6\20

HZS CBRNE DIARY

Dedicated to Global First Responders

June 2020

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

DIRTY R-NEWS

Bill Would Prohibit Use of Nukes against Hurricanes

Source: http://www.homelandsecuritynewswire.com/dr20200609-bill-would-prohibit-use-of-nukes-against-hurricanes

June 09 – On 1 June, the official first day of the hurricane season, Rep. Sylvia Garcia (D-Texas) introduced the Climate Change and Hurricane Correlation and Strategy Act which, among other things, explicitly prohibits the use of a nuclear weapon, or another "strategic weapon" – by the president or any other federal official — for the purpose of "altering weather patterns or addressing climate change."

Last August, *Axios* reported that President Trump repeatedly asked DHS experts and other top national security officials to consider using nuclear bombs to weaken, destroy, or change the direction of hurricanes.

"They start forming off the coast of Africa, as they're moving across the Atlantic, we drop a bomb inside the eye of the hurricane and it disrupts it. Why can't we do that?" Trump reportedly asked aides during one hurricane briefing.

After *Axios* published the story, Trump falsely denied that he had suggested that nukes be used to deal with hurricanes, but the report was confirmed by several official who were pressed by Trump on the issue.

Garcia told the *Washington Post* that her proposed bill was written with Trump's comments in mind.

"My bill also makes sure nuclear weapons can't be used against hurricanes. Normally I wouldn't think we'd need to legislate something so obvious, but given remarks this President made in August 2019, apparently, we do. Such use would result in radioactive fallout and cause significant public health and environmental harm."

Garcia notes that when her staff researched the subject, they discovered that the idea was put forth before.

James Fleming, a professor at Colby College, wrote a book about the idea — *Fixing the Sky: The Checkered History of Weather and Climate Control*– documenting how, from the beginning of the nuclear age, people have been intrigued by the possibility of using nukes to influence the weather.

In 1945, for example, Vladimir Zworykin, an associate research director at Radio Corporation of America, suggested that "if humans had technology to perfectly predict the weather, military forces could be sent out to disrupt storms before they formed, perhaps using atomic bombs."

According to CNN, the head of the U.S. Weather Service said in 1961 that he could "imagine the possibility someday of exploding a nuclear bomb on a hurricane far at sea." The same year, UNESCO director Julian Huxley spoke about the subject.

In 1963 the Partial Test Ban Treaty (PTBT) went into effect, prohibiting signatory nations from testing nuclear weapons in the atmosphere (underground nuclear tests were allowed).

Stanford University's Scott Sagan told the *Post* that the PTBT would not actually prevent a president from using nukes to destroy or weaken a hurricane. "It would be a stupid thing to do, but it would not be an illegal thing to do," Sagan said.

NOAA dismissed the idea as impractical, noting that the energy released by nuclear weapons pales in comparison to the energy released by a typical hurricane, which the NOAA describes as comparable to a 10-megaton nuclear bomb exploding "every 20 minutes."

While the detonation of even several nuclear bombs would not weaken a hurricane or change its direction, experts note that the radioactive fallout released downwind could have catastrophic impacts for people and the environment.

"It was a bad idea when [the NOAA deemed it impractical]," Phil Klotzbach, a meteorologist and tropical cyclone expert at Colorado State University, told the *Post*, "and it's still a bad idea."

Axios's reporting noted that Trump raised the idea not once, but on several occasions, including with top national security and intelligence aides.

Kerry Emanuel, a hurricane expert at MIT, does not see Trump's queries as off-the-cuff comments. He told the *Post* that she is more worried.

"If we have a leader who would contemplate using a nuclear weapon on a hurricane," he said, "we have a much more extensive and serious problem than could be covered by a specific bill like this one."

Have Pakistan's Nuclear Weapons Really Made It Invincible?

By Dr. David R. Leffler

Source: http://www.asiantribune.com/node/94187

On the 22nd anniversary of Pakistan's successful nuclear tests, Opposition Leader in National Assembly Shahbaz Sharif is quoted as saying: "May 28 would always be remembered as a day when Pakistan's defence was made invincible" ("Nawaz eulogised for 'making Pakistan nuclear power'", *Dawn*, May 29, 2020).

Invincibility is a laudable goal – but have nuclear weapons really made Pakistan invincible during these high stress times when terrorists can strike at any moment. Despite advanced technology and valiant efforts, the Pakistan military still struggles to eliminate violent extremism.

Ultimately the only way to become truly invincible is to not have any enemies. If there are no internal or external threats, there are no enemies. No enemies, no conflict. But how could such an ideal goal be achieved when tensions are so high? A proven scientifically validated approach is needed to reduce tensions resulting in violent extremism.

Violent extremism is a human problem requiring human solutions. The underlying cause of extremist social violence is accumulated social stress. Therefore, to eliminate such social problems, this collective societal stress must be reduced.

The answer to current high collective stress lies within us. Inner peace is the basis of outer peace. By going within, one gains clarity and is able to come up with positive solutions that work for everyone. A proven way of utilizing this inner wisdom is through the non-religious Transcendental Meditation (TM) and the powerful brain-based technology known as Invincible Defense Technology (IDT) in military circles. Militaries worldwide are forming Prevention Wings using IDT as a ground-breaking and effective means for solving supposedly insurmountable problems and creating lasting peace.

IDT utilizes the TM program and its advanced techniques to bring about major increases in calmness, clarity of mind, happiness, creativity, and energy, as proven by hundreds of independent research studies. This evidence-based approach is highly effective for stress-related conditions, brain function, and cardiovascular health.

In particular, the more advanced TM-Sidhi program is akin to using a laser instead of ordinary light; the effects are far more powerful. Scientific research has demonstrated over and over that this advanced IDT practice raises the consciousness of all those within its field. Positive solutions to ongoing problems occur naturally and society more readily shifts from division to unity.

How can this be? While it seems too simple to be true, sometimes the simplest approach is the most effective. Consider: IDT was utilized in Washington D.C. over a two-month period in the summer of 1993, where 4000 meditators gathered for an experiment to lower crime. The result, as documented by an independent board of criminologists, was a 24 percent reduction in criminal violence. This profound reduction in social stress also influenced the public approval of the US president, which suddenly changed from a negative trend to a positive trend, as predicted (Reference: *Social Indicators Research*, 1999, 47: 153-201).

A global experiment to assess the influence of the advanced practices of advanced TM on world trends was conducted December 1983 for three weeks. While a group of over 7,000 TM experts assembled in Fairfield, Iowa: international conflict decreased 32%, terrorist casualties decreased 72%, and infectious disease rates fell by 33% in US and Australia (Reference: *Journal of Offender Rehabilitation*, 2003, 36 Issue 1-4).

A study published in May 2019 in *Studies in Asian Social Science*, found that IDT implementation by students trained in advanced TM resulted in a 96% decline in sociopolitical violence in war-torn Cambodia as compared to violence in the preceding three years.

Extensive peer-reviewed scientific research repeatedly confirms that large groups of TM experts meditating in unison twice a day generate a powerful field effect which affects the surrounding population by raising the collective consciousness of all within its field. This results in measurable decreases in war deaths, terrorism, and crime.

For those who remain skeptical, we recommend the following book: *An Antidote to Violence: Evaluating the Evidence*, by Barry Spivack and Patricia Anne Saunders which details in depth the scientific research supporting this approach.

The military of Pakistan is responsible for protecting Pakistan; it is funded and its personnel are paid to perform their duties. It is thereby obligated to thoroughly examine all scientifically proven defense technologies to help them better protect the nation.

Thus, it is ultimately their sworn duty to explore using IDT to establish a Pakistani Prevention Wing of the Military to make Pakistan truly invincible.

***Dr. David Leffler** served as an Associate of the Proteus Management Group at the Center for Strategic Leadership, US Army War College. Currently, he serves as the Executive Director at the Center for Advanced Military Science (CAMS).*

Iodine-131 as yet Another Example of a CBRN Threat to the EU

Source: http://www.cbrneportal.com/iodine-131-as-yet-another-example-of-a-cbrn-threat-to-the-eu/

December 2011 – Early in November 2011, the International Atomic Energy Agency (IAEA) announced that very low levels of Iodine-131 (I-131) were detected in the atmosphere above at least six EU Member States. Later that same month, the IAEA notified that it had "most probably" identified the *Institute of Isotopes* in Hungary as the source of the radiation. In a reaction towards this allegation the director admitted a leak was found at the Budapest-based Institute. However, according to him it is "extremely unlikely" that the *Institute of Isotopes* was the source of relatively high levels of I-131 traced in the EU countries. The exact cause of the release is still under investigation by the IAEA.

Iodine-131

I-131 is a radioactive form of Iodine and is produced by the fission of uranium atoms during operation of nuclear reactors and by plutonium (or uranium) in the detonation of nuclear weapons. It has a half-life of about eight days and is also used in medicine to diagnose and treat disorders of the thyroid gland, as this gland easily absorbs iodine. Exposure to large amounts of I-131 is dangerous to human health. External exposure to large amounts can cause burns. Internal exposure in significant quantities can cause cancer, particularly in the thyroid gland. Internal exposure can take place through the inhalation of I-131 contaminated air or when ingested through food or water. Pregnant women and young children are especially susceptible to the effects of I-131 ingestion. Normally, no traces of I-131 should be detectable in rainwater or milk. In the weeks after the Fukushima disaster in March 2011 I-131 was measured on the US West Coast. In Europe, I-131 was detected after the Chernobyl disaster took place in 1986. It is important to mention that the levels traced in November 2011 are extremely low compared to rates observed after the Chernobyl tragedy.

Radiological hazards

By all accounts, the latest 'I-131 case' could hardly have any serious consequences for health and environment. However, it exemplifies the on-going threat that the EU faces from CBRN incidents, regardless of whether or not they are the consequences of natural or man-made disasters or accidents. Besides that, the case underlines the cross-border impact of CBRN incidents and the dependency of the various Member States on one another. Until now, radiological terrorist killing of more than one person has not been reported. All radiological substances can be potentially harmful if people are exposed. Most cases of people exposed to radiation have happened by accident. Unlike chemical and biological substances, radiological materials cannot be "neutralised" and many radiological materials have half-lives measured in many years. Radiological incidents are clearly a threat to human health and if densely populated, industrial or financial districts have to be evacuated following the detection there of radiological material it could have far-reaching economic consequences.

Terrorist have shown interest in I-131. In the 1970s the radiological material was used in terrorist attacks. In April 1974, in Austin, Texas, a domestic American group sprayed railway compartment cars with the radioactive material. As a consequence, six people were affected. I-131 was also used in the mid-1970s by Palestinian terrorists to contaminate a train in Austria. Even today, terrorists examine the possible consequences of I-131. In his 1500 page manifesto, '*A European Declaration of Independence'* terrorist and right-wing extremist Anders Breivik investigates possibilities for radioactive contamination. He classifies Iodine among high level contaminators.

"Dirty bomb"

Breivik, moreover, pays special attention to Radiological Dispersal Devices (RDDs) also known as "dirty bombs". He values this weapon greatly for its usefulness as a weapon to disrupt societies. Furthermore, al-Qaeda has openly expressed its desire to produce radiological weapons. According to the CIA, the group could easily construct a RDD. For this reason, it is crucial that terrorists like Breivik or members of al-Qaeda do not gain access to radiological facilities like the *Institute of Isotopes*. Terrorist groups armed with radiological weapons can be one of the serious risks our society faces. Unlike nuclear weapons, RDDs are not very hard to acquire, transport or build. A "dirty bomb" does not trigger a nuclear reaction or involve a nuclear explosion. It consists of a high explosive, (e.g. Semtex, dynamite or TNT), incendiary material (e.g. thermite), and radioactive material. The detonation of a RDD would contaminate personnel, equipment, facilities, and terrain. The fire caused by the incendiary material would carry the radioactivity up into the air, further spreading contamination.

The consequences of a "dirty bomb" are twofold. Firstly, detonation of a RDD would result in immediate deaths and serious injuries, caused by conventional explosive. Effects on the health of those exposed to radioactivity depends upon how long they remain in the contaminated area, the size of the particles released by the explosion, and the type of radioactivity emitted. Secondly, while such weapons would bring about far less damage than a nuclear explosion, which would result in hundreds of thousands of casualties, RDDs have enormous power to intimidate and also have the potential to cause serious social, psychological and economic disruption. Decontamination would be very costly and would last for weeks, if not months.

Orphan sources

RDDs are constructed with the intention to damage society. We can also identify unintentional radiological man-made incidents. Common accidents involving radioactive

materials are the consequence of so-called orphan sources. According to the IAEA "An orphan source is a radioactive source that poses sufficient radiological hazard to warrant regulatory control, but which is not under regulatory control because it has never been so, or because it has been abandoned, lost, misplaced, stolen or otherwise transferred without proper authorisation". Since in some regions the control of radioactive sources is non-existent and in other areas inadequate, these orphan sources are widely available throughout the world. Despite stronger regulatory frameworks in most countries the amount of available radioactive materials throughout the world is increasing. Primarily as a consequence of the industrialisation of developing regions, the use of radiological sources has increased. Moreover, old sources are being regularly replaced by new.
It is estimated that in the EU area approximately 30,000 disused radiological sources can be found of which up to 70 sources per year are said to be orphaned. Moreover, on the external side of the EU border with the former Soviet Union it is estimated that there are thousands of orphan sources of high threat category. Across the Atlantic, probably the most infamous incident with an orphan source took place in Goiânia, Brazil in 1987, when radioactive material coming from a hospital ended up at a scrap dealer. It took two weeks, after the scrap dealer and his family developed symptoms of radiation poisoning (nausea, vomiting, burns and ultimately death), before the illness was connected to the hospital material. By the time the radioactivity had been identified and the government informed, radioactive powder from the source had already been spread over a large area. Four people died as a result of radiation poisoning and 28 more received local radiation damage. 112,000 people sought medical attention. 600 sought attention for contamination but only 248 were actually contaminated.

Trade in nuclear material

According to the research '*Securing Air Traffic: case CBRN terrorism'* conducted by the University of Helsinki, "nuclear material that is directly usable for weapons and explosive devices exists in about 40 states. In many of those states, nuclear material can become available to terrorists." "Particularly vulnerable areas are understood to be in Pakistan (…) and in the DPRK (Democratic People's Rep ublic of Korea, VV), where the security situation is deteriorating. The threat of disseminating material and knowledge to unknown purposes is possibly increasing. In Russia the security measures, including the physical protection of facilities and material have been improved during the past 15 years (…), but the work is not yet completed."

Even within the borders of the EU, illegal trade in nuclear material takes place: in 2007, two people were arrested in Bratislava, Slovakia when the police caught them, supposedly, selling 2.2 pounds of highly enriched uranium (HEU) with a value of $1,000,000. HEU is the critical ingredient for making a nuclear warhead. There are many examples of trade in nuclear material at EU borders. For instance, in 2008, a load of uranium and caesium, worth $4,900,000, was captured in the Ukraine. The nuclear material was stolen from a nuclear facility in Kiev. Furthermore, in 2010, two individuals pleaded guilty to smuggling HEU into Georgia. It was the third time in seven years that HEU had been intercepted in Georgia. Obviously, it takes a lot more than obtaining materials such as HEU to build a nuclear device. Nevertheless, the above-mentioned cases should be of concern to EU Member States: illicit trade and trafficking in nuclear materials is present within, at and near the borders of the EU.

CBRN Incidents

In recent years we have seen an increase in the frequency and scale of natural and man-made disasters in Europe. The majority of CBRN incidents cannot be considered as accidents. From so-called 'lone wolves' to Islamic fundamentalist and from right-wing extremists to regionalist separatists, one can see a growing risk posed by terrorist groups seeking to get access to and use CBRN materials. As a consequence, governments need to prepare for the unthinkable: the aftermath of a terrorist attack using CBRN weapons. Despite the fact that, in the years following 9/11, Europe has been hit by a number of atrocious terrorist attacks, it has thwarted many others. Terrorists used CBRN agents in only a limited number of attempts. Consequently, the quantity of terrorist attacks involving CBRN agents is small. However, the consequences of a CBRN attack can be far more devastating than the aftermath of a terrorist attack carried out with conventional means.
Terrorist have to rely on criminal groups for access to chemicals. According to the Europol *'EU Terrorism Situation and Trend Report 2011'*, the connection between terrorist and organised crime groups' activities is an issue of growing concern. This means that an increasing number of terrorist groups have contact with organised crime groups in order to procure weapons.

EU Action Against CBRN Threats

As illustrated previously, the EU faces a variety of CBRN threats. Therefore, at EU level it is crucial to design a policy for preventing CBRN incidents that is as coherent as possible. Next to that, the EU should be well prepared for the aftermath of a CBRN incident. The second part of this report will concentrate on two policy tools the European Commission currently

has in the fight against CBRN threats: the EU CBRN Action Plan and the EU Internal Security Strategy, which respectively entered into force in 2009 and 2010.

EU CBRN Action Plan and the EU Internal Security Strategy

The EU CBRN Action Plan identifies three main arenas of work: prevention, detection and preparedness and response. In order to prevent CBRN incidents the Action Plan advocates the use of risk-assessments to prioritise high-risk CBRN materials, and then focus on the security and control of these materials and their related facilities. Moreover, the EU wishes to set up detection systems within the Member States and at its own external borders. At EU level, minimum CBRN detection standards will be established, and exchanges of good practices will be enhanced. The EU also aims to improve preparedness and response by raising awareness and increasing knowledge and information sharing on CBRN related subjects. Finally, it wants to amend response and emergency planning and means to increases the chances of finding and prosecuting terrorists and other criminals.

The EU Internal Security Strategy proposes five strategic objectives for the Member States to work together to be more effective: in fighting and preventing organised crime; terrorism; and cybercrime; to strengthen the management of the external borders and to build resilience to natural and man-made disasters. Regarding CBRN threats, two objectives are of importance: firstly, in order to "cut off terrorists' access to funding and materials" the EU should set up a network of CBRN law enforcement units, ensuring that Member States take CBRN risks into consideration into their national planning. Moreover, the EU means to establish a law enforcement Early Warning System at Europol for incidents relating to CBRN materials. Secondly, the EU wants to increase resilience to CBRN disasters. Therefore, management practices in terms of efficiency and coherence at EU level need to be improved.

Three Weaknesses

In both the Action Plan and the EU Internal Security Strategy the EU acknowledges a current lack of measures in the fight against CBRN incidents. Through the announcement of policy-adjustment the EU hopes to start improving prevention of and response to CBRN incidents. Nonetheless, one can distinguish three weaknesses the EU should deal with in its response to CBRN threats.

In the first place, since the responsibility to respond to CBRN threats mainly lies within the Member States, the EU does not have many competencies to coordinate action against them. Second, the Union has not yet created an EU-wide regulatory regime to prevent the diversion of CBRN materials for terrorist's purposes. EU rules on the security of CBRN materials are only designed to prevent industrial mismanagement and accidental environmental damage. Finally, EU Member States Home Affairs ministers differ in how they implement EU legislation. Some consider EU security agreements as sets of minimum standards to which they can add additional measures. Others consider EU rules primarily as suggestions.

Despite the fact that "many of today's security challenges are cross-border and cross-sectoral in nature and that (…) no single Member State is able to respond to these threats on its own", most Member States are not willing to assign more responsibilities to the EU on the subject of internal security, particularly in the area of intelligence. One can see a discrepancy in the Schengen Treaty, on the one hand and the way the various intelligence services operate on the other. EU citizens are able to cross national boundaries without limitations while, at the same time, the jurisdiction of the different national intelligence agencies stops at the border. Moreover, in recent years there has been an increase in the frequency and scale of natural and man-made disasters in the EU. According to the EU Internal Security Strategy, "this has demonstrated the need for a stronger, more coherent and better integrated European crisis and disaster response capacity as well as for the implementation of existing disaster prevention policies and legislation". For example, taking the I-131 case into account we cannot identify a single European nuclear watchdog, where every Member State has, at least, one nuclear agency. The I-131 case indicates that in several EU countries, including Hungary, the licensing and surveillance of the nuclear facilities and the laboratories using high amounts of radioisotopes are in the hands of different authorities. The administrative difficulties arising from this ambiguous arrangement probably account for the fact that the investigation into the definite source of the radiation of I-131 has been hampered until today.

Furthermore, taking the I-131 case into consideration, the EU could be well advised to, apart from updating its own mechanisms, support global systems for prevention and detection. Regarding radiological threats, for instance, the preparatory commission for the comprehensive nuclear-test-ban treaty organization (CTBTO) has already made good progress in creating a global system of surveillance of radionucleoids in the atmosphere.

Conclusion

The EU recognises the problems it faces in combatting CBRN incidents. Because the EU does not have many competencies regarding the internal security of the Member States, the responsibility for responding to CBRN terrorism and dealing with the aftermath of (cross-border) CBRN incidents lies in the hands of the Member States. However, most Member States seem reluctant to give up more independence in the field of security while being unable to handle a CBRN crisis without help from other adequately. Moreover, politicians are afraid to appear weak if they request other

Member States for help. Consequently, a comparison with the current Euro-crisis can be drawn: national interests in the short term appear to be more important than the EU's interests which, are of main importance to all the Member States in the long term. Politicians need to be reminded that the CBRN threat the EU faces is real. In the prevention and preparation for the response to the aftermath of a natural or man-made CBRN incident the EU Member States should focus on one keyword: co-operation. Within the current framework, an increase in co-operation without the violation of fundamental rights, such as privacy, is possible. To achieve this, the various Member States should seriously consider transferring more competencies to the EU regarding the subject of security. The EU, on its side should explore the possibilities and modalities for creating central agencies to help better manage cooperation in order to prevent CBRN incidents and to provide adequate support and responses to CBRN disasters.

CHINA: EMP THREAT

The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack

Dr. Peter Vincent Pry
Executive Director
EMP Task Force on National and Homeland Security
June 10, 2020

Source: https://www.centerforsecuritypolicy.org/wp-content/uploads/2020/06/CHINAempTHREAT2020logo.pdf

▶▶ **Read also:** China's surprise, years in the planning: An EMP attack

EDITOR'S COMMENT: Be a bit sceptic when reading this paper.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

Security experts worry about hand sanitizers on aircraft

Source: https://www.deccanchronicle.com/nation/crime/240520/security-experts-worry-about-hand-sanitizers-on-aircraft.html

May 24 – Back in 1987, a liquor bottle filled with explosives and placed in a carry-on bag in an overhead bin helped terrorists crash a South Korean airliner. All 115 on board died.

Then, in 1994, Al-Qaeda member Ramzi Yousef, architect of the first World Trade Center bombing, detonated liquid nitroglycerin that he had taken on board a Philippine Airlines flight in contact lens solution bottles. One passenger was killed and several were injured in the incident.

In August 2006, a major terror plot was busted by the British police wherein terrorists plotted to detonate liquid explosives disguised as soft drinks carried on board airliners travelling from the United Kingdom to the US and Canada.

Terrorists using liquid explosives to blow up airplanes was a major challenge to aviation security starting the late 1980s which continued through the early 2000s. But now, in the post Covid-19 scenario, as flight services resume across the country from May 25, the Ministry of Civil Aviation's (MoCA) move to allow hand sanitizer bottles (not more than 350 ml) inside aircraft has re-ignited the debate over liquid explosives.

While MoCA decided to allow hand sanitizers inside aircraft after much brainstorming over the security threat it can pose to airplanes, there has not been a single instance to suggest that hand sanitizers, when combined with other chemicals, can be used as explosives.

But the fact that is a cause of worry is that some of the ingredients in alcohol-based sanitizers are highly flammable.

What if terrorists carrying hand sanitizers, travelling separately on a plane, are able to ignite hand sanitizers?

This is the new concern for the security agencies. Highly placed sources who took part in the brainstorming sessions which led to flight services being resumed, told Deccan Chronicle that among the many concerns that were raised by various agencies, the aspect of allowing passengers with 350 ml hand sanitizers inside aircraft was a cause of concern, especially as it is flammable.

The brainstorming among officials over liquid explosives and its quantities, the chemicals used in them and past incidents of terrorists using it all were discussed threadbare.

One of the ingredients in alcohol-based hand sanitizers is a combination of isopropyl alcohol and ethanol, which is flammable. For alcohol-based sanitizers, the flash point is 63^0F, If stored at room temperature, it could ignite if it comes in contact with flames.

With hundreds of passengers carrying hand sanitizers, the agencies are looking at yet another challenge in aviation security.

"Across all airports, the terror threat has always been real and imminent. We have ETD checks (Explosive Trace Detection) in place besides all the advanced systems at the airports to detect explosives. Passengers were being allowed to bring quart-sized bag of liquids, aerosols, gels, creams and pastes in their carry-on bags but they were limited to travel-sized containers. Now, we will have every single passenger carrying hand sanitizers inside the aircraft which means presence of large quantities of sanitizers in the aircraft. It is a unique situation and will pose a huge challenge," a senior official from New Delhi said.

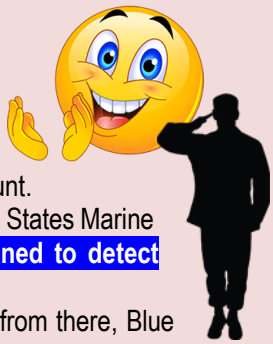
An explosives expert told Deccan Chronicle that though hand sanitizer is a high-energy material, there is no evidence so far to suggest that it can be used as an explosive.

"Though it does not explode, it can be ignited with just a spark. Even if it burns, it is low-flame but 350 ml may be enough to create a scare inside the aircraft. But if a group of terrorists were at work inside the aircraft, then obviously the quantity of flammable liquid is much higher which means more damage. It can pose a major threat," he explained.

While Deccan Chronicle's attempts to reach out to the Director General of Bureau of Civil Aviation and Security Rakesh Asthana proved futile, sources said that keeping the threat of liquid explosives in view, both BCAS along with Central Industrial Security Force (CISF) will take up regular reviews of this aspect of hand sanitizers.

"Once the flight services resume in a calibrated manner, only limited number of people will travel. The real challenge will be once all flight services are resumed," he said.

Sources explained that though hand sanitizers are flammable, the temperature inside the aircraft is generally maintained between 22⁰C and 24⁰C which is more or less the same temperature maintained in most office environments.
"In extreme heat conditions, hand sanitizers can catch fire when exposed directly, which is not possible in the aircraft as it is cold inside," they explained adding that various scenarios involving terrorist operations too were discussed keeping in mind the chemicals in hand sanitizers.



Marine veteran adopts dog who saved his life in Afghanistan

Source: https://www.today.com/pets/marine-veteran-adopts-dog-who-saved-his-life-afghanistan-t182905

June 02 – A black Labrador retriever named Blue has saved Byung "BK" Kang's life so many times, he's lost count.

The two served on more than 300 combat missions while serving together in the United States Marine Corps on a deployment to Afghanistan from 2011-2012. **Blue, a military dog trained to detect bombs** was so good at her job that she found one on their very first mission.

"That IED could have taken a couple of our guys out," Kang, 31, told TODAY. "So, from there, Blue started getting trust and the respect of my platoon."

As Blue's handler, Kang could read the dog's body language to know when she wanted to investigate a possible IED. He'd allow her to run ahead of the group — anywhere from four to 60 Marines and enlisted medical specialists, Navy corpsmen. When she'd lie down as a final indication that she'd detected an explosive, he'd call her back for her reward: playing with a toy.

Sometimes, there was time for emergency ordnance disposal technicians to confirm the existence of the IED and work to dismantle it. Other times, they'd take a step back for a security halt and get ambushed, needing to find a different path.

"Since we knew Blue is effective, it was almost impossible for a squad or a platoon to go out without Blue," he said. "Sometimes we went on three patrols per day and by the time we'd get back we're all exhausted because we've been walking miles and miles in over a hundred degrees of heat in Afghanistan. So, we did our best. Every chance, we tried to go out to possibly save the Marines and sailors."

Overwhelmed with gratitude to Blue for repeatedly saving his life and the lives of his fellow soldiers, one night in Afghanistan, Kang made a promise to the dog.

"I told her, 'What you've done for me and my guys over here in Afghanistan, we cannot pay back. So, I'm going to give you a good home where you can cuddle all day, not worrying about going to war and finding bombs.'"

After their tour ended, Blue was reassigned. Kang lost track of her, but he never forgot his promise. In fact, one of his first conversations with his future wife, Wendy, was about his plan to adopt Blue once she retired from service.

After seven years of honorable military service, Blue retired in November 2018 and moved to Lawrenceville, Georgia, where she lives with the Kang family.

Wendy Kang, herself a Marine veteran, used her connections with other female Marines to help track down Blue and to facilitate her adoption when she was finally retired. They welcomed her home in November 2018.

"I did everything in my power to make sure that we could get Blue home," Wendy Kang told TODAY. "After all the stories I've heard, I know for sure Blue is one of the reasons why BK is standing here with me and he's alive."

Now Blue, 11, enjoys retirement in Georgia with the Kang family, which includes two sons, five dogs and two cats. Her favorite pastime is cuddling.

Earlier this year, Blue had a cancer scare. Fortunately, the mass in her mouth turned out to be benign, but the experience motivated the Kangs to submit an application to the 2020 American Humane Hero Dog Awards. Blue is now a semifinalist in the military dogs category of the competition.

"Military dogs work side-by-side with our warriors, facing the same trials and dangers in order to keep our nation safe," said Dr. Robin Ganzert, president and CEO of American Humane, in an email to TODAY. "Their valor and sacrifices deserve to be better recognized.

Byung Kang said he's grateful not just for Blue but for all military dogs.

"These working dogs, they will give up their life for us," he said. "So we should be thankful to them and respect them and above all, trust the dog because dogs will not lie."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

CYBER NEWS

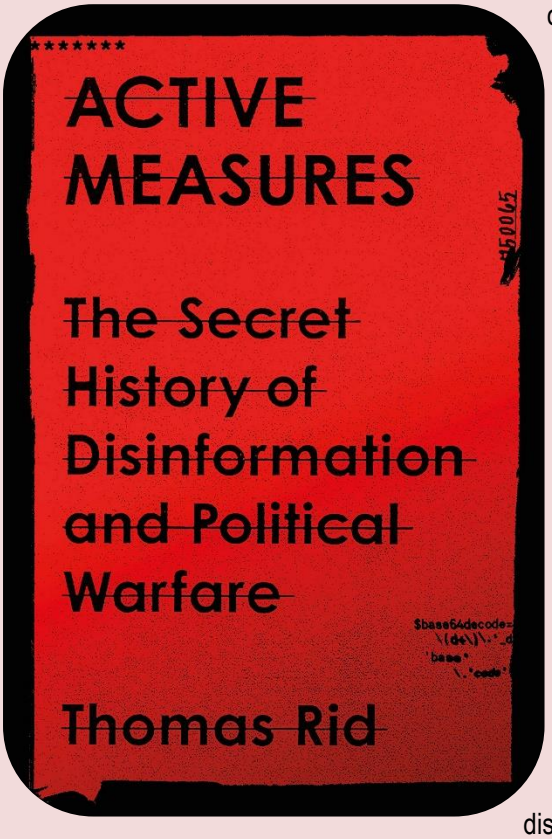
The Dark Arts of Disinformation Through a Historical Lens

By Arthur Martirosyan

Source: http://www.homelandsecuritynewswire.com/dr20200522-the-dark-arts-of-disinformation-through-a-historical-lens

Book review: Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (Farrar, Straus and Giroux, April 2020)

May 22 – History matters because sometimes it repeats itself. In his pioneering analysis of modern disinformation warfare from a historical perspective, Dr. Thomas Rid posits from the outset that "only by taking careful and accurate measure of the fantastic past of disinformation can we comprehend the present, and fix the future." When a political scientist writes a history book, you should still expect, if not a mid-range theory, then at least a thesis with a normative conclusion of recommendations for policy-making or problem-solving. Rid's timely book on the history of "active measures" by Soviet and post-Soviet Russian special services, along with those of other Eastern bloc and Western countries, is no exception. Rid writes that the merger of new technologies and the old school of strategic deception have made it "easier than ever to test, amplify, sustain and deny active measures, and harder than ever to counter or suppress rumors, lies and conspiracy theories."



"Active Measures" offers over a dozen case studies, organized chronologically, of operations run by disinformation warriors in the past hundred years. Rid weaves the historical canvas from a vast array of primary sources, mostly from the declassified documents of the U.S. Central Intelligence Agency as well as from the archives of East Germany, Czechoslovakia and Bulgaria, along with numerous secondary sources. If previously narratives were scattered throughout the memoirs of spymasters, the accounts of Soviet, Russian, Eastern bloc intelligence defectors and archival documents, now students of psychological warfare can find the outstanding cases in one volume, making it a "must-read," in my view. Given Rid's German background and that he teaches classes in information security at Johns Hopkins University, it should not be surprising that the most convex and detail-rich vignettes are about the operations of the East German Ministry for State Security (STASI; in particular, the author has drawn information from the archives of STASI's Department X, a disinformation unit and the more recent cases of Russian hacking and data leaking intended to weaken the targeted adversaries.

Although Soviet and Russian operations are thoroughly researched and evidenced, they contain some vexatious inaccuracies in the use of primary sources. For example, Rid asserts that at a March 1992 meeting with students of the Moscow State Institute of International Relations (MGIMO), "Primakov revealed that the AIDS story was 'created in the cabinets of the KGB' and had simply aimed to distract from the Red Army's use of chemical weapons." A quick fact-check of the reference reveals that Yevgeny Primakov, then the head of Russia's Foreign Intelligence Service (SVR) did not say a word about "the Red Army's use of chemical weapons" mentioned in that MGIMO meeting.

More critically, I was least convinced by Rid's claim that "the U.S. intelligence retreated from the disinformation battlefield almost completely … [w]hen the Berlin Wall went up in 1961 … and the West deescalated as the East escalated." As evidenced by Alvin Snyder, United States Information Agency (USIA) veteran, the political warfare didn't subside. On the contrary, I believe that it was on the rise in the 1970s and 80s. This is also confirmed by former U.S. Defense Secretary Robert Gates: "Most importantly, contrary to conventional wisdom, the Carter administration turned almost from the outset to CIA to carry out covert actions … Throughout that year and the next, CIA was asked to step up its activities targeted inside the USSR."

Moreover, a case in the history of the Cold War that, in my view, fits Rid's definition of the political warfare is conspicuously omitted: the story of U.S. President Ronald Reagan's Strategic Defense Initiative (SDI). The U.S. president seemed to have genuinely believed the so-called Star Wars program could defend America from ballistic missiles, but some saw it as a disinformation ploy against America's Cold War archenemy. The New York Times reported in 1993 that "the scheme deceived not only the Kremlin, but Congress, defrauding the American people of billions of dollars that could have been spent on real defense and domestic programs." In addition, Oleg Gordievsky, a Soviet

defector, wrote that it was a "large-scale disinformation operation" designed to force the Soviet negotiators into making concessions. One could argue that this political warfare operation was one of the most successful of the twentieth century because it achieved its goal: the Soviet leadership fell for it, hook, line and sinker.

Rid's lucid text reaches its crescendo when he gets to modern day active measures, as they are in his domain of cybersecurity. It is in the last pages that he makes the most compelling arguments for why history matters. Sometimes it repeats itself. Take the 1950s highly professional and effective CIA operation LC-Cassock, for example. It was a forgeries factory aimed at East Germany, an echo of a now more farcical and sloppier version—the Internet Research Agency (IRA) in St. Petersburg, also known as the "troll factory." Rid convincingly demonstrates why the troll factory was not effective in terms of its impact on 2016 U.S. voter preferences when measured by any matrix. "It is unlikely that the trolls convinced many, if any, American voters to change their minds: the overall volume of IRA activity [on Facebook] was lower than reported; a lot of the activity was audience-building; only 8.4 percent of IRA activity was election related, and the Russian messaging mostly stayed within echo chambers," Rid writes. "On Twitter, the IRA's impact practically vanished in the staggering number of election-related tweets … [t]he troll den generated less than 0.05 percent of all election-related posts. The IRA, according to the data released by Twitter, boosted candidate Donald Trump's retweet count with only 860 direct re-tweets over the entire campaign." And yet, Rid writes, "the House Democrats' release of the Facebook ads turned the ads, and the trolls' wider Facebook outreach, into a spectacular disinformation success story." And the overreaction by "the mainstream press generated the actual effect of the disinformation operation."

The volume is replete with many other lessons from the history of active measures. Deniability and the ability of intelligence agencies to learn from each other's "best practices" to surprise the opponent with a new modification of the mutated virus-like disinformation operation stand out among others. One example is *Schlagzeug*, the CIA-funded popular jazz magazine that featured one or two subversive articles targeting East Germans. Then, in 1958, the Soviet disinformation operators forged the CIA's own forgery, *Schlagzeug,* to disseminate Moscow's messages in West Germany.

Yet the most important merit of the book is in nudging the reader to think what's next in this conflict. As a specialist in conflict management, I inferred from reading "Active Measures" that there are essentially three options: 1. do nothing; 2. retaliate in an eye-for-an-eye replay of Cold War-era active measures; or 3. negotiate a new arrangement and set of rules.

The first option is the worst thing that can happen in a world facing epidemiological, climate change, cyber-terrorism and nuclear proliferation challenges. In the second option, if the U.S. were to play Russia's game by escalating retaliatory "political warfare," this would hardly assure a clear victory as the entire world could go blind through unintended consequences, as manifested by the Shadow Brokers case of the devastating leak of NSA hacking tools. The third option, however, is still possible. In fact, it has happened before. Alvin Snyder noted that in 1987, Soviet leader Mikhail Gorbachev told Charles Wick, the director of the USIA, "No more disinformation. I don't want politicians and bureaucrats creating all these tensions anymore, disinformation and all that. It's going to be a new day." Wick, in response, suggested that there should be regular meetings between him and his counterpart, Alexander Yakovlev, "for the purpose of improving communication, reducing conflict and putting our information relations on a basis of truth, fact and reciprocity."

But for the third option to materialize, it starts with understanding Russia today. In some limited ways it does resemble the besieged fortress of the Bolshevist Russia of the Operation Trust (1922-1927) days. In the words of George Kennan, it was the combination of Marx and Clausewitz that made Leninist Russia a formidable adversary. The Kremlin no longer has Marx in that combination, and it has no global mission of the Leninist scale. Putin's defensive-aggressive Russia is less interested in running the world than in ensuring that other powers cannot or dare not attempt to thwart it. What's missing now, therefore, is the political will of skilled leaders with realist mindsets to negotiate the norms and redlines in relations between the U.S. and its allies on one side, and Russia on the other. Whoever these leaders are going to be, Rid's book will provide them and their staff with valuable analyses of how the combination of traditional active measures tools and technology can make the world even less predictable and even more dangerous.

***Arthur Martirosyan** is a senior consultant with CMPartners.*

Cyber Terrorism: Why It Exists, Why It Doesn't, and Why It Will

By Stefan Soesanto

Source: https://isnblog.ethz.ch/cyber/cyber-terrorism-why-it-exists-why-it-doesnt-why-it-will

May 13 – The conversation on cyber terrorism began in the late-1990s amidst a wave of high-profile terrorist attacks in the United States, including the bombing of the World Trade Center in 1993 and the Oklahoma bombing in 1995. By 1997, the US Department of Defense conducted its first ever no-notice information warfare exercise to test the cybersecurity of its own systems, and in the same year, the Marsh Commission report on critical infrastructure

protection put the growing cyber threat landscape on the policy map in Washington.[2] Following the simultaneous bombings of the US embassies in Kenya and Tanzania in 1998 and the subsequent rise of al-Qaeda, terrorist attacks in and through cyberspace were seen as a potential future threat vector to the homeland. In October 1999, the Naval Post Graduate School prepared the first and to date most comprehensive study on 'cyberterror' for the US Defense Intelligence Agency.

The 1999 study included numerous definitions and statements that outlined the contours of cyber terrorism research. The authors for example noted that "*terrorist use of information technology in their support activities does not qualify as cyberterrorism*." Similarly, they also excluded script kiddie techniques, including dictionary attacks, spoofed emails, and the bombardment of e-mail inboxes. Overall, the study narrowly defined cyber terrorism as "*the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological*."[3] For a study compiled in 1999, this was a well-rounded framework. The only problem was that, in the United States, all cases that could theoretically fit the profile are statutorily considered either acts of cybercrime acts under the Computer Fraud and Abuse Act (18 U.S.C. 1030), or deemed armed attacks/acts of aggression under international law that would trigger the entire toolbox of US national defense mechanisms. For the last 20 years, cyber terrorism researchers have unsuccessfully tried to carve out their own space that could stand apart from cybercrime, hacktivism, and offensive military cyber operations. It should thus not come as a surprise that, writing in 2012, Jonalan Brickey still had to explain that cyberterrorism could be defined as "*the use of cyber to commit terrorism*," or characterized as the "*use of cyber capabilities to conduct, enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change*."[4] Similarly in 2014, Daniel Cohen literally wrote a book chapter on 'cyber terrorism: case studies' in which all examples are either cases of hacktivism, cybercrime, or nation state operations.[5]

Different government approaches

With cyber terrorism research hitting a wall very early on, some notions of cyber terrorism were nonetheless picked up by governments and agencies alike. 7000 miles away from Washington D.C., the Japanese government embarked on its mission to combat what it termed 'cyber terror' in the year 2000, when a combination of cyber-linked incidents caused by Japanese left-wing extremists, Chinese nationalistic hacktivist, and the Aum Shinrikyo doomsday sect, shook the public's confidence. In December 2000, Tokyo implemented an Special Action Plan which defined cyber terror as "*any attacks using information and communication networks and information systems that could have a significant impact on people's lives and socio-economic activities*."[8] In practice, this included everything from DDoS attacks, and the defacement of websites, to the deployment of highly advanced tooling like Stuxnet. Curiously, today, Japan's National Police Agency literally uses these three categories to officially define cyber terror.

For the Japanese government the primary motivation to introduce the term cyber terror was to mobilize government resources and secure the buy-in from critical infrastructure providers to build-out the nation's cybersecurity posture. Cyber terror was thus initially not viewed as a specific form of cybercrime or a distinct area of national defense but was more aching to a natural hazard that could negatively affect society as a whole. Over the years, the cyber terror narrative naturally crumbled as more precise definitions, distinctions, and insights degraded the terrorism aspect. Notwithstanding these developments, the term is still widely used in Japan and has practical implications for public-private cooperation. For example, the National Police Agency's 'Cyber Terrorism Countermeasure Councils' facilitate public-private partnerships and outreach on the prefecture level through discussions, lectures, and demonstrations. Meanwhile the 'Cyber Terrorism Countermeasures Council,' maintained by the Tokyo Metropolitan Police, serves a coordinating hub to secure all big events in Japan –including the 2021 Tokyo Olympics and Paralympics.

In the United States, the attacks on 9/11 introduced a host of legislative measures to tackle the threat of cyber terrorism. Stand out from the crowd are the US Patriot Act of 2001 and the Terrorism Risk Insurance Act of 2002. The Patriot Act provided federal law enforcement new tools to detect and prevent terrorism, including the "*authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses*" (Section 202), "*emergency disclosure of electronic communications to protect life and limb*" (Section 212), and "*interception of computer trespasser communications*" (Section 217).[7] According to the Department of Justice's 2005 Report, Section 202 was used on only two occasions which both "*occurred in a computer fraud investigation that eventually broadened to include drug trafficking*."[8] Meaning, it was never used to tackle a case of cyber terrorism. By contrast, section 212 was used, according to the DoJ's 2004 Report to

"*successfully respond to a cyberterrorist threat to the South Pole Research Station.*"[9] While it is indeed true that in May 2003 Romanian hackers intruded into the network of the National Science Foundation's Amundsen-Scott South Pole Station and threatened to "*sell the station's data to another country and tell the world how vulnerable* [the systems] *are*," the DoJ's 2004 Report falsely claims that "*the hacked computer also controlled the life support systems for the South Pole Station*."[10] In fact, this dramatic detail was not included in any of the FBI's public releases and according to internal memos, the station's network was "*purposely* [less secure] *to allow for our scientists at this remotest of locations to exchange data under difficult circumstances*," and was penetrated two months prior by another hacking group. When it comes to section 217 of the Patriot Act, under which "*victims of hacking and cyber-terrorism* [could] *now obtain law enforcement assistance in catching intruders on their systems*," neither the DoJ's 2004 nor the 2005 report offer any known connection to a cyber terrorism case. Instead, the Sunsets Report merely points out that section 217 was used in "*investigations into hackers' attempts to compromise military computer systems*" and serious criminal cases, such as "*an international conspiracy to use stolen credit cards*." [11] Overall, the DoJ's own reporting shows that even a law that specifically combats terrorism was not utilized to investigate one case of cyber terrorism.

In fact, the closest the DoJ has gotten to successfully prosecute an act of cyber terrorism was back in 2016, when 20-year old Ardit Ferizi –a citizen of Kosovo– was sentenced to 20 years in prison for "*accessing a protected computer without authorization and obtaining information in order to provide material support to ISIL*." and according to Assistant Attorney General for National Security John Carlin, "*this case represents the first time we have seen the very real and dangerous national security cyber threat that results from the combination of terrorism and hacking*." [12] But far from conducting an elaborate cyberattack, Ferizi only gained sys admin level access to a US company server that hosted the personally identifiable information of tens of thousands of US customers – including military personnel and government officials. Ferizi then proceeded to cull the data to approx. 1300 military and government individuals and forwarded it in June 2015 to Junaid Hussain –a former hacktivist and at the time ISIS' most prolific English-language social media propagandist. While Ferizi was subsequently arrested in Malaysia and extradited to the United States in October 2015, a US drone strike took out Junaid at a petrol station in Raqqa, Syria, in August.[13] The incident marked the first publicly known case of an enemy cyber operator being specifically targeted on the kinetic battlefield.

In contrast to the Patriot Act, the Terrorism Risk Insurance Act (TRIA) is a different animal. TRIA became necessary when following the 9/11 attacks, reinsurers began to exclude terrorist attacks from their coverage, with in turn forced insurance companies to excluded them, which I turn stalled development projects in their tracks due to the unavailability of terrorism risk coverage and uncertainty as to who would pay if another terrorist attack occurred. To ease the jitter, TRIA put in place a three-year Terrorism Insurance Program under which the US government would "*share the losses on commercial property and casualty insurance should a foreign terrorist attack occur, with potential recoupment of this loss sharing after the fact*."[14] The program has been reauthorized multiple times and is set to expire at the end of 2027. What makes TRIA important for the contextualization of cyber terrorism is that it does not specifically exclude cyber terrorism nor generally includes it from coverage. Meaning, the way terrorism is defined under TRIA would make it theoretically also applicable for every cyber incident if the Secretary of the Treasury, the Secretary of State, and the Attorney General of the United States, certify the incident to be act of terrorism or a "*violent act or an act that is dangerous to (I) human life; (II) property; or (III) infrastructure*." (Section 102). Complicating the matter further is that in 2016 the US Department of the Treasury issued a notice clarifying that cyber liabilities in cyber insurance policies are considered "property and casualty insurance" under TRIA. Meaning, cyber terrorism coverage cannot be excluded from any cyber insurance policy. Now, given that many insurers have chosen to exclude acts of war and other items from their cyber insurance policies, cyber terrorism faces a fundamental theoretical conundrum. Let's assume for a moment we would ask our insurance company to draw up a cyber insurance that does not cover anything. Nothing at all. Let us also assume that a cyber incident occurs, and the US government classifies it as an act of terrorism. Would my cyber insurance –which does not cover anything– still have to cover the incident under TRIA? If true, then is an act of cyber terrorism only cyber terrorism when the US government says it is? Similarly, how would an insurance company correctly price my cyber insurance premium? Would they sell it to me for almost nothing, since it does not cover anything, or would the probability of a cyber incident being identified by the US government as an act of cyber terrorism form the baseline for the premium calculation?

Apart from the US and Japan, numerous other governments have sporadically incorporated the term cyber terrorism into their strategic documents for one reason or another. Austria's 2013 Cyber Security Strategy for example defines cyber terrorism "*as a politically motivated crime of state and/or non-state actors."*[15]And South Korea's 2012 Defense White paper specifically calls out "*various forms of cyber terrorism: Hacking, DDoS attacks, denials of service, logic bombs, Trojan horses, Worm viruses,* [High-Energy Radio Frequency] *guns etc.*"[16] Looking at the variety of cyber terrorism interpretations out there, it ought to be obvious that from a strategic point of view, the conversation on cyber terrorism is all over the place everywhere. But what if we could introduce some sense of sanity into the discussion by operationalizing fragments of cyber terrorism to clarify what threat vectors we ought to be looking for? Let's give it a try.

Operational thinking

From an operational point-of-view, we have to treat an act of cyber terrorism as a black box, similarly to how first responders treat any incident affecting their network. Meaning, for our analysis it does not matter who is behind the attack. It could be a non-radicalized individual with no links to any terrorist organization. It could be a hardcore terrorist group that regularly interfaces with cybercriminals. Or it could be a nation state. Equally, because the attacker's political, religious, and ideological motivations remain largely hidden from us, the "*tie to terrorism may not reveal itself for days, weeks, or months, if ever.*"[17] Therefore our focus has to be on technical attribution e.g. (a) how did the attacker do it, (b) when did he do it, and (c) did he achieve his objective? Analytically, we are thus trying to discern whether the attack was targeted, coordinated, and persistent, rather than diffuse, opportunistic, and random.

The second item we have to de-conflict is whether the attack actually terrorized the intended target. The reason for this is simple: Image there is a blackout affecting your entire neighborhood. Then the lights come back on for a moment –everyone is relieved– and then the lights go out again. There are numerous plausible explanations as to why the blackout occurred, and in most cases, those affected might never get to know the underlying reason after the incident is finally fixed.Now, compare that to a blackout that only affects your apartment. You go into the kitchen and your smart-light bulbs do not light up. You look at bulb, tinker around with your network, and search for possible fixes online, but you cannot locate the problem. Then suddenly, the lights go on… and switch off again. Which one of those two blackouts would terrify you more? Analytically, the only two differences that are important to us are: (a) the distance between the attacker and the intended target –e.g. how personal is it?–, and (b) the psychological resonance effect emanating from the attack –e.g. how "terroristic" is it.

Let's briefly showcase this with the help of one real-life case.

In 2007, then 14-year old Polish teenager Adam Dabrowski was struck by a combination of curiosity and evil ingenuity that led him to conduct nightly break-ins into the tram depot of the city of Lodz. His objective: figuring out how the tram network worked and whether he could control the trams remotely. Combined with months of online research and his electronic classes at school, Adam succeeded sometime in early-2008 in converting an old tv remote to exploit a flaw in Lodz' infrared based signaling system. Under the right circumstances –as Adam figured out– it was possible to capture the track switching signal at one junction point and play it back at another junction point to get the same result.[18] According to Miroslaw Micor, spokesman for Lodz police, Adam subsequently treated the Lodz tram network "*like any other schoolboy might a giant train set, but it was lucky nobody was killed. Four trams were derailed, and others had to make emergency stops that left passengers hurt. He clearly did not think about the consequences of his actions.*"[19]

Now imagine if Adam would have continued his spree and would have never had been caught. Would this qualify as a case of cyber terrorism? From a strategic point-of-view it ticks several boxes. First, Adam succeeded in collecting actionable intelligence on a critical infrastructure target. Second, Adam was persistent enough to build a targeted exploit over month of dedicated work. And third, Adam did cause bodily harm by disrupting tram operations with his device. But what we are strategically lacking is any information on the attacker's motivation, his objective, and whether he is potentially connected to a terrorist cell. Meaning, Adam's campaign only becomes terrorism in case of self-attribution, e.g. if Adam leaves behind clues that explain his reasoning or a tape that shows him declaring his allegiance to a terrorist group.

Operationally, we do not need any of that information. Technically, Adam's campaign fulfills the notion of targeted, coordinated, and persistent. But on the second pillar it notably falls short. In terms of how personal the attack was, our investigation would have to figure out whether there were any common targets in the trams that were derailed and whether the campaign had any major repercussions for the company that maintains the Lodz tram network. In both instances we will not find much. Similarly, given the low severity and frequency of the incidents, the fallout radius of the attack's psychological effect will be fairly small. To turn Adam –operationally– into a terrorist he would have to do one of two things: Either build more devices and get more people involved to increase the frequency and spread of the derailments. The downside of which is an expansion of trust, information sharing, and a decline in absolute control (e.g. outsourcing). Or, Adam could walk in the opposite direction by targeting specific trams at specific times to terrorizing specific individuals. Which would necessitate an information gathering operation aimed at mapping real-time target locations, habitual movement patterns, and potential insights into a target's social interactions (e.g. espionage).

In essence, by closing the proximity to the desired target and persistently engaging it over time, the modified campaign becomes the vehicle for the subsequent creation of terror –

even though the individual attacks stay the same. Thus, rather than looking at the severity of a cyberattack, e.g. physical destruction and disruption –investigating attacker motivations, or question the feasibility of terrorism in cyberspace altogether, analyzing adversarial campaign tactics and maneuvering behavior will provide a much richer framework to explore, replicate, and defend against the terror component. Indeed, valuable lessons have yet to be learned from issues as disparate as cyber stalking and mental recovery after a cyber incident, to hacking back in the civilian realm and converging military cyber operations with information warfare campaigns.[20]

Conclusion

In sum, cyber terrorism is probably best viewed as an operational tactic aimed at a distinct psychological outcome rather than a field of research that connects the cyber domain at the hip to terrorism in real space. Notably, while cyber terrorism research and policy has hit somewhat of a deadlock in recent years, leveraging tactical approaches to create terror in and through cyberspace is only at its beginning.

Notes

1 See: Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004; Zahri Yunos and Sharifuddin Sulaman, 'Understanding Cyber Terrorism from Motivational Perspectives', *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 1-13; Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, Vol. 7, No. 11-4, November 2002.
2 'Critical Foundations. Protecting America's Infrastructures', October 1997.
3 Defense Intelligence Agency, 'Cyberterror. Prospects and Implications', pp. 10 and 9, respectively.
4 Jonalan Brickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *CTC Sentinel*, August 2012, Vol. 5, No. 8, p. 6.
5 Daniel Cohen, 'Cyber terrorism: Case studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13.
6 Prime Minister's Office, 'Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure', December 15, 2000.
7 Public Law 107–56, October 26, 2001.
8 Department of Justice, 'USA Patriot Act. Sunsets Report', April 2005, p. 6.
8 Department of Justice, 'Report from the Field: The USA Patriot Act at Work', July 2004, p. 33.
10 'Report from the Field', p. 27.
11 'USA Patriot Act. Sunsets Report', p. 48.
12 Department of Justice, 'ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison', *Justice News*, September 26, 2016.
13 Frank Gardner, 'UK jihadist Junaid Hussain killed in Syria drone strike says US', *BBC News*, August 27, 2015.
14 Congressional Research Service, 'Terrorism Risk Insurance. Overview and Issue Analysis', December 27, 2019, p. summary.
15 Federal Chancellery, 'Austria Cyber Security Strategy', 2013, p. 21.
16 Ministry of National Defense, 'Defense White Paper', 2012, p. 10.
17 ISE Bloggers, 'Unpacking Cyber Terrorism', May 31, 2016.
18 John Bull, 'You Hacked: Cyber-Security and the Railways', *London Reconnections*, May 12, 2017.
19 John Leyden, 'Polish teen derails tram after hacking tram network', *The Register*, January 11, 2008.
20 Ellen Nakashima, 'U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election', *The Washington Post*, December 25, 2019.

***Stefan Soesanto** is a Senior Researcher in the Cyber Defense Team at the Center for Security Studies (CSS) at ETH Zurich.*

ISIS Cybersecurity Magazine Warns of 'Nightmare' Windows in 'Fierce War' Online

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/isis-cybersecurity-magazine-warns-of-nightmare-windows-in-fierce-war-online/

May 26 – A new 24-page cybersecurity magazine for ISIS supporters walks jihadists through step-by-step security for smartphones — while encouraging them to use a computer instead for more secure terror-related business — and warns of "nightmare" Windows collecting user data from geolocation to browsing history.

The inaugural issue of "The Supporter's Security," published in English and Arabic versions, was produced by the Electronic Horizons Foundation, which launched in January 2016 as an IT help desk of sorts to walk ISIS supporters through how to encrypt their communications and otherwise avoid detection online while coordinating with and recruiting jihadists.

"It is time to face the electronic surveillance, educate the mujahideen about the dangers of the Internet, and support them with the tools, directives and security explanations to protect their electronic security, so that they don't commit security mistakes that can lead to their bombardment and killing," the group said in its founding announcement.

The EHF publishes a weekly cybersecurity bulletin consisting of a handful of headlines pulled from tech news publications, including topics ranging from data breaches to Google and Windows vulnerabilities. The group has also released a series of print and video tutorials covering a range of mobile security and dark-web how-tos. (Electronic Horizons Foundation)

The new magazine notes that "supporters rely on computers for media work and publishing, starting with design, montage, programming and publishing on social networks, communication, coordination and management of work, and the most popular operating systems that supporters use is Windows developed by Microsoft, which is a security nightmare as it collect all your data, and sends it to Microsoft."

ISIS supporters are urged to use alternate operating systems such as Qubes, Tails or Whonix. EHS follows this advice with two pages of detailed Whonix system installation instructions.

The magazine laments that tech development is "led by polytheists" and "they have the upper hand of it, they work their efforts day and night to use it against the religion of Allah, and humiliate the Muslims, so that they become under their control and mercy, and move under their surveillance."

Islam "has obligated in such a case that Muslims should learn and prepare what strengthens them," the EHF argues, and "one of the most important tools of our time is Information technology."

"Some of it needs specialization and long study, and some of it needs some serious attention, and Muslims are in such big need for both of them, the need is urgent," the group adds. " …We are inside a fierce war, our sites and accounts in social media got deleted because the intelligence services realize the danger of Muslims gaining security awareness, which will make it difficult to track them and cut off the ways for them to arrest the monotheists, but we do not leave this field, Allah willing, until Allah decides what needs to be done."

The magazine begins with a lengthy assessment of the pros and cons of smartphone use, with the former limited to cost and accessibility and the latter being that "the Mujahideen started to use smartphones to communicate, publish, plan and work without knowing the real security risks they face."

"The Mujahideen have been warned more than once about the danger of smartphones, which led to the arrest of many brothers due to the security negligence, so you must realize as a supporter of the truth that the security measures that need to be applied for you are completely different from the security measures used by anyone else," the article states. "Understand the security threats facing you and how to choose the appropriate tools and methods to conduct your business and bypass electronic control, which includes every device connected to the Internet or cellular networks now."

EHF walks through various operating systems for Android in their setup guide, pages of graphics detailing what settings to use on both Android and iPhone to better secure their communications. "Good iOS security starts with having a really strong passcode," the group advises. "If this is something that's easily guessable then everything else you do is pretty much pointless."

The writers acknowledge that choosing the right smartphone can be confusing for a jihadist, thus let readers know they can "contact us via technical support accounts to guide you to the phone that is suitable for you."

The ISIS cyber group also highlights "wrong security practices" including browsing the internet without Tor or VPN, downloading apps from third-party sources, failing to encrypt the device or storage devices, neglecting to install security updates, failing to use fake credentials on social media, and using social media via apps instead of logging on through a browser. Jihadists are also warned against opening potentially malicious links that can open them to a security breach.

"You must trust the underlying operating system running the program," EHF says. "The tasks of the program are limited to what the operating system tells it to do, so you must trust that the operating system prevents leaks of the tasks you are working on for anyone else."

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Previously she was an editorial board member at the Rocky Mountain News and syndicated nation/world news columnist at the Los Angeles Daily News. Bridget is a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is a Senior Risk Analyst for Gate 15, a private investigator and a security consultant. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, New York Observer, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.*

Ethical guidelines for COVID-19 tracing apps

By Jessica Morley, Josh Cowls, Mariarosaria Taddeo and Luciano Floridi (University of Oxford)
Nature 582, 29-31 (2020)
Source: https://www.nature.com/articles/d41586-020-01578-0

May 28 – Technologies to rapidly alert people when they have been in contact with someone carrying the coronavirus SARS-CoV-2 are part of a strategy to bring the pandemic under control. Currently, at least 47 contact-tracing apps are available globally (see go.nature.com/2zc1qhk). They are already in use in Australia, South Korea and Singapore, for instance. And many other governments are testing or considering them.

Here we set out 16 questions to assess whether — and to what extent — a contact-tracing app is ethically justifiable. These questions could assist governments, public-health agencies and providers to develop ethical apps — they have already informed developments in France, Italy and the United Kingdom. They will also help watchdogs and others to scrutinize such technologies.

What do COVID-19 contact-tracing apps do? Running on a mobile phone, they inform people that they have spent time near someone with the virus. The contacts should then respond according to local rules, for example by isolating themselves. Prompt alerts are key because the incubation time of the virus is up to two weeks[1–4].

These digital interventions come at a price. Collecting sensitive personal data potentially threatens privacy, equality and fairness. Even if COVID-19 apps are temporary, rapidly rolling out tracing technologies runs the risk of creating permanent, vulnerable records of people's health, movements and social interactions, over which they have little control.

More ethical oversight is essential. So far, such concerns have focused on rights to privacy (see go.nature.com/3e7jntx). Some governments have pledged to protect data privacy (see go.nature.com/3qrwfe8). Apple and Google are developing a common interface to support apps that do not require central data storage (see *Nature* http://doi.org/dwc6; 2020). However, other ethical and social considerations must not be cast aside in the rush to quell the pandemic.

For instance, contact-tracing apps should be available and accessible to anyone, irrespective of the technology needed or their level of digital literacy. Yet many apps work only with certain phones. Australia, for example, has no plans to make its app work with phones that use software older than Apple's iOS 10 or Android 6.0. In the United Kingdom, around one-fifth of adults do not use a smartphone, and so might be excluded from a digital contact-tracing programme.

Rolling out an app without considering its wide ethical and social implications can be dangerous, costly and useless. For example, Bluetooth signals that show the proximity of two individuals' mobile phones are not a certain indicator of infection risk — two people might be in the same space but physically separated, for example, by a wall. A high level of false positives from such an app (for instance, as a result of self-reporting) could lead to unjustified panic. And minimal protections against false negatives (people not using the app to report that they are unwell) could spur a false sense of safety in others and increase the risk of infection.

Guidelines: is this contact-tracing app ethically justifiable?

Those responsible for contact-tracing apps should answer the following.

Principles: is this the right app to develop?

1. Is it necessary?
- Yes, it must be developed to save lives (+).
- No, there are better solutions (–).

2. Is it proportionate?

• Yes, the gravity of the situation justifies the potential negative impact (+).
• No, the potential negative impact is disproportionate to the situation (–).

3. Is it sufficiently effective, timely, popular and accurate?

• Yes, evidence shows that it will work, is timely, will be adopted by enough people and yields accurate data and insights (+).
• No, it does not work well, is available too late or too early, will not be used widely, and is likely to collect data that have false positives and/or false negatives (–).

4. Is it temporary?

• Yes, there is an explicit and reasonable date on which it will cease (+).
• No, it has no defined end date (–).

Requirements: is this app being developed in the right way?

5. Is it voluntary?

• Yes, it is optional to download and install (+).
• No, it is mandatory and people can be penalized for non-compliance (–).

6. Does it require consent?

• Yes, people have complete choice over what data are shared and when, and can change this at any time (+).
• No, default settings are to share everything all the time, and this cannot be altered (–).

7. Are the data kept private and users' anonymity preserved?

• Yes, data are anonymous and held only on the user's phone. Others who have been in contact are notified only that there is a risk of contagion, not from whom or where. Methods such as differential privacy are used to ensure this. Cyber-resilience is high (+).
• No, data are (re)identifiable owing to the level of data collected, and stored centrally. Locations of contacts are also available. Cyber-resilience is low (–).

8. Can users erase the data?

• Yes, they can do so at will; all data are deleted at the end point (+).
• No, there is no provision for data deletion, nor a guarantee that it can ever be deleted (–).

9. Is the purpose of data collection defined?

• Yes, explicitly; for example, to alert users that they have encountered a potentially infected person (+).
• No, the purposes of data collection are not explicitly defined (–).

10. Is the purpose limited?

• Yes, it is used for tracing and tracking of COVID-19 only (+).
• No, it can be regularly updated to add extra features that extend its functionality (–).

11. Is it used only for prevention?

• Yes, it is used only to enable people voluntarily to limit spread (+).
• No, it is also used as a passport to enable people to claim benefits or return to work (–).

12. Is it used for compliance?

• No, it is not used to enforce behaviour (+).
• Yes, non-compliance can result in punishment such as a fine or jail time (–).

13. Is it open-source?

• Yes, the code is publicly available for inspection, sharing and collaborative improvement (+).
• No, the source code is proprietary, and no information about it is provided (–).

14. Is it equally available?

• Yes, it is free and distributed to anyone (+).
• No, it is arbitrarily given only to some (–).

15. Is it equally accessible?

• Yes, it is user-friendly, even for naive users, and works on the widest possible range of mobile phones (+).
• No, it can be used only by those with specific devices and with sufficient digital education (–).

16. Is there a decommissioning process?

• Yes, there is a process for shutting it down (+).
• No, there are no policies in place (–).

The public might reject apps that breach principles of privacy, equality and fairness. This would frustrate the efforts and waste the resources being invested in developing and deploying such technology. Lack of consideration of ethics could erode trust in the government and public-health services — as happened last month, when the Norwegian

Data Protection Authority accused the Norwegian Institute of Public Health of failing to carry out a proper risk assessment of its contact-tracing app, **Smittestopp**.

Many approaches

Temporarily restricting some fundamental rights and freedoms might be ethically justifiable in the context of hastening the end of the pandemic. Quarantining individuals, for example, helps to prevent the spread of the disease. Arguably, it might be unethical not to use digital tracing apps when necessary. Nevertheless, much depends on the effectiveness of the app, the goal pursued, the type of system and the context in which it will be deployed.

Countries and regions are taking different approaches. China's Alipay Health Code app assigns a digital QR code to each user, which is colour-coded red, amber or green to indicate that person's quarantine status and thus their ability to move around. People quarantined in Hong Kong must wear an electronic bracelet that shares their location with local authorities through an app. Poland requires citizens to self-isolate for 14 days after returning from overseas, and to send geotagged 'selfies' to the police to prove they are at home. Singapore's TraceTogether app has been downloaded by about 25% of its population, much less than the 60% needed. This has led the country to introduce its SafeEntry system, which requires users to check in to public places using their national identity card or by scanning a QR code with their phone.

Apps differ in how they collect and store data. For example, they might rely on systems that are centralized, as in Australia and Singapore, or decentralized, as in Germany and Italy (see also *Nature* http://doi.org/dwc6; 2020). Centralized apps send pseudonymized data collected by a user's phone to a central database controlled by, for example, a national health agency, where contacts are matched. Decentralized approaches instead match contacts on the user's device (see go.nature.com/3e7jntx). Use of an app can be voluntary, as the European Commission recommended in April (see go.nature.com/2x2hrat), or not. India's app, for instance, is mandatory for citizens living in virus-containment zones and for all government and private-sector employees. Apps in Argentina and the United Kingdom ask users to self-report their symptoms, whereas the Norwegian app relies on the user having a formal diagnostic test.

More coordination is needed. Some supranational efforts to harmonize the apps are under way. The World Health Organization, for example, is developing a symptom-checking app that might also enable contact tracing in under-resourced countries. The European Data Protection Supervisor has called for a Europe-wide contact-tracing app[5]. The European Commission has outlined requirements for digital tracing solutions deployed in the European Union, including compliance with EU data protection and privacy rules[1].

Countries and regions should consider a broader set of ethical concerns, including equality and fairness. Government agencies and developers working under pressure might find it hard to make these judgement calls quickly. In other contexts, such as bioethics, ethical review boards typically have much more time to deliberate. Expert groups might be set up to advise, as France, Italy and the United Kingdom have done. (L.F. is a member of the UK National Health Service COVID-19 App Data Ethics Advisory Board; see go.nature.com/3cxyzrw).

Four principles

To be ethical, a contact-tracing app must abide by four principles: it must be necessary, proportional, scientifically valid and time-bound. These principles are derived from the European Convention on Human Rights, the International Covenant on Civil and Political Rights (ICCPR) and the United Nations Siracusa Principles, which specify the provisions in the ICCPR that limit how it can be applied.

However, there are many ways in which an app can meet these principles. To address this gap, we have synthesized 16 questions that designers, deployers and evaluators should answer (see 'Is this contact-tracing app ethically justifiable?'). For each, we give examples of how an app might be designed and used in a more (+) or less (–) ethically justifiable way. These questions apply to apps that have been released, as well as for those in development[6].

In theory, an ethical app should satisfy all 16 factors. The questions themselves might not be controversial, but the answers are likely to generate disagreement about whether and how much an app satisfies a factor, and which ethical factors should be a priority.

In practice, there will be trade-offs. These will depend on the laws, values, attitudes and norms in different regions, as well as on changes over time in the spread and scale of the virus and the available technology. For example, it might be more ethically justifiable to deploy an app that does not fully meet the stipulation that it should "work on the widest possible range of mobile phones" in a country with high smartphone penetration, such as South Korea — where more than 95% of people owned a smartphone in 2018. But it might be less justifiable in Japan, where 66% of the population did.

Similarly, what was ethically justifiable in one place yesterday might not be so tomorrow. For example, Germany shifted from a centralized to a decentralized app after some 300 experts

signed an open letter strongly criticizing the centralized approach. The same happened in Italy after Apple and Google announced their plan to support decentralized apps. Singapore could follow suit. Its centralized TraceTogether app was developed before the Apple–Google interface was available, and developers are now aiming to make it compatible.
An app's implementation strategy and impact must also be considered. Something that looked good on paper can turn out to be ineffective in practice. This was the case with the Australian COVIDsafe app. Concerns about third-party access to user data and low compatibility with phones running old operating systems have led to a low level of adoption. More than a month since deployment, the minimum threshold of 40% has not been met. This is making the app irrelevant for managing the pandemic in Australia.
If an app fails, it becomes unnecessary, and thus unethical. Apps that are no longer beneficial should be improved or decommissioned. A review and exit strategy must be in place to establish when and how fast this should happen. These assessments should be conducted by an independent body, such as a regulator or an ethics advisory board, and not by the designers or the government itself. Circumstances and attitudes are changing quickly, so the questions in our framework must be asked anew at regular intervals.

One chance
Governments might not have a second chance to get an intervention right — failure now could breach public trust for the foreseeable future. Governments, developers and deployers must ensure that COVID-19 contact-tracing apps satisfactorily address the ethical questions we set out. Apps that do not should not be deployed; alternatives should be considered.
Simply rolling out a tracing app without ethical consideration is not acceptable. Even in a crisis, a 'try-everything' approach is dangerous when it ignores the real costs, including serious and long-lasting harms to fundamental rights and freedoms, and the opportunity costs of not devoting resources to something else.

Cybercriminals Are Now Targeting Critical Electricity Infrastructure

By Henri van Soest
Source: http://www.homelandsecuritynewswire.com/dr20200605-cybercriminals-are-now-targeting-critical-electricity-infrastructure

June 05 – Amid the constant stream of news on the coronavirus pandemic, one event passed relatively unnoticed. On the afternoon of May 14, a company named Elexon was hacked. You probably haven't heard of it, but Elexon plays a key role in the UK's electricity market, and though the attack did not affect the electricity supply itself, as an academic who researches cybersecurity in the electricity system, I am worried. This near miss reveals just how vulnerable our critical infrastructure is to such attacks – especially during a pandemic.
Elexon plays an important role in the operation of the country's electricity system. In such a system, the levels of supply and demand need to be balanced at all times. Otherwise, the system becomes unstable, which can lead to blackouts. To avoid this, Elexon compares the amount of electricity that generators promise they will produce, with the amount of electricity that suppliers say will be consumed. Where needed, the company determines the difference in price and transfers funds between the parties on either side of the transaction.
The lockdown has made Elexon's role significantly more difficult. Usually, electricity demand is pretty fixed, as people broadly go to work, return home, cook dinner and watch TV at roughly the same hour every day. However, the lockdown has ripped up the rule book on all this. Despite many people staying at home, electricity demand has also dropped by about 20% compared to this time last year due to the closure of factories and businesses. In sum, it is a lot harder to correctly predict demand.
The drop in demand also means that less electricity is needed. The drop in demand also means that less electricity is needed. Because wind and solar power are now the cheapest forms of electricity available, coal and gas plants are generating less, and there has lately been a big increase in renewable energy sources in the overall mix. However, wind and solar power experience large swings in supply, depending on whether the sun shines and the wind blows. This again makes supply and demand more complicated to manage.

Held to ransom
The Elexon attack used ransomware, in which a computer virus encrypts the contents of a computer, and it can only be decrypted after a ransom has been paid, typically in bitcoin or another cryptocurrency. The most famous ransomware attack is no doubt the 2017 WannaCry attack, which particularly affected the UK's National Health Service.
Several reports indicate that the Elexon attack relied on REvil/Sodinokibi ransomware, the same as was used in a cyberattack on financial company Travelex on New Year's Eve 2019. The Travelex hack was traced back to a Russian hacking collective, and although it is notoriously difficult to attribute cyberattacks with certainty, it is likely that Elexon fell victim to

the same hackers. On June 1, the hackers posted some of the stolen Elexon data online, in an attempt to pressure the company to pay the ransom.

A cybercrime pandemic

The attack on Elexon does not stand alone. As countries around the world have locked down, cybercriminals have launched attacks on a wide range of targets, mostly using ransomware. The lockdown-induced rise in home-working has been a big enabling factor, as lots of professional communication now takes place over the general internet, which is a lot more insecure than using a local company network with a firewall around it.

Critical infrastructures have been hit particularly hard. In recent months, cyberattacks have been launched on hospitals, coronavirus research facilities, ports, water supply infrastructure, and the Brussels-based ENTSO-E, the European Network of Transmission System Operators for Electricity.

This sort of infrastructure is in the crosshairs for two main reasons. First, cybercriminals bet that operators will be less hesitant to pay ransom than other targets, because the continued operation of electricity, water, hospitals and so on is so important.

But it's also because their computer systems are often outdated. While it may seem paradoxical, the reason for this is the fact that critical infrastructures should always be available. When a system works fine, there is little incentive to change it, especially when changes to computer systems can easily lead to incompatibilities, errors or crashes. For instance, three years after the WannaCry attack, the NHS is once again exposed to an attack because many of its computers are still running on Windows 7, which is no longer supported.

Ransomware attacks are typically not very complicated. They make use of known software vulnerabilities that have already been patched, and the criminals specifically target those computers that have not been updated. These inherent vulnerabilities, combined with the lockdown-induced difficulties in balancing the electricity grid, mean that a more sophisticated cyberattack on Elexon could have had big consequences for the UK electricity system.

As it happens, the attack only affected Elexon's internal IT systems, and the rest of the electricity system, as well as the electricity supply itself, was not affected. But this should force us to think about how vulnerable our critical infrastructure is to cyberattacks.

What would have happened if the attack had indeed affected the electricity supply? It would have seriously hindered the UK's response to the pandemic, and it is possible that we would have struggled to get the power back up, as all resources are currently going into fighting the virus. In addition, it is unlikely that a lockdown without electricity and internet could be maintained for long. The fact that cybercriminals know this only makes our critical infrastructures more appealing targets.

***Henri van Soest** is Ph.D. Candidate in Land Economy, University of Cambridge.*

What's 5G, And Why Are People So Scared of It? Here's What You Need to Know

Source: https://www.sciencealert.com/what-s-5g-and-why-are-people-so-scared-of-it-here-s-what-you-need-to-know

June 06 – This year, there have been attacks on 5G towers around the world linked to coronavirus fears. Last year, the Belgian government halted a 5G test over radiation concerns. Switzerland is monitoring risks posed by the 5G network. A member of the UK House of Commons warned the parliament of the "unintended consequences" of the 5G upgrade.

5G fears have become mainstream. But their point of origin is anything but.

If you go digging into the claims behind these fears, you'll discover some truly wild conspiracy theories. Some people claim that 5G is in the same wavelengths as weapons. Or that it's being used by the military to break the enemy's spirit.

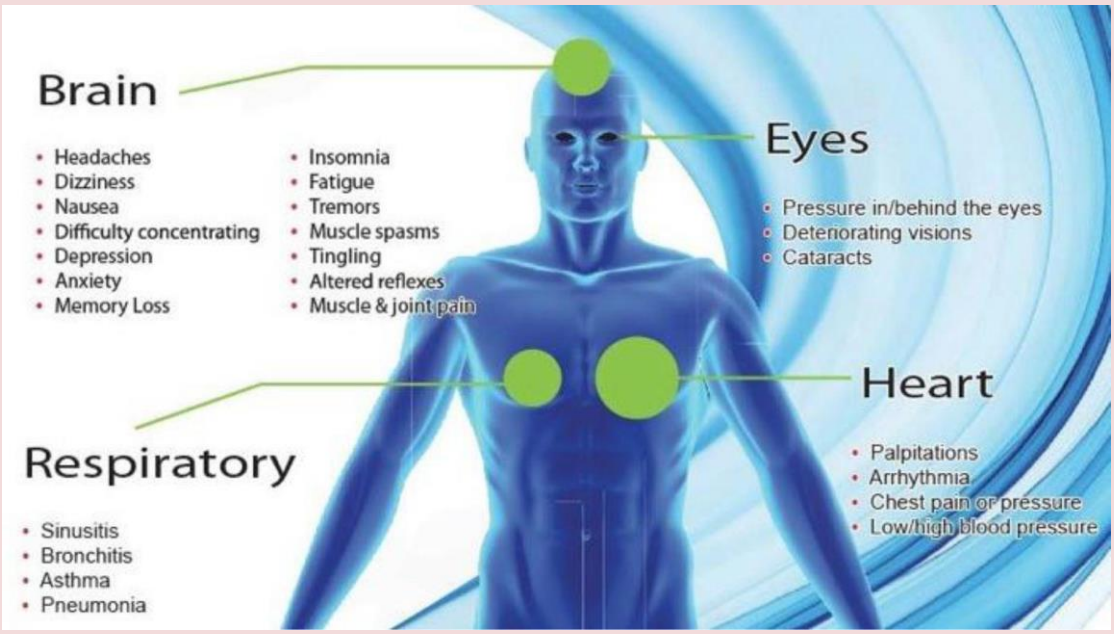
People have argued that the smaller wavelengths used in each new generation of mobile phone infrastructure have never been tested, and therefore we are guinea pigs for this technological experiment. By and large, claims about the harms of 5G are not far from gay frog conspiracies.

You'll be happy to know that none of those claims are true.

"The wavelengths that 5G uses and will use are all entirely safe and have been in research and testing for decades," Howard Jones, the head of technology communications at UK's mobile network provider EE, recently explained to *The Guardian*.

"It's a red herring to say it's a new technology and therefore hasn't been tested."
There's an awful amount of terror out there over a phone network. Chances are many people couldn't explain what 5G even is, so here's a brief overview of the actual technology.
When you use your phone, it interacts with a phone tower nearby, via radio waves. The phone tower then connects (also via radio waves) to a core network, which then passes on the information it receives and sends information back.

Currently, if your phone uses 4G, the frequency band of the radio waves it employs is anywhere from 2 - 8 GHz. This is a slightly higher frequency than 1.8 – 2.5 GHz for 3G (and can be slightly different, depending on your region).
Using higher frequencies has both advantages and disadvantages. The higher the frequency of a radio wave, the shorter the wave itself. Similarly to sound waves, shorter waves lose energy faster as they move, so they cover less distance.



The area covered by the phone tower - also known as a base station - is called a 'cell', and these are usually around 1 to 20 kilometres wide, although they can be a lot smaller, depending on how many phones there are in the area.
At weaker frequencies, one tower covers less area, therefore you need more towers. However, shorter waves also mean that many more devices can be connected to one phone tower at once. 5G potentially offers network connection speeds that will be substantially higher than what's currently available.
One of the reasons people are so worried about 5G, is that the new network can support frequencies of up to 300 GHz, although the various countries where it's being rolled out will cap the frequencies differently.
These higher frequencies are called 'millimetre wavelengths', because they are between 1 and 10 millimetres in width. Shorter waves with their larger energy might seem dangerous at face value, but there's no basis for these concerns.
"Higher frequency doesn't mean higher intensity: it's really like comparing blue with red light – it's a different wavelength," Andrew Wood, an electromagnetic bioeffects researcher from Swinburne University in Australia, told ScienceAlert.
"For 5G's 26 GHz the radio wave is absorbed in the outer layers of the skin rather than getting into the brain tissue. There are nerve endings in the skin which would warn of any over-exposure."
Wood, as part of his research, is using advanced computer modelling to predict the absorption of radio frequency in various parts of the skin.

Because shorter wavelengths don't penetrate like longer ones, it also means 5G phone towers need to be placed closer together, something which doesn't impress those already nervous about the ubiquitous presence of radio waves in our environment.

"Another significant change for 5G will be to centralise much of the processing that in the past was carried out at the base station. Dealing with the high density of devices and doing sophisticated processing requires a great deal of computing power," explains Philip Branch from Swinburne University of Technology for The Conversation.

"Rather than having each base station doing it, the raw data will be transmitted to a central location and be processed there."

So, why are people so scared? Fears of electromagnetic radiation are nothing new; the most simple explanation is that the promise of a 5G rollout is just bringing up the same old technology concerns people have had for decades - just dressed up in a new guise.

"The exposure levels for the general public will be well below the limits set by ICNIRP, the international review agency linked to WHO," says Wood.

"The prevalence of phone handsets has gone from zero in the early 80s to over 90 percent of the Australian population now, without an appreciable change in brain cancer rates."

But experts have noted that maybe, just maybe there is one source we can blame for this uptick in 5G phobia: Russia.

"There's a theory around that the Russians want to slow the 5G roll-out in the West, to enable their technology to catch up," says Wood.

We seriously couldn't make this stuff up if we wanted to.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

A 'pandemic drone' and other technology could help limit the spread of coronavirus and ease restrictions sooner, but at what cost?

Source: https://www.abc.net.au/news/2020-05-01/new-surveillance-technology-could-beat-coronavirus-but-at-a-cost/12201552

June 12 – Software being developed at the University of South Australia in conjunction with Canadian drone manufacturer Draganfly could see drones used to monitor the health of people, including spotting sneezes and tracking whether they have a fever. It is just one-way technology could be used to track and slow the spread of a virus like COVID-19. But experts warn that new surveillance technologies must include privacy safeguards before they are adopted.

Heart rate can be detected within 8 metres

Professor Javaan Chahl, who holds positions with the University of South Australia and the Department of Defence, is developing software for the pandemic drone.

The device uses thermal cameras and artificial intelligence to measure some of the indicators of coronavirus in groups of people: heart rate, body temperature, coughing and sneezing. "Heart rate can be measured in two different ways," he told 7.30.

"From a drone, we normally would measure it by a subtle change in skin tone that's associated with each heartbeat.

"And it's caused by changing the volume of blood in the skin. It also causes slight movement." The drone would also be able to detect a cough from "15-20 metres away", while heart rate can be detected within 6-8 metres with only a "very small" margin of error.

It could also be used to monitor social distancing. While still six months from completion, Professor Chahl hoped it would be used to collect data on a large scale and track patterns of behaviour to paint a broad picture of the spread of COVID-19 in a city, rather than monitor individuals. "When you look at thousands of people, or millions of people, you'll start to see a trend," he said. "And I think we don't have systems in place to surveil for that, particularly.

"It would be very useful to know how many people are suffering from symptoms associated with respiratory distress.

"So, if you see a lot of people coughing and sneezing and with elevated heart rates and breathing rates and fever, okay, that's good to know. "And if that's increasing, that's very important to know."

Concerns about 'big brother surveillance'

Professor Chahl does acknowledge the technology could also be used to watch and target individuals if a future user wanted to.

"All such technologies carry a risk with them," he said.

"I might think it's a very bad idea to use drones to chase people around who might be sick. But perhaps others might have different ideas.
"And it's very hard to restrain them from using it like that once the genie is out of the bottle."
Police in the US city of Westport, an hour north of New York, were trialling the software along with Draganfly, but pulled out last week over privacy concerns.
"There's a lot of discussion going on at the moment about how we manage that privacy so that you don't take away people's freedom, or start imposing on them unnecessarily," Professor Chahl said.
"But you do want to watch for the presence of this infectious disease. So there's a lot of challenges."
Artificial intelligence expert Professor Toby Walsh urged a cautious approach towards adopting technologies like the pandemic drone.
"I think the devil is in the detail: how it's rolled out, what safeguards are put in place," he said.
"There's every reason that this technology could be a useful tool in our armoury with rolling back the restrictions and allowing people to go about somewhat more normal lives.
"But, equally, there are concerns that you'd have about people's privacy and about whether when normality has returned, that we are not finding ourselves in a big brother surveillance state."

Surveillance tech already used overseas

Hong Kong makes arrivals to the territory wear a tracking wristband and self-isolate for 14 days. *(ABC News)*

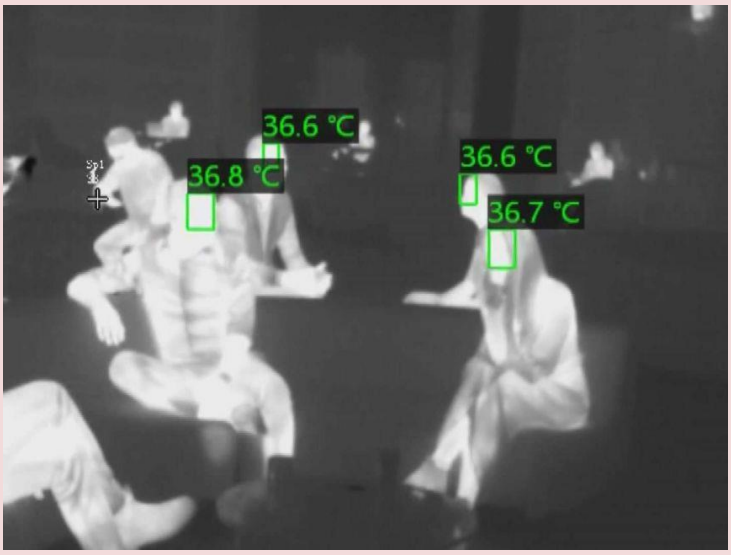
Several places in east Asia, including Hong Kong, Taiwan and South Korea, have taken a more technology-driven approach to fighting coronavirus, successfully slowing the rate of transmission without enforcing the same strict lockdowns seen in Australia and some European countries, and keeping shops and restaurants open.

Everyone who lands in Hong Kong must download a mandatory phone app and wear a wristband for two weeks while in compulsory quarantine.
The app and wristband work together to track the user's whereabouts, along with regular video calls from health officials.
Professor Walsh doubts that level of surveillance would go down well in Australia.
"These are extraordinary times, but I think those are extraordinary measures that I suspect most people in Australia would find too much down the road to taking us to what [authors] George Orwell, Huxley and other people have warned us about the surveillance state that we could be in," Professor Walsh said.
Another distinct feature of Hong Kong's tech-driven approach to tackling the virus is the routine use of temperature checks, which are a common sight at the entrance to restaurants, offices, shopping malls and government buildings across the city.

Fever scanning

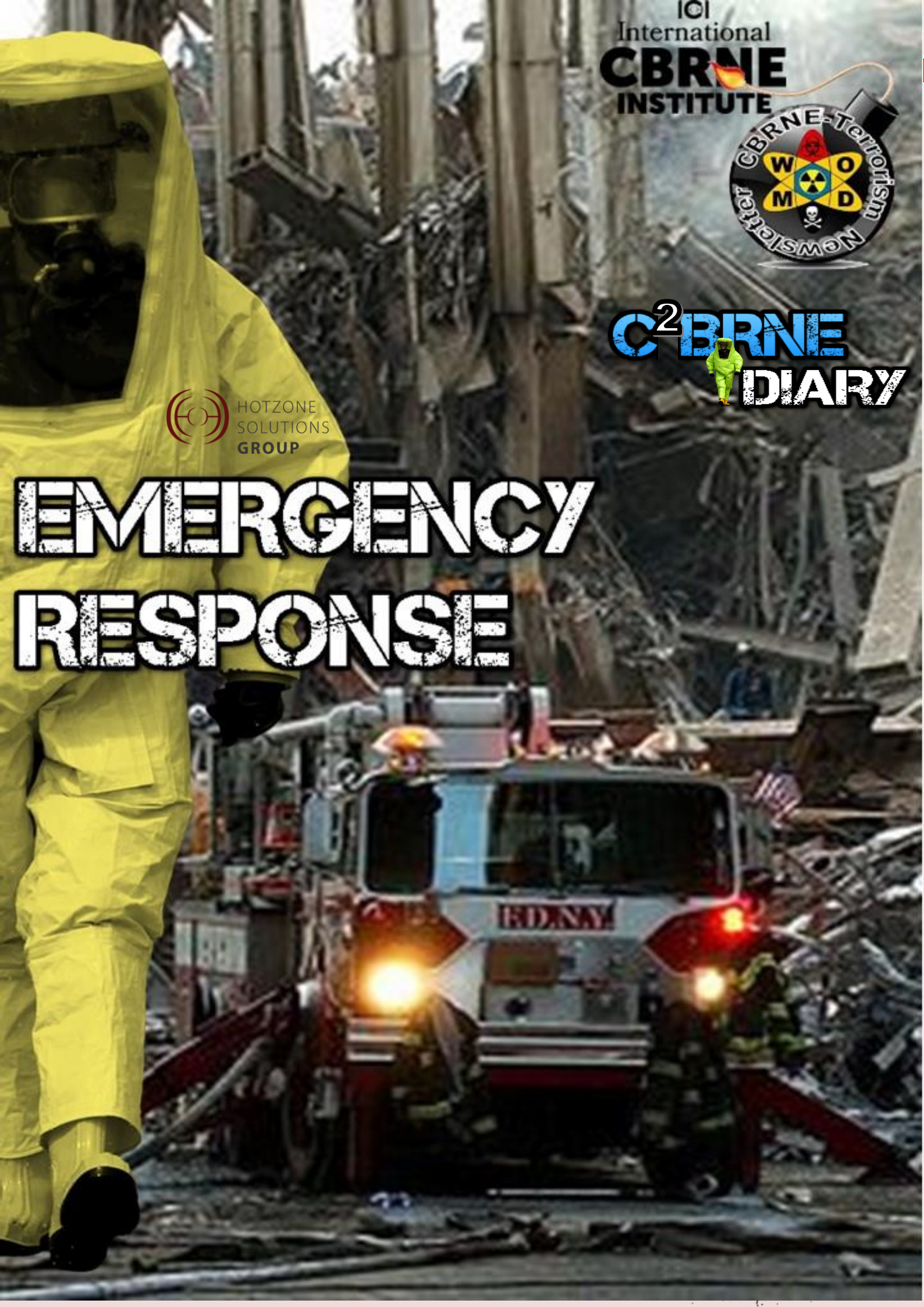
Australian entrepreneur Rustom Kanga hopes that temperature-taking technology will soon be more widespread here.
His company iOmniscient has developed an automated fever scanning system which can operate through CCTV cameras to check the temperatures of people in crowds.
He claimed it was accurate "to about 0.2 of a degree Celsius".
"Now and in the future, we will be releasing the lockdown, there'll be lesser restrictions," he told 7.30.
"And in those environments we are going to still have to keep track of everyone.
"We are going to have to monitor people to make sure that there is no one round with a fever, because the fever is the first external indication, usually, of an infection of the coronavirus."
Dr Kanga said the software used artificial intelligence, including facial recognition, to automatically read the body temperature of "hundreds of people" at once in a crowd and alert authorities if someone had a fever.
The system could then track them through a network of cameras until they could be identified by a staff member or official.
"It uses what is called a thermographic camera, which is a camera that can detect the heat of things in the environment," he said.
"In this case, it's detecting the temperature of a person's skin."
Dr Kanga believed the technology could be useful in places where people are still gathering in groups such as schools, pharmacies, shops, defence facilities, hospitals and prisons.
"Today there is no real checking in public areas of whether people have fevers," he said.
"A system like this will give them an early indication that there's someone who potentially has a fever."

We won't be able to 'go back to our normal lives'



Proponents say technology like automated fever scanning could help ease coronavirus restrictions sooner. *(ABC News)*

The use of facial recognition technology is highly controversial and concerns have long been raised by civil liberties groups about its use in public spaces and about the potential for authorities to use it to track citizens.
But Dr Kanga said his software "anonymised" faces by default and people would only be identified when requested by the user.
"Everyone's face can be redacted so that nobody sees anything," he said.
"However, if there's a person with a fever, that person's image is sent to the smartphone or the paramedic so that he can be checked out."
Professor Walsh said technologies like this could be part of Australia's approach, but won't replace the need for social distancing.
"It's worth pointing out those modern technologies are not going to be a panacea," he said.
"They're not going to allow us to go back to our normal lives, we are still going to have to social distance, we are still going to have to keep ourselves isolated physically as much as possible from each other until we have a vaccine.
"And, until that point, our lives are going to be somewhat on hold."


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

Researchers Find Commonalities in All Crises

By Guro Kulset Merakerås

Source: http://www.homelandsecuritynewswire.com/dr20200608-researchers-find-commonalities-in-all-crises

June 08 – The coronavirus crisis has made civil protection a highly relevant area of research.

Major crises often trigger this kind of response. The last such wave peaked following the July 22, 2011 terror attacks in Oslo and Utøya. Increased interest in emergency preparedness and civil protection is completely natural but not necessarily helpful for achieving the desired security.

The actual key to success is regular, ongoing groundwork that can help connect resources when a crisis arises. This approach requires establishing cross-sector collaboration, open communication and effective information flow.

Interdisciplinary Efforts Often a Critical Piece

Although no one can predict the next crisis, researchers at NTNU Social Research find that whatever the crisis turns out to be will most likely be best solved through interdisciplinary efforts. Research shows that this is a common feature of all major crises and often a critical piece in achieving a successful outcome.

Both the July 22 terror attacks and swine flu (H1N1) are examples of how the handling of these crises suffered from a lack of clear roles and responsibilities between agencies.

"Regular meeting points and formalized processes for interacting are always useful measures. Talking together can contribute to a common understanding and better insight into topics that extend across sectoral boundaries. We should make sure that agencies with different points of view build relationships, because over time that can contribute to better cooperation when crises occur," says Marie Nilsen. She is supported by her colleague at NTNU Social Research, senior researcher Stian Antonsen.

"Collaboration and coordinated effort are important, and we need to invest in cultivating our collaborative ability 'in peacetime'. This prevents crises from becoming larger than they need to be as a result of mismanagement," he says.

Management Phase Dominates When We Evaluate

All preparedness and safety work can be broken down into five phases.

Phase one involves risk assessment, phase two is about preventing crises, and phase three involves management planning. All these steps have to occur before a crisis hits.

Once the crisis occurs, the fourth phase kicks in, where we have to manage the situation by mobilizing resources, informing citizens and mitigating injury.

Finally, phase five entails normalizing the situation. Remedying damage, communicating information and transitioning to normal operations become the important tasks. This phase is also the time to evaluate, learn and report out.

"When we look back on a crisis situation, we tend to focus on the management phase, and we forget to examine the underlying causes and contingency planning. This can lead to introducing measures that don't actually make the system more robust, but only change the way we would solve the just-completed crisis if we had to do it over again," says Nilsen.

COVID-19 Expands Our Powers of Imagination

Modern Norwegian society has a relatively short list of major crises upon which to draw.

Nilsen, who is currently a PhD candidate in NTNU's Department of Industrial Economics and Technology, previously reviewed evaluation reports following several international and Norwegian crisis events: the 2004 tsunami, the swine flu in 2009, the ash cloud in 2010 and the July 22 terror attacks in 2011, as well as the extreme weather cyclone Dagmar, May 2011 inland flooding, and the fire in the historic village of Lærdal in 2014.

"Following crises or adverse events, we reflect on what's gone well, what could have been done better and what parts of the system failed. Some events also help expand our powers of imagination in terms of worst-case scenarios. The 2011 Norway attacks definitely did," says Nilsen.

"COVID-19 seems to be doing the same," she says. She believes that the pandemic could change our view of the individual's responsibility for society's preparedness.

In dealing with the current crisis, the importance of mobilizing ordinary community members, NGOs and public-private cooperation has been recognized.

"In previous crises, we've repeatedly seen that what these groups contribute in terms of their resources and local knowledge has reduced the consequences of adverse events," says Nilsen, citing the fire in Lærdal as an example.

The invisible Aspects of Preparedness

"Creating good, inclusive communities is preventative civil protection work. These invisible aspects of our preparedness deserve to be made visible and recognized," says Antonsen.

He points out that every year volunteers provide thousands of hours of work, along with equipment and resources and a willingness to contribute to the community.

"This volunteerism contributes to building viable and resilient communities and is an invaluable addition to the formal preparedness of emergency agencies and authorities," Antonsen says. Our social capital and ability to take responsibility not only for ourselves, but also for each other needs to be safeguarded and further developed in the quiet periods between crises.

This time period – the quiet spell between crises – is the best time to tackle improvements that will really make a difference.

It isn't only new equipment and changes in planning that will improve our overall preparedness, although these are visible, measurable and thus attractive measures for politicians and leaders who want to show that they are taking action.

Nilsen and Antonsen believe what is needed is to look at the basic regulatory framework for addressing security and preparedness. This would include the actual willingness to spend money on measures we hope we never need, and that "no one" sees.

This kind of preparation also involves evaluating not only individual crises, but looking at the totality of what we can learn from past events and determining the basic and transferable factors that we can become better at. And then we have to insert the relevant measures in those spots.

Three Important Areas

Nilsen points to three important areas of preparing for crises:

- To begin with, we need to deconstruct barriers where the pride in individual sectors stands in the way of efficient information flow and collaboration, and instead create bridging elements that counteract the tendency of sectors to only work towards their own goals. Silo thinking does not belong in emergency preparedness work.
- Second, we need to ensure a good balance between the preparedness for major crises, that fortunately rarely occur, and the preparedness for critical events that occur more often.
- Third, we need to avoid excessive focus on the previous crisis in the evaluation and action phase, so that new measures are seen in the context of existing measures and systems.

Antonsen believes that we should already be asking ourselves whether we have the necessary platform in place for a collective, cross-sectoral evaluation of the corona crisis.

"If we don't," he says, "it seems likely that everyone will go back to their sectoral evaluation towers after the corona crisis. That would be unwise, since we know that cross-sectoral thinking is essential for improving our ability to avoid and manage crises effectively."

References

Nilsen, Marie; Albrechtsen, Eirik; Nyheim, Ole Magnus. (2017) Changes in Norway's societal safety and security measures following the 2011 Oslo terror attacks. *Safety Science.*

Almklov, Petter Grytten; Antonsen, Stian; Størkersen, Kristine Vedal; Roe, Emery. (2018) Safer societies. *Safety Science.* vol. 110 (Part C).

Albrechtsen, Eirik; Almklov, Petter Grytten; Antonsen, Stian; Nyheim, Ole Magnus; Nilsen, Marie; Bye, Rolf Johan; Johnsen, Stig Ole; Wasilkiewicz, Kinga; Aalberg, Asbjørn. (2017) *Har samfunnssikkerheten blitt bedre etter 22.juli 2011? Populærvitenskapelig rapport fra forskningsprosjektet The next disaster*

Guro Kulset Merakerås *is a writer at Norwegian SciTech News. The article is published courtesy of Gemini – Norwegian SciTech News, which publishes research news from NTNU: Norwegian University of Science and Technology and SINTEF.*

HOTZONE
SOLUTIONS
GROUP

A holistic approach in CBRNe operations

Consultation
Products
Training

www.hotzonesolutions.org