress and other affected offices."

He adds:

> To any computer security professional, maintaining physical security over computers and other devices is a condition for maintaining cybersecurity. What happens when a threat actor has compromised this essential aspect of cybersecurity? These concerns arose during a conversation with my long-time cyber colleague Eugene Spafford at Purdue University — what devices and computers did the mob physically access during their breach of the countless desks and offices in the Capitol? And how did they use that access? Have listening devices been planted in these offices? Have USB sticks been used to download data from House or Senate computers, or worse, to upload "back doors" that would enable subsequent unauthorized remote access?

To the best of my knowledge, only the Capitol was breached—personal and committee offices in the various House and Senate office buildings remain secure. But members often have offices in the Capitol as well. It is thus a matter of the highest operational priority for those who provide cybersecurity support for the House and Senate to ascertain the nature and extent, if any, of cybersecurity compromises resulting from the occupation. Every office with a computer and every telecommunication closet accessible from public corridors (whether or not behind a locked door) will have to be scanned and swept for malware and additional but unauthorized hardware (e.g., a USB device that is not supposed to be attached that might be used as a covert channel for exfiltrating information).
And it is not only a technical scan and sweep that are necessary—user passwords are often written on sticky Post-it notes; even worse, they are often reused on different computers. House and Senate staff should *immediately* change all passwords on all computers, ensuring of course that they use different passwords for different accounts.

Germany Reviews Parliament Security after U.S. Capitol Riot

Source: http://www.homelandsecuritynewswire.com/dr20210107-germany-reviews-parliament-security-after-u-s-capitol-riot

Jan 07 – The president of Germany's lower legislative house, Wolfgang Schäuble, on Thursday said officials would examine improvements that could be made to parliamentary security in Germany after the storming of the U.S. Capitol building.
Schäuble's office said he would examine "what conclusions should be drawn from this for the protection of the Bundestag," as the lower house is called, in light of the scenes from Washington.
The German government has requested its embassy in Washington provide a report on how the "violent excesses could have happened in the Capitol."
It is expected that the review will involve consultation with the security representatives of the various political parties in parliament, as well as the state of Berlin and the German Interior Ministry.
Chancellor Angela Merkel said the scenes from Washington, D.C. had made her "angry and sad," and that President Donald Trump shared some of the blame for not conceding defeat in last year's presidential elections.
However, the revision of security at the Bundestag is not only prompted by the events in Washington. It also comes after demonstrators against coronavirus restrictions tried to storm Germany's parliament building, the Reichstag, in August. Protesters also breached the building in November, prompting questions about security there.

Cause for Reflection at Home
German Foreign Minister Heiko Maas drew a comparison with the scenes on Wednesday in Washington and the attempts by anti-lockdown demonstrators to enter parliament in Berlin. He also cited deadly far-right terror attacks in the German cities of Halle and Hanau as reasons it would be self-righteous to point the finger at the US without reflecting on matters closer to home.
"Even here, in Hanau, Halle, on the steps of the Reichstag, we have had to experience how agitation and inflammatory words turn into hateful deeds," Maas said.
Maas had also mentioned events at the Reichstag in his initial response to Wednesday night's violence in a tweet that drew a comparison between the two. He said: "Seditious words turn to violent actions — on the steps of the Reichstag, and now in the #Capitol."
Lawmakers from the far-right Alternative for Germany (AfD) party, some of whom had marched in increasingly aggressive virus-skeptic demonstrations, have been accused of inviting protesters into the German parliament building who went on to harass other lawmakers.
The AfD on Thursday released a statement denying any links to the protests in front of the Reichstag building last year, and accusing others of seeking to use the latest events in the US to score political points.
"Anyone who equates the unrest in Washington with the demonstrations that took place before the Reichstag building in Berlin, and who points to our party's sympathy for these events, is abusing the anarchist events for political purposes in Germany," party leaders said in a statement.

EDITOR'S COMMENT: I am sure that many other countries will follow the German example although this is not necessary if governors remember the "*of the people, by the people, for the people*" Abraham Lincoln's quote.

COVID-19 Effect – Tokyo Olympics Cybersecurity Measures Increased

Source: https://i-hls.com/archives/106243

Jan 09 – The forthcoming Tokyo Olympics events due to open on July 23 could be targeted by cyberattacks, especially over the backdrop of the coronavirus pandemic. Since many officials working for the Tokyo Games have been teleworking due to the pandemic, there has been growing concern that devices being used to work from home will be targeted.

Moreover, the Tokyo Games may limit the number of spectators, which increases the demand for events to be streamed. "The games themselves will be in cyberspace. The host country has the responsibility to share (them) with the world," a Japanese government official said.

These concerns have led the organizing committee to train 220 IT security experts or so-called white hat hackers to protect the Games from cyberattacks. Those "ethical hackers" now working for the organizing committee are mostly employees of Japanese companies, including Nippon Telegraph and Telephone Corp and NEC Corp.

They participated in an extensive training program developed by a technology research institute, the National Institute of Information and Communications Technology, consisted of lectures on 20 subjects and exercises, where the members were divided into groups to protect their system from the attacks of the other team, according to the officials.

In a bid to protect critical infrastructures, such as electricity and transportation systems, teams of cybersecurity experts have also been established in their respective business fields to share information and to hold drills, according to japantoday.com.

The Pyeongchang (South Korea) Winter Games in 2018 fell victim to a cyberattack and suffered system problems on the day of the opening ceremony, which forced the organizers to make changes to parts of the program, while there were also disruptions to internet access and broadcasting services.

Last year, the U.S. Justice Department charged six Russian military intelligence officers in connection with international hacking, accusing them of worldwide cyberattacks that included targeting the Winter Olympics in South Korea.

The British government also said Russia's military intelligence service carried out cyberattacks against the organizers of the Tokyo Olympics and other entities associated with the upcoming games.

Medical Equipment Packaging Company Hacker Sentenced

Source: https://www.fbi.gov/news/stories/hacker-who-disrupted-ppe-shipments-sentenced-010621

Jan 06 – When the COVID-19 pandemic reached the United States last spring, a Georgia-based medical equipment packaging company worked to get personal protective equipment (PPE) to medical workers treating sick patients.

But a disgruntled former employee thwarted those efforts at a time when protective equipment was desperately needed.

Christopher Dobbins, a vice-president in the company who'd been fired a few weeks earlier, still had a secret account on the company's computer system that he'd created before he was fired. Although the employer revoked his access, Dobbins used this secret account to get back into the company's computer system from his home in late March. Once in the network, he changed or deleted critical data that the company needed to function, such as shipping information. It delayed the company's ability to send out shipments of PPE.

"It was both a chance for the company to contribute to the national response and a business opportunity," said Special Agent Roderick Coffin, who investigated the case out of the FBI's Atlanta Field Office.

The company quickly figured out its systems had been breached and alerted the FBI. The company's operations ground to a halt briefly, and disruptions continued for months.

The FBI Atlanta Cyber Task Force gathered evidence that showed Dobbins was behind the hack. He pleaded guilty to computer intrusion charges in July 2020 and was sentenced to one year in prison in October 2020.

"Given the pandemic, it was especially urgent that we figure out what happened and ensure there was no continuing compromise," Coffin said. "We also wanted to make a statement that the FBI and the U.S. Attorney's Office are going to investigate and prosecute these types of crimes."

In this case, like so many cyber cases the FBI investigates, a collaborative relationship with the victim company was key to success. "In computer intrusion cases, the crime scenes are the systems in these companies' offices, and we need their assistance to process that in a way it's admissible in court," Coffin said. "The FBI works very hard to proactively establish trust with companies, so when these types of things occur, we can quickly figure out what happened, and they can move forward."

Supply chain viruses, the new face of cyber warfare

By Prosenjit Datta (Senior business journalist)

Source: https://www.newindianexpress.com/opinions/2021/jan/14/supply-chain-viruses-the-new-face-of-cyber-warfare-2249942.html

Jan 14 – Should India start worrying about "supply chain" viruses and hackers? Should a couple of hacking exploits that affected the US government and, perhaps, the government of Vietnam set off alarm bells in India? Yes, because in an increasingly digital and connected world, this could be the new face of cyber warfare. In the last week of 2020, news came in that Vietnam had been found to be the target of a sophisticated supply chain cyber attack.

A group of hackers had managed to compromise many Vietnamese private companies and government departments by compromising the Vietnam Government Certification Agency (VGCA). This department is responsible for issuing digital certificates that would be used for electronically signing documents. While the malware—a Trojan called PhantomNet—that was inserted wasn't very complex, it served as a wireframe for other more potent viruses.

Before that, in the second week of December, the technology world was rocked by the news of a "supply chain" cyber attack that had managed to infiltrate the networks and systems of multiple US government departments, tech majors like Microsoft and Cisco, and hundreds of big and small companies around the world working in sensitive areas. The implications of the hack and the amount of information the hackers managed to get are still being worked out.

Though the US government officials or the technology companies did not name anyone, the finger of suspicion pointed towards a Russian group of hackers called CozyBear, acting with state support. It was a highly sophisticated indirect attack. These are termed "supply chain" cyber attacks because instead of attacking a target, the hackers rely on infecting one of its suppliers instead to gain access. CozyBear exploited a vulnerability and attached a malicious code in the software update that the well-known Texas-based IT management company SolarWinds was preparing to roll out for clients.

The company counts Microsoft, Deloitte, Nvidia, Cisco and many other global leaders as its clients. The attack was initiated as early as March, when the hackers managed to insert their code into the SolarWinds software update. When the SolarWinds update was implemented by its clients, the code got access to parts of their networks as well. The hackers were exceedingly patient and did nothing for several months. After that, they slowly started stealing some data, taking care to avoid detection. It was almost by accident that the exploit came to light in December when an employee in the US cyber security firm FireEye realised that someone had logged into the company VPN using his credentials. This led to a search for the intruder, which in turn made the company realise that the hackers had got access when it implemented the SolarWinds' Orion update.

In 2020, apart from the SolarWinds and VGCA attacks, three other supply chain hacking cases had been detected. In two cases, China was involved. One Chinese bank apparently forced foreign companies operating in the country to install a backdoor tax software toolkit. In the second case, Chinese hackers had managed to compromise the update mechanism of a chat app used by Mongolian government agencies. The fifth case of the year was a

North Korean attack that delivered malware to South Korean users. Supply chain attacks are not new and have been around for several years.

Earlier, most hackers preferred to attack their target companies directly. However, as big companies beefed up their cyber security measures, such attacks could be quickly detected and counter measures taken. Unlike direct attacks, supply chain hackers are relatively difficult to guard against. The US government cyber defense system for example could not detect the CozyBear attack because it came in via a trusted source, SolarWinds, which it had no reason to suspect of any malicious intent.The bigger danger though that is cropping up is of motive. In the past, many big hacking exploits were looking to make money. This typically meant inserting ransomware or the stealing of credit card and bank details or other data. Occasionally, hackers attacked companies because they felt these were evil and needed to be punished.

But increasingly, government to government or government-sponsored attacks on rivals are gaining currency. Instead of asking for money, hackers are instead slowly gathering critical information, compromising data and inserting more malicious and complex codes that can be used one day to paralyse entire government departments or private companies and their clients, thus spreading chaos. This is the new digital warfare that seeks to bring a country to its knees by attacking its key functions and biggest companies instead of attacking it through conventional means.

As in the case of fishing stories, in hacking too, it is not the ones that are caught that are important. It is the ones that got away undetected that have the potential to do most harm. Among the countries particularly known for using hacking attacks at the government level are Russia, China and North Korea, as well as a few East European countries. For India therefore, the threat from China or Pakistan may not come from the areas it is keeping an eye on—but in the form of a cyber attack that is hard to detect and therefore counter. This is the new threat that India needs to be worried about.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Chinese Drone Giant Blacklisted – What's the Effect on the Drone Market?

Source: https://i-hls.com/archives/105902

Dec 23 – The Chinese drone manufacturer DJI, one of the largest and most popular drone companies in the world — has been added to the US Bureau of Industry and Security (BIS) at the Department of Commerce 'Entity List', identifying the company as a national security concern and banning US-based companies from exporting technology to the company.

According to industry estimates, DJI makes somewhere between 70-80% of the world's commercial drones, and over three-quarters of those sold in the US. It is estimated that this year, consumers in the US bought some 7m of the company's drones.

DJI is one of four companies accused of enabling wide-scale human rights abuses within China through abusive genetic collection and analysis or high-technology surveillance, and/or facilitated the export of items by China that aid repressive regimes around the world, contrary to U.S. foreign policy interests, according to uasvision.com.

Commerce Secretary Wilbur Ross said in a statement the department would "not allow advanced U.S. technology to help build the military of an increasingly belligerent adversary."

This is likely a reference to DJI's reported involvement in providing drones to the Chinese government to surveill detention camps in the Xinjiang province.

The Financial Times evaluated that the move will make it far harder for the company to secure American supplies, and threatens to scramble the global market for camera drones, which the Chinese manufacturer dominates.

"DJI is disappointed in the U.S. Department of Commerce's decision," a representative of the company said in a statement. "Customers in America can continue to buy and use DJI products normally."

British Army trialing "heavy-duty" Bug nano drone

Source: https://newatlas.com/military/uavtek-bae-systems-bug-nano-drone-uk-army/

Dec 28 – Drone company UAVTEK has collaborated with BAE Systems to deliver 30 prototypes of the Bug nano drone to the British Army for field evaluations. Weighing 6.91 ounces (196 g), the Bug is designed to operate in winds of up to 50 mph (80 km/h).

One of the remarkable things about the burgeoning drone market is the wide variety of functions, shapes, and sizes it encompasses. At one end of the scale are ever larger UAVs designed for reconnaissance, combat, and even launching small satellites. At the other end are tiny craft, like the Bug, designed for tasks like acting as a pocket-sized recon unit that the average foot soldier can deploy in a moment.

Making a drone tiny isn't that hard. The hobby and toy shelves are full of these. What's difficult is making the UAV smart enough to carry out its mission, with enough endurance to get to the target and back, and tough enough to stand up to rugged field conditions and bad weather.

The Bug is about as heavy as a smartphone, has a range of 1.25 miles (2 km) and a battery life of forty minutes. It can hit speeds of 80 km/h (22m/s), send vision back to multiple devices and handle winds of 35 knots, gusting to 45 knots, which according to BAE, made it the only nano-UAV to get through the inclement weather at the recent Army Warfighting Experiment (AWE) event in the UK.

The next step will be to improve the Bug by adding sensors and integrating it with other military gear.

"In even the toughest weather, the Bug can deliver vital tactical intelligence on what's around the corner or over the next hill, working autonomously to give troops a visual update," James Gerard, Principal Technologist at BAE Systems' Applied Intelligence business. "Combined with our other information advantage products, this video feed could be shared

multi-domain, enabling commanders on land, sea and air to increase their situational awareness and inform their decisions."

Knuckles-5 allows drone pilots to keep one hand free

Source [video]: https://newatlas.com/drones/knuckles-5-one-handed-drone-controller/

Dec 30 – Conventional dual-joystick drone controllers require pilots to use both hands – this can be inconvenient, plus not everyone *has* two functional hands. That's where the one-handed Knuckles-5 controller is designed to come in.

Created by "an international team of specialists from various fields related to the drone industry," the device is currently in functioning prototype form. Once it reaches production, it could also be utilized in non-drone applications such as gaming.

Knuckles-5 replaces the two traditional joysticks with two trackballs – one is moved by the index finger, while the other is moved by the thumb. Each one controls the drone along two

axes of movement. Another two axes are controlled by a thumb-activated mini joystick, while a further two are controlled by an IMU (inertial measurement unit) that detects the direction in which the controller is being tilted.
It all adds up to control over eight axes of movement. A small LCD screen on top of the device displays drone data such as battery charge level.

The commercial version of Knuckles-5 will be wireless

Additional functionality (more for things like gaming) is made possible via four customizable pushbuttons and three switches – the two trackballs also double as buttons. By assigning different actions to these different controls, it's reportedly possible to control movement along up to 19 axes, or to access as many as 40 button functions.
"Having worked in this field for about seven years, I realized that numerous models of drone controllers do not fully utilize the abilities of the human hand," says Knuckles-5 founder and CEO, Kostiantyn Borysov. "Our team is developing Knuckles-5 as an alternative to a classic two-handed remote controller. Its purpose is to overcome the disadvantages of a two-handed controller and to offer more possibilities and freedom to its users."
Borysov tells us that the controller should be available as of the end of next year, priced at about US$250 to $300. It's demonstrated in the video below, and will make its official debut next month at CES 2021.
Potential buyers might also want to check out the FT Aviator, which takes a different approach to *sort of* one-handed drone control. The Shift drone additionally featured a one-handed controller, but its Kickstarter campaign was cancelled.

How Israel Brings Together Robots and AI into a Lethal Combo

By Seth Frantzman
Source: https://www.meforum.org/61917/israel-brings-together-robots-and-ai

Dec 31 – On the back porch of a rundown building near the sea in central Israel a plank leads to an unlikely machine. A robot dog is surveying the area, preparing for a mission. Alongside it, like a sidekick, a drone is hovering and awaiting orders. Soon the two systems will enter the building, mapping it room by room and identifying threats. In another room a

wall of computer screens are mounted were soldiers will see the feed coming back from the robots. A three-dimensional model of the rooms that are mapped will be printed and a team will analyze the building to understand the threats within. A short video of the operation in progress can be seen below.

Rafael uses Ghost Robotics' SPIRIT four-legged robot to carry out surveillance and attack missions indoors. (Rafael)

This demonstration was done in December by Rafael Advanced Defense Systems, one of Israel's major defense companies and the traditional research and development wheelhouse behind the Israel Defense Forces technological advancements. Rafael built Israel's Iron Dome air defense system and the Trophy system used to protect Israeli and American tanks. It is also at the forefront of targeting and using electro-optics for surveillance. The driving force now behind all this is the latest advancements in artificial intelligence and what the company calls "automatic target recognition." In essence that means that a targeting pod on a plane, or a missile or a robot dog can see a truck or an RPG and determine if it is a threat or if the RPG is actually just a broomstick.

This matters in today's battlefield because unlike the First World War or Vietnam-era where you could just bombard enemies into submission and destroy civilian infrastructure to do it, modern armies want as close to zero casualties as possible. That means zero casualties among your own force and no civilians killed. If enemies can be neutralized in a more precise manner, using maximum lethality, that is also better, than waging a war of attrition. This is what Israel is doing through its multi-year Momentum plan.

Rafael's demonstration of its "indoor" capabilities (click on video to the left) is designed to showcase how robots and drones can work together using the open architecture technology that Rafael has developed. For them it's not about the platforms, such as the robot dog which is named Spirit from Ghost Robotics, or the drones, named Raven, it's more about the sensors you pack the machines with and how those sensors bring back data and fuse the data using other systems the company has such as Fire Weaver. Rafael has been developing a plethora of networked technology that it sees as transforming the digital battlefield. What that means is a commander and officers now have more access to computers and can see on screen where their forces are, identify the threats and decide which force can be used to neutralize the threat. This is important in an urban environment because you might have one enemy sniper or RPG-team and getting at that enemy through a window is important. But which force will you use?

Modern militaries often have too much in the way of technology and information. The challenge is not really about having enough weapons, it's about finding the right weapon, whether using a missile from an F-35, or a loitering munition such as Rafael's Firefly missile, or special forces with rifles. With developments of more artificial intelligence and automatic target recognition the burden on commanders to have to deal with too much incoming data is reduced while preserving the issue of having a "man in the loop." In essence that means not letting the technology decide who to kill, because that would look a little too much like the nightmares envisioned in films like Terminator.

During the demonstration Rafael's Shmuel Olanski, the vice-president and head of land innovation programs as well as Noam Barak, head of the innovation center and research and development of the engineering division of the company, spoke about the advances. The modern battlefield is developing rapidly, and the need to make ground forces more digital is clear. This has already been accomplished for naval and air forces and is being input into tanks. Ground forces need more technology at their fingertips and they need to be able integrate it so it doesn't burden soldiers, but rather leverages their capabilities. A rifleman can't be distracted with a hand-held tablet all the time. But giving the soldier better tools to know what is in the houses in front of them, where terrorists may be lurking among civilians, is essential. This is the "multi-dimensional" battlefield that Israel is seeking to revolutionize.

In the demonstration in December Rafael sent its robot dog and drones into a building to clear nine rooms and identify the threats there. The unmanned systems found nine people in the rooms, five rifles and an RPG. On a tour of the facility, mocked up with a photo of Hezbollah's Hassan Nasrallah to make it feel authentic, we could see what the robots had seen previously.

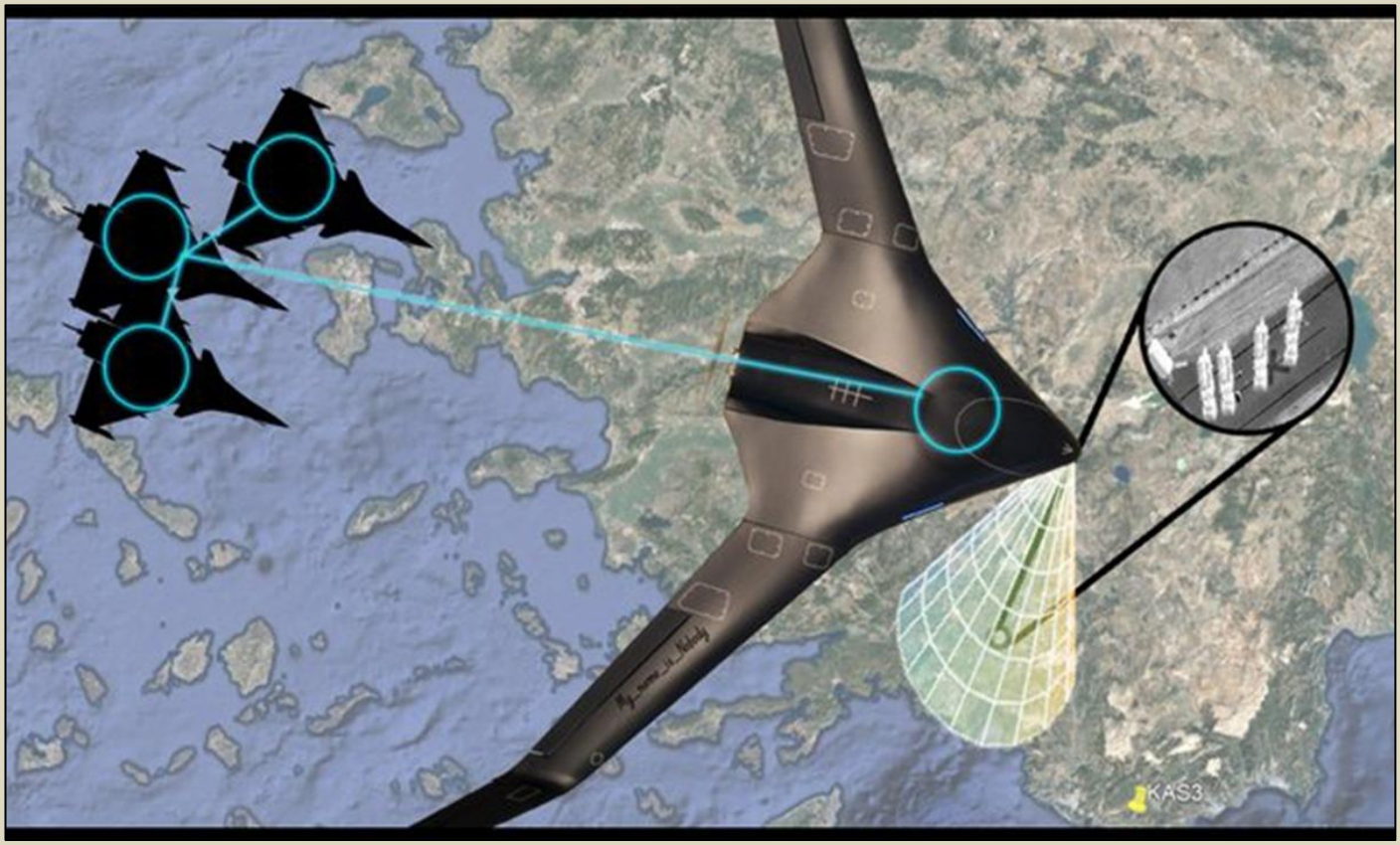
The demonstration leads to questions about what comes next. Slow-moving robot dogs can be shot at by terrorists, unless they are all sleeping. Drones are also noisy. These kinds of issues are still technological hurdles. That is why Rafael is focusing more on the sensors and technology that can be plugged into the platform than on the platforms themselves. Robots are going to become increasingly stealthier and more flexible. There will be robot snakes and smaller, quiet drones. Israel is at the forefront of a lot of this technology. Often in Israel when the country develops systems,

such as the defense systems put on the new Sa'ar 6 corvettes, it uses the best technology from its three major defense companies. That means technology and weapons from Elbit Systems, Israel Aerospace Industries and Rafael. In turn these companies often own portions of, or work with, other smaller Israeli companies such as Rafael's Aeronautics and IAI's Elta or Controp which makes electro-optics. Israel also has a plethora of small drone makers. The country is also developing future combat vehicles through a program called Carmel.

***Seth Frantzman** is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at The Jerusalem Post.*

EDITOR'S COMMENT: This article reminded me an inside tour at Ben Gourion International Airport in Tel Aviv and a demonstration of a unique (at that time) unmanned armed patrol/perimeter vehicle.
Since then, unmanned technologies on land, air and sea have been combined with modern artificial intelligence and robotics showing how the future might be both in the field but also within the urban environment.

Coming soon over Aegean Sea!



LOTUS (GR): Next Generation Tactical ISR UAV

Keeping drones flying when a motor fails

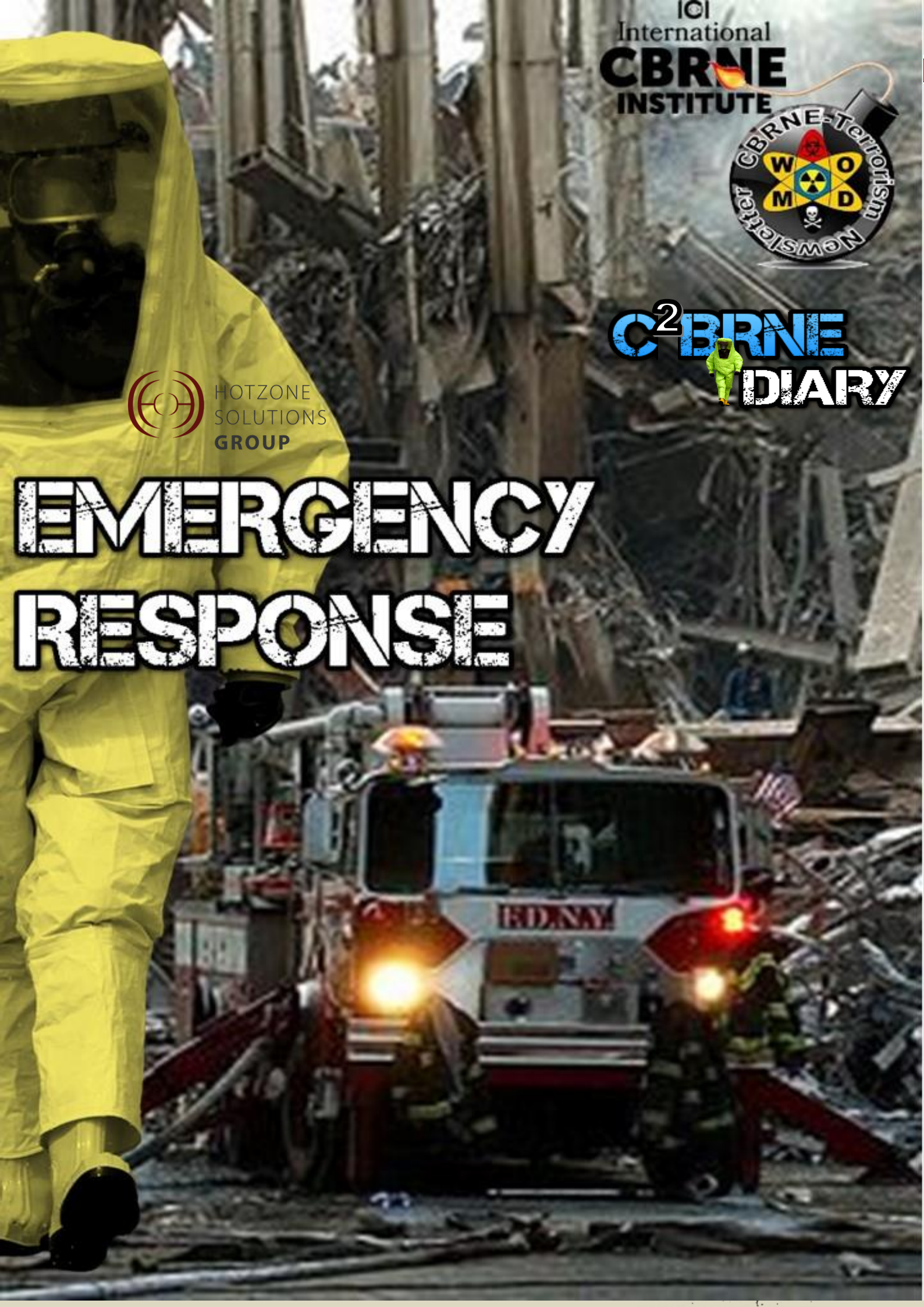
Source [video]: https://www.eenewsembedded.com/news/keeping-drones-flying-motor-fails

Jan 19 – In contrast with commercial aircraft that can easily continue to fly even if one of the engines stops working, for quadcopters (drones with four propellers) the failure of one motor is a bigger problem. With only three rotors working, the drone loses stability and inevitably crashes unless an emergency control strategy sets in.

Researchers at the University of Zurich and the Delft University of Technology have now found a solution to this problem. They show that information from onboard cameras can be used to stabilize the drone and keep it flying autonomously after one rotor suddenly gives out.

"When one rotor fails, the drone begins to spin on itself like a ballerina," explains Davide Scaramuzza, head of the Robotics and Perception Group at UZH and of the Rescue Robotics grand challenge at NCCR Robotics, which funded the research. "This high-speed rotational motion causes standard controllers to fail unless the drone has access to very accurate position measurements." In other words, once it starts spinning, the drone is no longer able to estimate its position in space and eventually crashes.

One way to solve this problem is to provide the drone with a reference position through GPS. But there are many places where GPS signals are unavailable. In their study, the researchers solved this issue for the first time without relying on GPS, instead using visual information from different types of onboard cameras.


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

Groundbreaking Firefighter Tracking Technology

Source: http://www.homelandsecuritynewswire.com/dr20210108-groundbreaking-firefighter-tracking-technology

Jan 08 – In the U.S. alone, approximately 80 to 100 firefighters are lost in the line of duty each year according to the National Institute for Occupational Safety and Health. More than 50,000 are injured according to the National Fire Protection Association. Countless others risk their lives every day to serve and protect our communities. Because of these alarming statistics, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) joined forces with NASA's Jet Propulsion Laboratory (NASA JPL) to develop critical technology that will allow first responders to more accurately locate their team members in burning buildings.

Last month, S&T and NASA JPL successfully tested the Precision Outdoor and Indoor Navigation and Training for Emergency Responders (**POINTER**) technology at the Veteran's

Affairs Greater Los Angeles Healthcare System. During the demonstration, multiple POINTER devices were evaluated with members of S&T's First Responder Resource Group and industry partner Balboa Geolocation Inc. to ensure that they met first responder requirements. The tests, conducted as a first step prior to operational field testing with several fire response agencies across the country throughout 2021, focused on POINTER's tracking, visualization, and data collection capabilities, component. A commercial product is projected to be available in early 2022.

"There are currently no commercialized tracking devices like POINTER on the market," said S&T First Responder Portfolio Director Greg Price. "This device goes far beyond GPS capabilities to give first responder teams more accurate guidance in locating their colleagues in emergency scenarios."

Here are some initial findings from the recent testing:

- ✓ POINTER command station, transmitters, and receivers were deployed in a 5-level, 8,000 sq. foot structure meant to represent a residential home. The system tracked multiple first responders from a standoff distance of up to 70 meters.
- ✓ POINTER was able to accurately locate the responders in 3D within 1 meter—in many cases, within just centimeters—throughout all levels of the building.
- ✓ The receiver technology worn by first responders has been updated to the size of a cell phone, powered by a small rechargeable lithium battery and weighing just ounces.

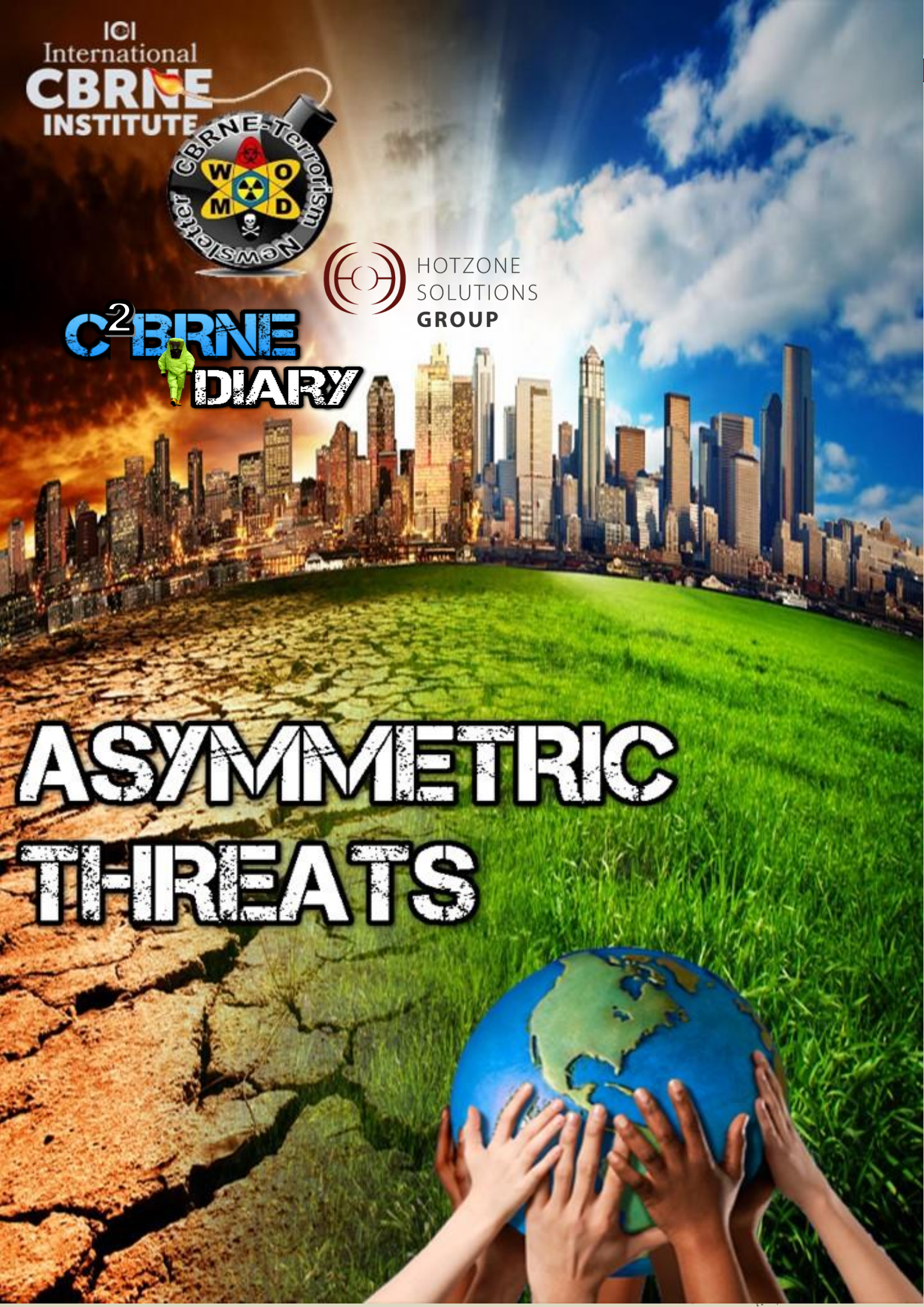
Many existing tracking technologies use GPS, Ultra-Wideband, or other identification methods that rely solely on radio position location—these can suffer reduced performance in non-line-of-sight and indoor environments. POINTER, on the other hand, uses magnetoquasistatic fields to three-dimensionally orient and track responders in emergency

settings, helping incident command pinpoint their location within one meter. This is critically important, especially when visibility is low due to heavy smoke, debris, or obstructions. Maintaining this degree of situational awareness not only enhances real-time response efforts but also saves valuable time when a responder is injured or lost.
"Responders have told us that tracking technology is their number one priority," said Price. "This never-seen before POINTER technology will soon change the way firefighters experience and overcome the challenges they face."

Rescuers at Risk: Emergency Personnel Face Trauma, PTSS

Source: http://www.homelandsecuritynewswire.com/dr20210119-rescuers-at-risk-emergency-personnel-face-trauma-ptss

Jan 19 – A new study in *Frontiers in Psychiatry* has for the first time, demonstrated differences in the prevalence of post-traumatic stress symptoms (PTSS) in different groups of rescue workers and emergency personnel, including firefighters, police officers and psychiatric nurses. The researchers showed that the varying experiences and circumstances these workers encounter, such as handling aggressive people, working with families or dealing with deaths and suicide, are tied to varying levels of PTSS and suicidal thoughts, with emergency department staff and psychiatric nurses showing the highest levels of PTSS and suicidal thoughts out of the emergency professions studied. The findings highlight the urgent need for bespoke training and counseling services across the rescue and emergency industries, which would help staff to cope with the trauma they experience, improving their quality of life and mental wellbeing in such high-risk professions. The study was led by Dr. Leila Soravia and Dr. Thomas Müller at the University of Bern's Hospital of Psychiatry in Switzerland.
Rescue workers and emergency personnel often encounter traumatic events as part of their roles and are therefore at a higher risk of developing PTSD and suicidal thought patterns than the general public. Dr. Soravia explains:
"Though rescue workers across different professions will often be engaged at the same event or emergency, they have very different roles and responsibilities on the scene: this can mean the stress experienced by different workers is very subjective—whether that's from dealing with deaths, working with families of victims, or being exposed to violence. The mental wellbeing training that is offered to staff to teach them how to cope with this stress and trauma also often varies across these different professions. We therefore speculated that the prominence of PTSS and other related factors would vary across different rescue workers, which has not been studied so far."
The researchers distributed an anonymous online survey to rescue workers across Bern, Switzerland, which included police officers, firefighters, ambulance personnel, emergency department staff and psychiatric nurses. All the participants were asked questions about traumatic events they had experienced before and during the course of their job, any PTSS or suicidal thoughts they experienced, and were also asked to rate how well they thought they coped with stress and PTSS.
The study found significant differences in the prevalence of PTSS between different professions, and notably, emergency department staff and psychiatric nurses featured the highest prevalence of PTSS. For individuals who demonstrated PTSS, dysfunctional coping strategies, such as alcohol abuse or avoidance of a situation or emotion related to their stress was one of the most robust predictors of their symptoms.
"The findings highlight how even the same emergency situations can affect the mental health of rescue workers differently. We urgently need profession-specific training that can improve emergency workers' abilities to cope with the stresses of their job to reduce their PTSS and enhance their quality of life in such high-risk professions," highlights Dr. Soravia.
"Long term studies would help us understand the predictors of PTSS in emergency personnel—a more profound understanding of these symptoms could then be a valuable basis for mental wellbeing training and support in the future."


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

A fragile and divided European Union meets Covid-19: further disintegration or 'Hamiltonian moment'?

By Giuseppe Celi, Dario Guarascio and Annamaria Simonazzi

Journal of Industrial and Business Economics | Volume 47, pp.411–424 (2020)
Source: https://link.springer.com/article/10.1007/s40812-020-00165-8

Abstract

Despite being symmetric in its very nature, the Covid-19 shock is affecting European economies in a very asymmetric way, threatening to deepen the divide between core and peripheral countries even more. It is not Covid-19 itself, however, but the contradictions within the EU's growth model and institutional architecture that would be to blame for such an outcome. The dramatic impact of the economic crisis brought on by the pandemic and the threat that it poses to Eurozone survival seem to have forced a reluctant Germany into action: a minor step, but an important signal. This note analyses the crossroads currently facing Europe—the risk of disintegration vis-a-vis the opportunity for a 'Hamiltonian moment'—discussing possible future scenarios in the light of past developments.

Coronavirus, invisible threats and preparing for resilience

By Gunhild Hoogensen Gjørv

Source: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html

May 2020 – The corona virus pandemic is the security scenario we were least prepared for. While nation states are responsible for security, they depend highly upon civilian resources and resilient populations. This is a test for civil-military cooperation and requires a comprehensive approach.

Just like the fall of the Berlin Wall and the collapse of the Soviet Union – and despite the warnings – we really did not see this coming. The possibility of a global pandemic has long been bandied around as hypothetical threat. But had health been seriously considered more broadly as a security issue, we might have thought more effectively about this scenario, and prepared for it differently.

Framing a pandemic as a security issue does not mean "it is time to panic," nor that a pandemic should be equated to a war or a military issue. It is, however, definitely a security issue. As such, the pandemic requires clear heads and the best information possible, often in a situation of incomplete data. This crisis illustrates the complex nature of security, where multiple actors are involved and civilians are central to understanding the security picture.

Today, we are surrounded by incomplete information, misleading information, disinformation and, in fact, too much information (an "infodemic"). This overload of information and fake news targets people with a view to trigger actions and reactions which could contribute to potential destabilisation. Reduced trust and/or increased polarisation between people and their governments affects how populations respond to crises.

The coronavirus crisis provides insight into challenges that do not typically fall under militarised (use of force) security but could nevertheless destabilise, if not cripple, whole societies. It is an important test of "resilience" across society, as well as an opportunity to revisit how we define "resilience".

The pandemic increases our understanding of security scenarios, including those associated with hybrid threats and hybrid warfare, where militaries or NATO are not the primary security actors. Yet, at the same time these actors need to be able to react proportionally, mitigate harm, and adjust thinking according to context. As part of ensuring national preparedness, it is important to evaluate the extent to which our understandings of resilience are realistic and/or need modification, and who is included in that process.

Resilience

Article 3 of NATO's founding treaty addresses resilience, with the expectation that each member country is able to resist and recover from a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack on the basis of "their individual and collective capacity". Resilience is understood as "a society's ability to resist and recover easily and quickly from such shocks and combines both civil preparedness and military capacity."

Resilience reflects an ability to "bounce back" and tackle a crisis and/or threat, but also an ability to evolve or adapt to abrupt and potentially long-lasting change. Assumptions about resilience are evident in narratives about "returning back to normal" after the coronavirus crisis. Such assumptions do not take into account how changes themselves may become normalised over time, and how attitudes and behaviours – not least among citizens – change

as a result. People expect governments to solve a crisis as soon as possible. But what if, like in the coronavirus crisis, that is not possible? Resilience in society may demand adjustments to "new" normals, including new perceptions of insecurity.
Examining the current pandemic is useful for reviewing our understanding of resilience as well as national and NATO preparedness for three reasons:

1. The COVID-19 virus presents a threat to the health, economy and social cohesion of societies on a global level, generating a crisis response.
2. The pandemic increases our understanding of how governments and populations respond to such a widespread crisis over time.
3. It is simultaneously a crisis that is increasingly subjected to attempts to politicise it through disinformation campaigns, which provides us with real-time data on how societies and their populations react when crises are further complicated by politics.

Invisible, hybrid and "grey zone" threats

Threats to society today are increasingly generated through non-military or non-violent means. Rather than crossing borders with tanks or firing weapons, adversaries have found easier ways to create crises or conflict. Today's strategy of choice for state and non-state actors is to use disinformation or cyberattacks to erode trust in authorities and foster societal and/or political unrest, for example, by undermining services and infrastructure, promoting extremism or violence, and exploiting existing politicised vulnerabilities from elections, to migration, to pandemics. Such destabilisation activities are often cheaper to conduct than armed attacks – they pose invisible threats, which are difficult to detect and trace, and to attribute to a specific adversary.
Though not necessarily an enemy in itself, disease is an invisible threat, which can be used politically and has recently been exploited for the purposes of misinformation, disinformation and infodemics. We need to understand how invisible threats – whether generated by human activity or natural causes – can be operationalised and, often unwittingly, amplified by average citizens.
Check out this video to see how NATO is responding to disinformation on COVID-19. © NATO
Many of the invisible threats and attacks that lead to destabilisation are commonly referred to as "hybrid". Evolving from earlier conceptions of hybrid warfare, which maintained a kinetic or lethal component, the increased use of information warfare and targeting of public opinion as well as cyberattacks on infrastructure became a core distinguishing feature by 2014.
Invisible, hybrid threats are a central feature of "grey zone" conflicts, a term that refers to the increasingly blurred distinction between peace and war, creating a "continuum of conflict". War has always had an "end state." The distinction between peace and war are far less clear now as disinformation and cyberattacks are continuous, rolling campaigns designed to disrupt and destablise, possibly without end. The grey zone encompasses measures that create destabilisation and conflict below the threshold of overt violence, including disruptive tactics such as disinformation, psychological operations and destabilising legal processes. Crisis and conflict are part of the same continuum of insecurity, where crisis is an earlier stage of instability and uncertainty before conflict that represents even greater, hostile instability, which can move from a non-violent to violent nature. Much of this continuum represents instabilities that are not strictly military in nature.
One of the largest challenges is that we do not adequately know how civilian populations will react and/or behave during a crisis. Our resilience baseline requirements are top down, that is, dependent upon state and alliance actors to implement, often making a default assumption that average civilians are passive elements in a crisis situation. However, lack of trust in authorities could lead to increased "self-help" solutions by individuals or groups of people based on false or misleading information. Thus, defence against disruption or destabilisation requires not only state-based measures, but also societal capacities.

Reinvigorating a comprehensive approach?

Preparing for the complexity of invisible and hybrid threats requires a much more complex approach than for conventional warfare. It calls for a flexible balance and coordination between civil and military resources depending on the nature of the crisis. A comprehensive approach includes a large repertoire of non-military-centric responses, allowing for different constellations of actors according to the context.
Resilience is an important component in a comprehensive approach and civilian resilience (both institutional and within society itself) is crucial. Elisabeth Braw noted, at a 2018 NATO seminar on civil preparedness, that the civil-military relationship and particularly societal resilience is a part of modern deterrence. This entails an improved civilian situational awareness and a clear understanding of evolving relationships between civilian and military – but prioritises citizen leadership relying on trust between citizens and the authorities to work together and support each other in crisis. However, as Braw also noted, open and democratic societies can be extremely vulnerable to disinformation and polarisation of political views, which destabilises the social trust upon which cooperation relies, and reduces resilience capacities to adapt or "bounce back".
Maintaining a well-educated and informed citizenry is essential for an effective comprehensive approach. Independent and transparent information/media outlets combined

with rigorous, science-informed and socially responsible education programmes are crucial to in times of crisis. Some NATO member states, including Estonia and Germany, and partner countries such as Sweden and Finland, have issued guidance to their citizens in the form of brochures. Finland even starts its fight against fake news in primary schools.

Learning from the pandemic

Hostile actors are using disinformation about the pandemic to polarise views amongst civilians and generate selective distrust, as noted in a recent special report published by the European External Action Service. Selective distrust occurs when people pick and choose which guidelines, measures or authorities to heed, often on the basis of who they are or the politics they represent.

The ways citizens choose to act and react to disinformation say a lot about how successfully authorities, in cooperation with communities, establish security in society. It makes a difference to security when people express distrust in a unified response to a threat, for example by defying quarantine regulations, hoarding toilet paper or responding with anti-social bravado ('I am not afraid of a disease'). Those countries that have higher levels of trust – regardless of political regime – have been more successful in combating the pandemic than those with lower trust levels.

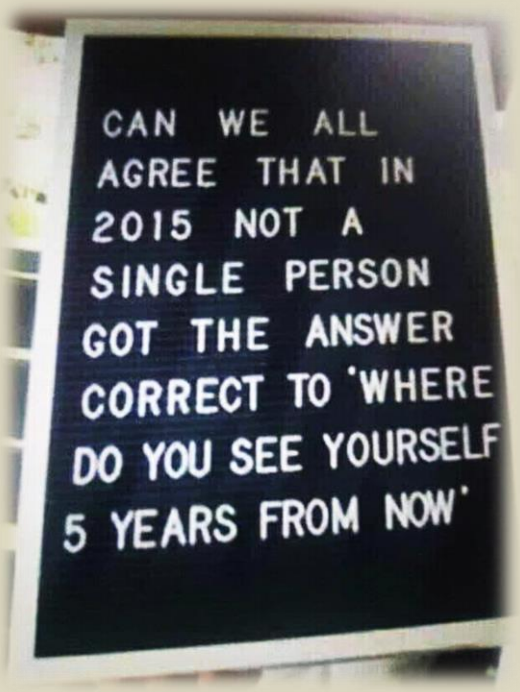
Understanding threats, developing responses, and sharing insights with its member states and cooperating with partners (including the European Union) is a NATO task. Increasingly complex threats require complex solutions. It is clear from the current pandemic that to manage crises, we need to think critically about the role of comprehensive approaches involving multiple actors from governments to research, civil society, the private sector, militaries and police, and not least, citizens in their communities.

Starting with lessons learned from previous attempts, we need to redesign a comprehensive approach with current contexts in mind, learning from real-time coronavirus crisis data and building from the community/ground up. We need to map resources and strengths that already exist in communities including: developments in education programmes; the role of local civil-society organisation and short-notice capacities to recruit volunteers; availablility and reliability of local resources (transport, energy, communictions, food and water); status of municipal information and preparation measures; and how societal trust works at local, regional and national levels. This bottom-up approach combined with the guidance of the baseline requirements for resilience will provide the groundwork to identify further initiatives or gaps to be addressed, including national crisis preparation initiatives supporting civilians, evaluation and preventative strengthening of essential social services (health, transportation, infrastructure) and extensive exercising with multiple civilian actors.

We need to seize the opportunity provided by the current pandemic to learn crucial lessons about trust, resilience, comprehensive approaches, and the complexities involved in creating and ensuring security in todays's world of invisible threats.

Gunhild Hoogensen Gjørv *is professor in peace and conflict studies at the Centre for Peace Studies, UiT The Arctic University of Norway. She is also project leader of the "Resilient Civilians" project, funded by the NATO Science for Peace and Security Programme.*

.



HOTZONE SOLUTIONS GROUP

HAPPY new year 2021

A holistic approach in CBRNe operations

Consultation

Products

Training

www.hotzonesolutions.org