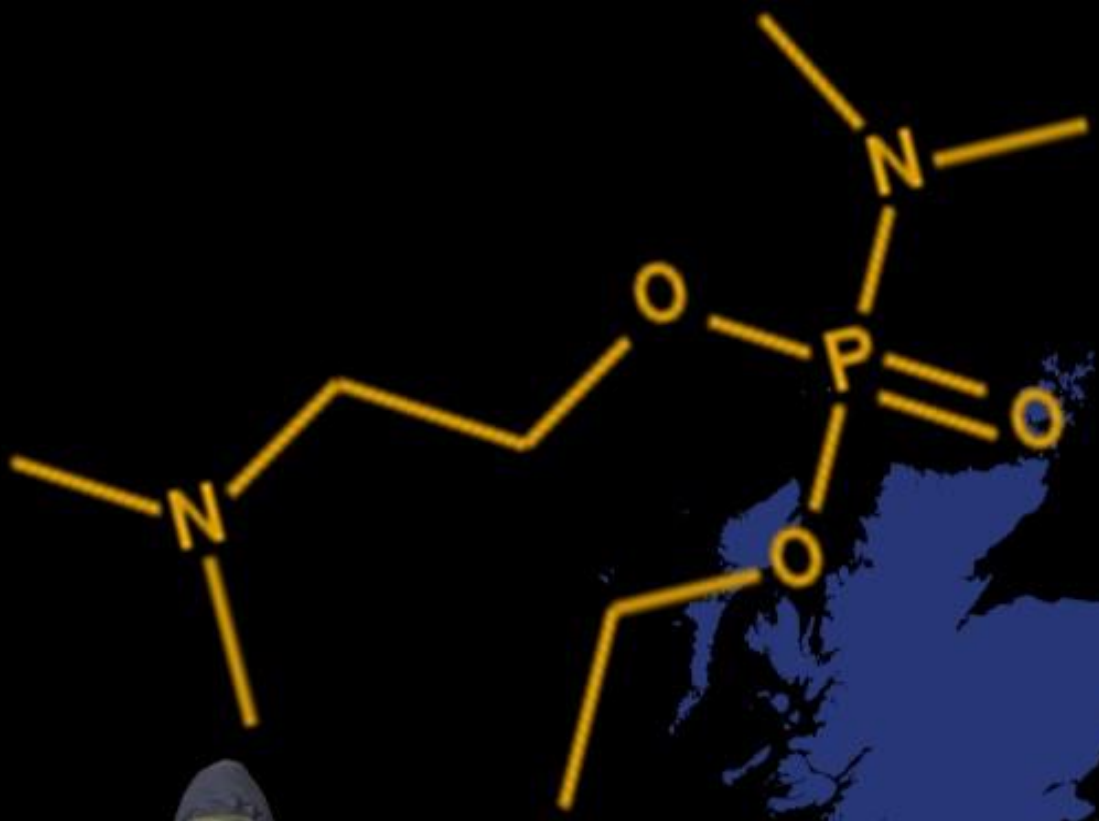
Dedicated to Global First Responders

# CBRNE NEWSLETTER TERRORISM

CBRNE-Terrorism Newsletter

March 2018



www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

# DIRTY R-NEWS

# Is Radiation Education Fearmongering?

**By Scott Masiella**

Source: https://www.thermofisher.com/blog/identifying-threats/is-radiation-education-fearmongering/

Feb 27 – Recently I came across a conversation on social media that pointed to our previously published article, Where Can Radiation Be Found in the U.S.? The article addressed how radiation sources are more common than you might realize. In our article, we supplied a video map that outline the various locations of radiation threats

The article invited good conversation and several readers discussed how radiation is found everywhere from a variety of sources, including from natural resources like the sun. However, some readers thought we were creating undue anxiety by letting people know that radiation sources can be found in ports and border crossings, in food and packaging analysis and testing facilities, at construction sites, scrap metal recycling yards, and oil and gas exploration locations, on the roads and rails, as well as in medical facilities – not to mention at nuclear power plants.

Another reader thought we just wanted to scare people so they would buy more products from us. I apologize if the article came off as fearmongering, but I assure you I was not trying to promote radiation fright to sell products with this map. Of course all businesses want to sell more products, but our company believes in educating in the name of safety.

The purpose of the map is to alert first responders, fire, and police departments that nearly every city and region has radiation sources. The sources, if involved in an accident could produce unwanted exposure. Think about it: if firefighters were called to a warehouse fire where bottling or packaging occurred or where density gauges were stored without radiation measurement devices, how would they know if they were being exposed to dangerous levels without radiation detectors? Knowing that radiation sources are near, not always in plain sight like a hospital or nuclear power plant, and also knowing there is available grant money to procure state of the art instruments to measure and quantify the radiation, is the point of this map.

Many communities believe there is no danger from radiation near them if there is no nuclear power plant. That's not true, which is why many fire departments and police carry radiation detectors today, most from the Cold War era. Upgrading those aged detectors to also pull double duty to combat domestic terrorism threats, respond quickly to small amounts of radiation, alert users when radiation dose rates are high, are needs that every community should consider.

Radiation detection and measurement is just another safety precaution that should be addressed by all communities. Safety and security personnel should be able to detect, localize, identify, and measure radioactivity in any scenario. And the first step is being knowledgeable enough to know where the radiation concerns could be located.

# North Korea Asks for Direct Nuclear Talks, and Trump Agrees

Source: https://www.nytimes.com/2018/03/08/us/politics/north-korea-kim-jong-un-trump.html

Mar 08 — North Korea's leader, Kim Jong-un, has invited President Trump to meet for negotiations over its nuclear program, an audacious diplomatic overture that would bring together two strong-willed, idiosyncratic leaders who have traded threats of war.

The White House said that Mr. Trump had accepted the invitation, and Chung Eui-yong, a South Korean official who conveyed it, told reporters that the president would meet with Mr. Kim within two months.

"He expressed his eagerness to meet President Trump as soon as possible," Mr. Chung said at the White House on Thursday evening after meeting the president. Mr. Trump, he said, agreed to "meet Kim Jong-un by May to achieve permanent denuclearization."

The president expressed his optimism about the meeting in a post on Twitter, saying that Mr. Kim had "talked about denuclearization with the South Korean Representatives, not just a freeze."

"Also, no missile testing by North Korea during this period of time," Mr. Trump added. "Great progress being made but sanctions will remain until an agreement is reached. Meeting being planned!"

Mr. Chung, whose talks with Mr. Kim on Monday in Pyongyang resulted in the invitation, noted that the North Korean leader said he understood that joint military exercises with the United States and South Korea would go ahead as scheduled after the end of the Paralympic Games this month.

For Mr. Trump, a meeting with Mr. Kim, a leader he has threatened with "fire and fury" and has derided as "Little Rocket Man," is a breathtaking gamble. No sitting American president has ever met a North Korean leader, and Mr. Trump himself has repeatedly vowed that he would not commit the error of his predecessors by being drawn into a protracted negotiation in which North Korea extracted concessions from the United States but held on to key elements of its nuclear program.

Meeting Mr. Kim now, rather than at the end of a negotiation when the United States would presumably have extracted concessions from North Korea, is an enormous gesture by the president. But Mr. Trump and Mr. Kim share a penchant for bold, dramatic moves, and their personal participation in a negotiation could take it in unexpected directions.

The announcement itself was delivered in an improvisational style that belied its historic significance. Mr. Trump himself teased the news, popping into the White House briefing room shortly after 5 p.m. to tell reporters that South Korea would make a major announcement at 7.

Then the White House left it to Mr. Chung, who is President Moon Jae-in's national security adviser, to deliver the news to reporters, standing in the darkened driveway in front of the West Wing. The White House later confirmed Mr. Trump's plan to meet Mr. Kim in a statement from the press secretary, Sarah Huckabee Sanders.

Behind the scenes, events unfolded even more haphazardly. Mr. Trump was not scheduled to meet Mr. Chung until Friday, but when he heard that the envoy was in the West Wing seeing other officials, the president summoned him to the Oval Office, according to a senior administration official.

Mr. Trump, the official said, then asked Mr. Chung to tell him about his meeting with Mr. Kim. When Mr. Chung said that the North Korean leader had expressed a desire to meet Mr. Trump, the president immediately said he would do it, and directed Mr. Chung to announce it to the White House press corps. Mr. Chung, nonplused, said he first needed approval from Mr. Moon, who quickly granted it in a phone call. Mr. Trump later called Prime Minister Shinzo Abe of Japan, and the two discussed coordinating diplomatic efforts. Mr. Trump also plans to call President Xi Jinping of China.

By day's end, dazed White House officials were discussing whether Mr. Trump would invite Mr. Kim to come to the United States. That seemed entirely likely, the senior administration official said, though American officials doubt the North Korean leader would accept.

The announcement capped another day of swirling drama at the White House, in which the president defied his own party by announcing sweeping tariffs on steel and aluminum imports and sought to ignore a mushrooming scandal over a pornographic film actress who claims to have had an affair with him.

White House officials had expected to deliberate for several days over how to respond to North Korea's proposal for direct talks between the countries, which South Korean officials had first conveyed by telephone this week. But Mr. Kim's offer of a leader-to-leader meeting accelerated, if not upended, the administration's plans.

Embarking on a high-level negotiation will pose a stiff challenge to the administration, which has built its North Korea policy around imposing crippling sanctions, backed by the threat of military action. People briefed by the administration said it had done little planning for how a negotiation with the North would unfold.

The State Department's chief North Korea negotiator, Joseph Yun, recently announced his departure from the Foreign Service. The White House also scotched a plan to nominate another experienced negotiator, Victor Cha, as ambassador to Seoul.

North Korea, by contrast, appears to have planned its diplomatic overture methodically, starting with Mr. Kim's conciliatory message toward the South in his New Year's Day

address, and continuing through the North's charm offensive during the Winter Olympic Games in Pyeongchang, South Korea.

The South Korean envoys visited the White House on Thursday to brief Mr. Trump and his staff on their meeting with Mr. Kim, which was the first between South Korean officials and Mr. Kim. While they said they were carrying additional messages from North Korea, an American official said that the envoys did not deliver a letter from Mr. Kim.

In South Korea, people greeted the news of a meeting between Mr. Kim and Mr. Trump with relief. South Koreans had nervously watched the Korean Peninsula edge toward the brink of a possible military conflict last year.

"We hope that these developments will become an important turning point for realizing the denuclearization of the Korean Peninsula and firmly establishing peace there," Lee Yu-jin, a government spokeswoman, said Friday.

Since taking power last May, Mr. Moon has repeatedly called for a dialogue with North Korea, even as Mr. Trump has escalated pressure on the North with increasingly harsh sanctions, more vigorous military maneuvers and a string of hostile tweets.

Mr. Kim rattled the region last year with a series of nuclear and long-range missile tests. Then he suddenly responded to Mr. Moon's overtures for dialogue, in which he proposed talks with South Korea, saying he was willing to send athletes to the Olympics.

The two Koreas have also exchanged high-level envoys in recent weeks, including Mr. Kim's sister, Kim Yo-jong, who met Mr. Moon in Seoul last month.

Analysts expressed skepticism about Mr. Trump's decision to meet Mr. Kim, saying there was no indication that North Korea had given up its determination to be a nuclear weapons state.

"There is every reason to believe that North Korea is attempting to blunt sanctions and secure de facto legitimacy for its nuclear weapons program with this gesture," said Michael J. Green, a former Asia adviser to President George W. Bush, speaking by telephone from Tokyo.

Evan S. Medeiros, an Asia adviser to President Barack Obama, said that any direct talks would elevate Mr. Kim and legitimize him. "We got nothing for it. And Kim will never give up his nukes," Mr. Medeiros said. "Kim played Moon and is now playing Trump."

This week, administration officials had spoken in scathing terms about North Korea's offer of direct talks. They noted that Mr. Kim said nothing about halting the production of nuclear bombs or missiles during negotiations — which meant the North could build its arsenal while stringing out the talks.

It seemed that the only thing that changed was Mr. Kim's invitation to meet Mr. Trump himself. The president's deal-making skills, one of his aides said on Thursday, could produce an outcome different from previous rounds of diplomacy, which have always ended in failure and disappointment.

The highest-level American official to meet with a North Korean leader was Secretary of State Madeleine K. Albright, who visited Pyongyang in 2000, near the end of the Clinton administration. Dr. Albright had planned to arrange a visit by President Bill Clinton.

But it fell apart when Kim Jong-il, the father of the current leader, would not agree to a missile deal in advance; he wanted to negotiate it face-to-face with the president. Mr. Clinton decided not to take the risk, skipped the trip, and used his last weeks in office to make a race for Middle East peace instead.

## Kazakhstan signs Treaty on Prohibition of Nuclear Weapons

Source: https://astanatimes.com/2018/03/kazakhstan-signs-treaty-on-prohibition-of-nuclear-weapons/

Mar 11 – On the day of the 26th anniversary of Kazakhstan's accession to the United Nations – March 2, an official ceremony for signing the Treaty on the Prohibition of Nuclear Weapons by Kazakhstan took place at the UN Headquarters.

Permanent Representative of Kazakhstan to the United Nations Kairat Umarov signed the agreement.

Kazakhstan had participated in the elaboration and adoption of the treaty, which became the first legally binding document in the history of nuclear disarmament. Its main provisions are in line with the principled position of Kazakhstan, which has taken a path of becoming a leader in nuclear disarmament and non-proliferation after being a one-time holder of the world's fourth nuclear arsenal.

"This was inspired by the historical decisions of President Nursultan Nazarbayev, in particular, on the closure of the second largest nuclear test site and renunciation of the

nuclear legacy of the Cold War. Our country's denuclearisation was not an accidental decision, but a well-considered and thoughtful act by a responsible state that had learned the horrors of nuclear tests, which have resulted in the suffering the worst possible consequences, subsequently even in the third generation," reads the statement from the Ministry of Foreign Affairs.

Permanent Representative of Kazakhstan to UN Kairat Umarov signs Treaty on Prohibition of Nuclear Weapons

Despite the unwillingness of a number of states, including the de jure and de facto nuclear powers, to disarm, the Kazakh President continues to tirelessly urge the world community to achieve a world free of nuclear weapons, the statement said.


At the high-level thematic meeting of the UN Security Council on the topic "Non-Proliferation of Weapons of Mass Destruction: Confidence-Building Measures", organized by the Kazakh presidency of the UN Security Council on Jan. 18, Nazarbayev once again called on everyone to build a world without nuclear weapons by 2045 – the UN's centennial.

"The strength is not in nuclear bombs and missiles. The trust of the world community is a real defence," said the Kazakh President at the Security Council stressing that only nuclear disarmament and confidence-building measures through the complete elimination of nuclear arsenals constitute the only and absolute guarantee against the use or threat of use of nuclear weapons.

The President also noted that the nuclear weapons states bear the highest responsibility to humanity for preventing nuclear catastrophe.

"It is the largest nuclear powers that should be in the lead of the struggle for a nuclear weapons-free world and set an example by reducing WMD. This does not mean that the rest of the countries should stand by and that their actions are irrelevant", said Nazarbayev.

On the other hand, he stressed, if the largest nuclear weapon states insist on keeping their nuclear status and modernising their weapons, while prohibiting other countries from acquiring nuclear weapons, this will not lead to positive results.

Convinced that mankind in the 21st century is able to travel the path to a world free from the threat of weapons of mass destruction, Nazarbayev called "for joint efforts in this direction". He also reminded the audience of the special role of the Security Council and its historical mission in building a safer world and a just world order as stated in the UN Charter.

There are only three types of WMD – nuclear, chemical and biological but only nuclear weapons have not been legally banned, until now. The pillar of the Treaty on Prohibition of Nuclear Weapons is Article 1 "Prohibitions", which contains provisions on the comprehensive prohibition of nuclear weapons. The treaty is designed to remove the legal gap in the international legal field and is the first step towards the elimination of nuclear weapons.

The Treaty on the Prohibition of Nuclear Weapons was adopted July 7, 2017 with the support of 122 UN Member States. It was the outcome of two sessions of a UN Conference to

negotiate a legally binding instrument to prohibit nuclear weapons, leading towards their total elimination. The conference took place on March and June-July 2017 in New York. It was open to the participation of all UN member states. However, nine de facto and de jure nuclear weapons possessing states and their allies boycotted these talks. To date, the treaty has been signed by 56 states, five of which have ratified it. **Kazakhstan has become the 57th signatory state.** The treaty shall enter into force 90 days after the fiftieth instrument of ratification has been deposited.

# Expanding real-time radiological threat detection to include other dangers

Source: http://www.homelandsecuritynewswire.com/dr20180312-expanding-realtime-radiological-threat-detection-to-include-other-dangers

Mar 12 – **Advanced commercially available technologies—such as additive manufacturing (3-D printing), small-scale chemical reactors for pharmaceuticals, and CRISPR gene-manipulation tools—have opened wide access to scientific exploration and discovery. In the hands of terrorists and rogue nation states, however, these capabilities could be misused to concoct chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) weapons of mass destruction (WMD) in small quantities and in form factors that are hard to detect.**

DARPA says that to meet this challenge, it was announcing its **SIGMA+ program**, an expansion of the existing SIGMA program, which detects radiological and nuclear materials. SIGMA+ seeks to develop new sensors and networks that alert authorities to chemical, biological, and explosives threats as well.

"The goal of SIGMA+ is to develop and demonstrate a real-time, persistent CBRNE early detection system by leveraging advances in sensing, data fusion, analytics, and social and behavioral modeling to address a spectrum of threats," said Vincent Tang, SIGMA+ program manager in DARPA's Defense Sciences Office (DSO). "To achieve this, we've pulled together a team of DARPA program managers who bring expertise in chemistry, biology, data analytics, and social science to address the broad and complex CBRNE space."

The program calls for the development of highly sensitive detectors and advanced intelligence analytics to detect minute traces of various substances related to WMD threats. SIGMA+ will use a common network infrastructure and mobile sensing strategy, a concept that was proven effective in the SIGMA program. The SIGMA+ CBRNE detection network would be scalable to cover a major metropolitan city and its surrounding region.

To uncover chemical and explosives threats, SIGMA+ seeks unprecedented **long-range detection of hundreds of chemicals at trace levels** to help authorities identify bomb-making safe houses in large urban areas, for example. Successfully developing scalable, long-range chemical sensors would help enable interdiction of improvised chemical and explosive threats or their constituent materials before an attack occurs.

To quickly alert officials of a biological terror attack, such as the release of anthrax, smallpox or plague viruses, SIGMA+ seeks **sensors that can detect, in real time, traces of a wide range of pathogens**. The program aims to provide immediate, continuous monitoring of pathogen background levels and spikes, which could indicate malicious release of a biological agent.

New environmental, as well as biomechanical and biochemical sensing methods for detecting threats could provide system sensitivity ten times greater than the state-of-the-art, which would enable detection of a wider range of biological attacks days earlier, maximizing the effectiveness of countermeasures and prophylaxis. For natural pandemics, SIGMA+ sensing methods could yield awareness of major outbreaks weeks sooner than currently is possible.

The program is structured around two Phases with two planned Broad Agency Announcement (BAA) solicitations. The first phase focuses on developing novel sensors for chemicals, explosives, and biological agents. The Phase 1 sensors BAA is expected to be released on FedBizOpps in March. The second phase focuses on network development, analytics, and integration. The Phase 2 BAA is expected to be released in late 2018.

"If successful, SIGMA+ will demonstrate that automated, distributed networks of sensors, combined with automated intelligence analytics and insights from social science, can be

deployed and practically scaled to significantly increase the probability of interdicting CBRNE WMD attacks," said Tang.

DARPA notes that in addition to Program Manager Vincent Tang, the SIGMA+ management team includes the following DARPA researchers:

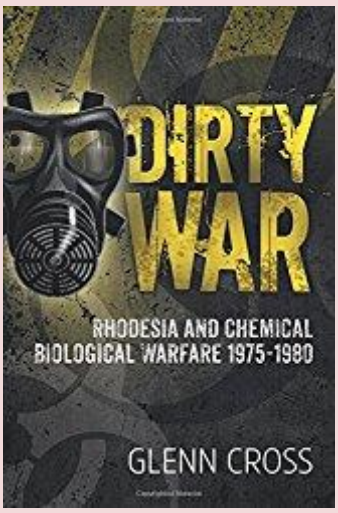
- Mark Wrobel is SIGMA program manager in DSO. Launched in 2014, SIGMA has successfully demonstrated an operationally effective, continuous radiation-monitoring network of wearable, vehicle-mounted, and stationary radiation detection sensors that provide coverage across a large city or region. SIGMA capabilities are currently transitioning to operational use with various law enforcement and counterterror entities. SIGMA+ aims to achieve sensitivity enhancement over the current SIGMA system for interdicting radiological and nuclear threats.
- Anne Fischer is a program manager in DSO. For SIGMA+, she is leading the chemical sensor network development and integration.
- Matt Hepburn is a program manager in the Biological Technologies Office. His focus in SIGMA+ is biological-agent detection sensors and rapid-diagnostics technologies.
- Carey Schwartz, a program manager in the Information Innovation Office, will focus on the information analytics element of SIGMA+.
- Adam Russell, a DSO program manager, will lead the social and behavioral modeling aspects of SIGMA+.

# Dirty War: Rhodesia and Chemical Biological Warfare 1975-1980 1st Edition

**By Glenn Cross** (Author)

Source: http://outbreaknewstoday.com/rhodesias-top-secret-use-chemical-biological-weapons-interview-dr-glenn-cross-32381/

Dirty War is the first comprehensive look at the Rhodesia's top secret use of chemical and biological weapons (CBW) during their long counterinsurgency against native African nationalists. Having declared its independence from Great Britain in 1965, the government—made up of European settlers and their descendants—almost immediately faced a growing threat from native African nationalists. In the midst of this long and terrible conflict, Rhodesia resorted to chemical and biological weapons against an elusive guerrilla adversary. A small team made up of a few scientists and their students at a remote Rhodesian fort to produce lethal agents for use. Cloaked in the strictest secrecy, these efforts were overseen by a battle-hardened and ruthless officer of Rhodesia's Special Branch and his select team of policemen. Answerable only to the head of Rhodesian intelligence and the Prime Minister, these men working alongside Rhodesia's elite counterguerrilla military unit, the Selous Scouts, developed the ingenious means to deploy their poisons against the insurgents. The effect of the poisons and disease agents devastated the insurgent groups both inside Rhodesia and at their base camps in neighboring countries. At times in the conflict, the Rhodesians thought that their poisons effort would bring the decisive blow against the guerrillas. For months at a time, the Rhodesian use of CBW accounted for higher casualty rates than conventional weapons. In the end, however, neither CBW use nor conventional battlefield successes could turn the tide. Lacking international political or economic support, Rhodesia's fate from the outset was doomed. Eventually the conflict was settled by the ballot box and Rhodesia became independent Zimbabwe in April 1980. Dirty War is the culmination of nearly two decades of painstaking research and interviews of dozens of former Rhodesian officers who either participated or were knowledgeable about the top secret development and use of CBW. The book also draws on the handful of remaining classified Rhodesian documents that tell the story of the CBW program. Dirty War combines all of the available evidence to provide a compelling account of how a small group of men prepared and used CBW to devastating effect against a largely unprepared and unwitting enemy. Looking at the use of CBW in the



context of the Rhodesian conflict, Dirty War provides unique insights into the motivation behind CBW development and use by states, especially by states combating internal insurgencies. As the norms against CBW use have seemingly eroded with CW use evident in Iraq and most recently in Syria, the lessons of the Rhodesian experience are all the more valid and timely.

## Turkish police seize radioactive Californium element in Ankara

Source: https://www.dailysabah.com/investigations/2018/03/19/turkish-police-seize-radioactive-californium-element-in-ankara

Mar 19 – Turkish police have seized a valuable cache of the radioactive Californium element in an operation in the capital Ankara, according to a report published Monday by Turkish broadcaster NTV.

Californium, a rare and dangerous non-natural element, is being used in nuclear warheads and nuclear energy plants as well as in the oil and mining industries, with a **worth of approximately $4 million per gram.**

The article reported that anti-smuggling teams in the city conducted the operation in Pursaklar district upon a tipoff, detaining four suspects believed to be a part of a larger criminal organization.

**The suspects reportedly agreed to sell the cache of 1.441 kilograms of the element for $72 million on the black market. At regular market value, that amount could fetch $5.8 billion.**

The seized Californium was taken to the Turkish Atomic Energy Authority (TAEK) for safeguarding.

The U.S. and Russia are the only producers of Californium.

First developed in the 1950s in the U.S., Californium is a "strategic" element due to its limited area of use. **It is widely used in gold, silver and oil mining operations to determine water or oil layers underground**.

Media outlets reported that the suspects smuggled californium from another country, but the source was still unclear. Turkish language daily, Sabah said police was suspecting that the material might have been smuggled in from Russia. An investigation was already underway.

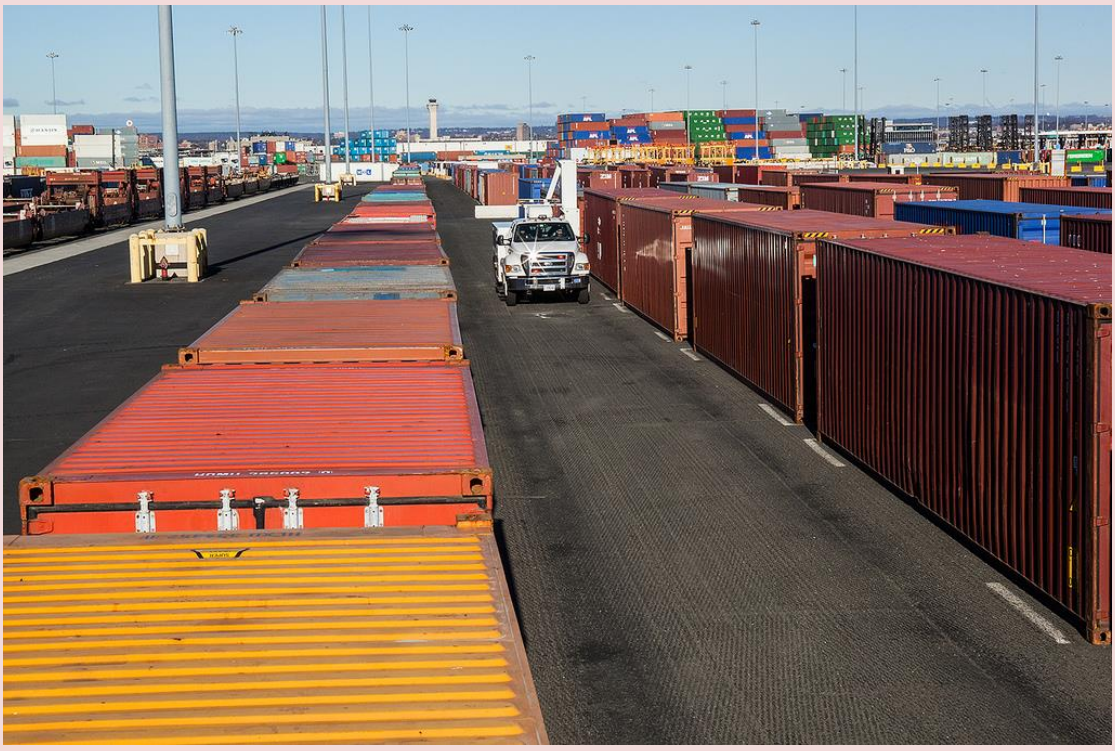
Authorities occasionally clamp down on nuclear material smugglers in Turkey, which lies at a transit route between Asia and Europe. **In 2016, police seized 13 nuggets of pure aluminum, a material used in nuclear energy production.** In a separate incident, two Georgian nationals were detained for smuggling cesium and red mercury, also used in the nuclear industry.

# What's Happening Behind Scenes to Thwart Radiological Attacks

**By Rico Chandra**

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/whats-happening-behind-scenes-thwart-radiological-attacks/

Mar 19 – Over the course of 2017, the global political landscape shifted significantly. More than one of the developments is likely to have heightened, rather than diminished, the concerns that another large-scale malicious attack on U.S. soil is looming. Just three months ago, a man detonated a pipe bomb in the New York City subway system near Times Square. Thankfully, the explosion did not result in deaths, though a handful of minor injuries were reported. While this appears to be an isolated and amateurish incident, it once more highlights the alarming and potentially tragic consequences of terrorism.



Yet despite tensions growing year by year, our nation has not suffered a single casualty in an act of radiological terrorism. As a reminder, the threat could come in the form of a strong radioactive source the size of a pencil hidden in a packed stadium, invisibly exposing crowds to the point of acute radiation sickness. Or, it could be a rogue nation, whose ballistic missiles might not be quite as reliable as a shipping container destined for Los Angeles.

The absence of radiological attacks on the U.S. homeland is not entirely coincidental. Behind the scenes, a monumental effort is being carried out by multiple U.S. and international agencies. They are working to prevent some deeply troubling scenarios from jeopardizing our way of life. A multi-layered defense has successfully protected U.S. citizens from a radiological attack. Even as the sophistication of terrorist organizations increases rapidly, the government uses technology – including new and emerging technologies – and intelligence to remain one step ahead in this race.

**Mitigating threats at the source**

In July 2017, the *Washington Post* published an article on how ISIS nearly stumbled upon the ingredients for a "dirty bomb." Indeed, over a prolonged period of time Daesh's territorial control of Mosul made them the unknowing owner of more than one strong radioactive source. It would have taken little skill to repurpose these sources into daunting radiological weapons of terror.

Obviously, Mosul is not the only place on earth where strong radioactive sources exist. Just about every country in the world has strong radioactive sources. Add to that the presence of nuclear material – uranium and plutonium – that if processed the right way are the key ingredients to yield nuclear weapons.

Yet despite the abundance of these radiological threats, we have remained safe from their effects. The United States has worked with international partners to reduce this risk in many ways, starting with reducing the number of such threats and cataloging the ones that cannot be avoided. The National Nuclear Security Administration (NNSA) of the Department of Energy has helped foreign governments secure some of the most dangerous of these materials at the sites where they are stored. Adding onto that a second layer of protection, the NNSA has helped deploy radiation detection equipment to the borders of vulnerable countries, for instance at the periphery of the former Soviet Union. And in yet another building block of this global nuclear detection architecture, radiation detection equipment is installed in most modern seaports, monitoring U.S.-bound maritime containers for radiological signatures.

Regardless of our best-laid plans, we must still assume that nefarious actors will be able to move illicit material to their target location. But the knowledge and logistics necessary to evade the many layers of this detection-net forces adversaries to inform themselves and to plan. Such communication in turn increases the digital footprint of nefarious actors that intelligence services can target.

**Prevent at points of entry**

Almost every truck or maritime container entering the U.S. passes through a so-called Radiation Portal Monitor (RPM). These highly sensitive systems are mounted on either side of traffic lanes 12 feet high; tall enough to monitor vehicles in their full height. Well over a thousand such devices are installed at the northern land border, the southern land border, and at the seaports of both coasts. The Department of Homeland Security's Countering Weapons of Mass Destruction (C-WMD) office (until recently, the Domestic Nuclear Detection Office) is currently running a technology evaluation with the goal of replacing many of the aged existing RPMs with cutting-edge technology.

The new technology will have a particular emphasis on cybersecurity. While older generations of systems had been integrated in a cyber-secure manner, the new systems will be *cyber-hardened by design*. A higher degree of network integration will result in lower manpower needs of the new systems, allowing personnel tied up babysitting the current systems to be deployed in more effective ways. The new RPMs will have benefited from novel technologies developed over the last decade, making them significantly lower cost to acquire and operate than earlier generations were. Above all, the new systems will be more precise in being able to differentiate between actual threats and benign sources of radiation, an important economic factor. In June 2017, the port at Charleston, S.C., was shut down for hours after a potential "dirty bomb" was suspected upon a docked freighter. Though that particular threat never materialized, it highlighted that even the credible threat of a weapon, without the weapon itself, can have a grave economic impact.

**Protect citizens at the local level**

The federal government has been supporting state and local authorities in their efforts to protect important cities. In Washington, for example, Metro Transit Police officers are in the process of being outfitted with portable radiation detectors to identify potential dirty bomb threats. Similar efforts are underway in major cities that terrorists are likely to view as high-value targets. Historically, the detection of radiation has relied on equipment that tended to generate too many false alarms to be practical in public spaces. Moving forward, technology has advanced to the point that scalable, highly efficient detectors can be used in concert with pager-sized devices to improve the possibility of finding a source in a large area.

The combination of static and mobile detection, when used in conjunction with data analytics, enabled by the growth of ubiquitous cloud computing, can

increase the success of detection as it reduces the overall cost to conduct radiological searches. By affording more radiation detectors that can be interconnected, the United States can develop revolutionary ways of identifying threats, and therefore preventing attacks and protecting U.S. citizens.

**Developing the future of radiation detection**

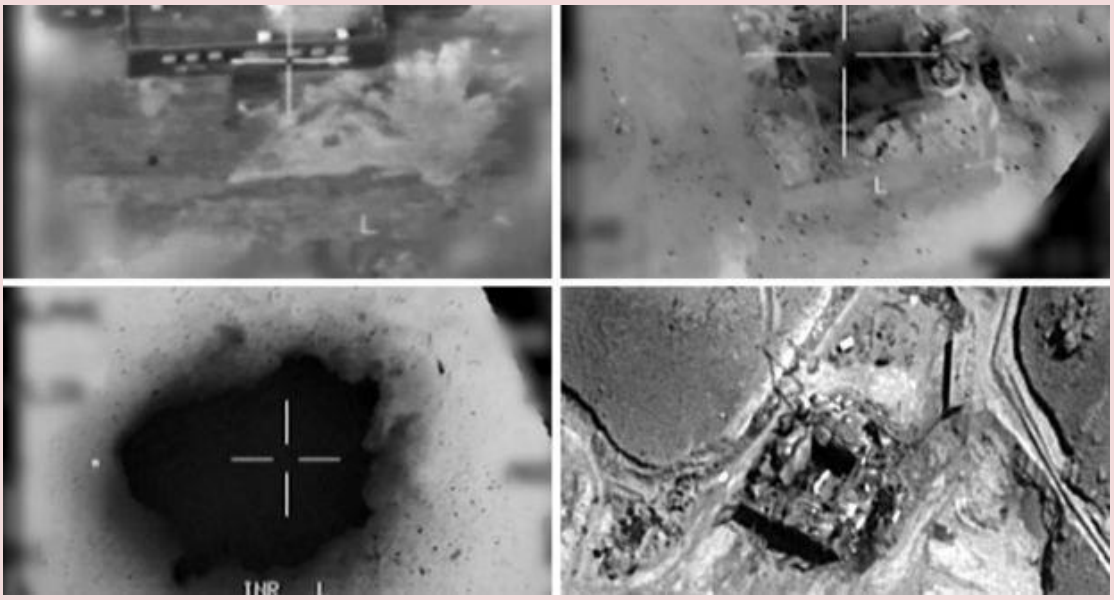
With the help of next-generation radiation detection systems, government agencies including DHS can identify, prevent, and protect against incoming threats caused by radioactive and nuclear materials. Once radiation detection systems have been successfully integrated, regular testing will help strengthen the agency's detection capabilities and overall preparedness. A lot has been invested into building the global nuclear detection architecture, parts of which have been described above. Given that the general public has remained safe from radiological attacks, the strategy of layered protection appears to have served us well. Despite the overwhelming number of radiological threats present in the world, such weapons have not been turned against us. And through continuous investment into development of new technology and deployment of reliable systems, the government has managed to stay one step ahead of the bad guys.

***Dr. Rico Chandra,*** *CEO and co-founder of Arktis Radiation Detectors, has a PhD from ETH Zurich, awarded for his work in dark matter detector R&D at CERN, Geneva. His experience includes consulting work performed for the European Commission in security questions, strategic consulting of several SMEs, and technology consulting as a council member of the Gerson Lehrman Group.*

# Israel admits destroying Syrian reactor in move seen aimed at Iran

Source: http://www.homelandsecuritynewswire.com/dr20180321-israel-admits-destroying-syrian-reactor-in-move-seen-aimed-at-iran

Mar 21 – **The Israeli military has formally acknowledged for the first time its destruction of a suspected Syrian nuclear reactor in 2007, saying the air strike removed a major threat to Israel and was a "message" to others.**



Israel's announcement on 21 March about Operation Out of the Box was widely seen as a veiled warning to arch-enemy Iran as it builds up its military presence in Syria [see a detailed report on the September 2007 attack in Yossi Melman and Dan Raviv, "Inside Israel's Secret Raid on Syria's Nuclear Reactor," *Politico* (20 March 2018)].

Israel has warned against the establishment of a permanent Iranian military presence in Syria, particularly in areas close to Israel, and last month it shot down an Iranian drone that it said entered its airspace.

"The message from the attack on the nuclear reactor in 2007 is that the state of Israel will not allow the establishment of capabilities that threaten Israel's existence," Israel's military chief, Lieutenant General Gadi Eizencot, said.

"This was our message in 2007, this remains our message today, and will continue to be our message in the near and distant future," he said.

Israel's decision to go public and justify the decade-old strike against Syria comes after repeated calls in recent months by Israeli Prime Minister Benjamin Netanyahu for the United States and international community to take tougher action against Iran, which is Syrian President Bashar al-Assad's closest ally.

Netanyahu has repeatedly warned that Israel will not allow Iran to develop a nuclear weapon — "not now, not in ten years, not ever" — or to build missile factories in Syria that could threaten Israel, or provide advanced weapons for Hezbollah, the Iran-backed Shi'ite group in Lebanon.

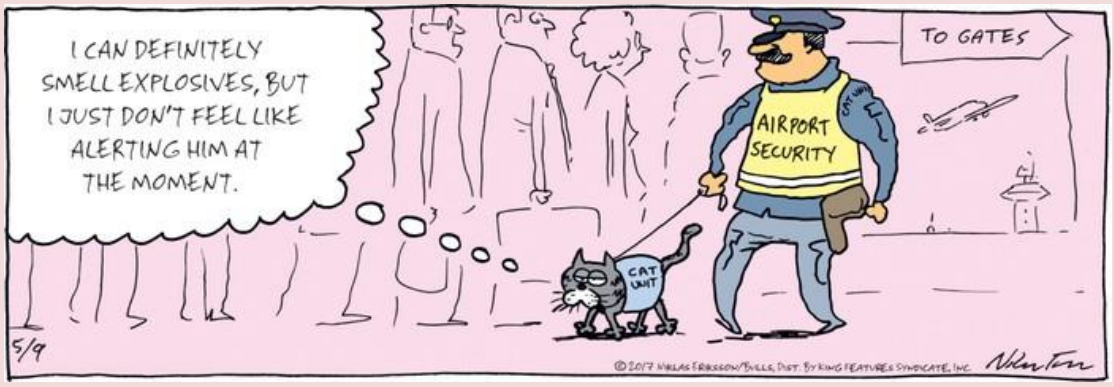
Throughout Syria's seven-year civil war, Israel has carried out well over 100 air strikes, most believed to have been aimed at suspected weapons shipments destined for Hezbollah forces operating alongside Assad's forces in Syria.

Iran did not immediately respond to Israel's warning and disclosure about its previous strike against the Syrian facility.

The Israeli military's announcement was accompanied by the release of newly declassified materials, including photographs and cockpit video said to show the moment that an air strike destroyed the Al-Kubar facility in the desert near Deir al-Zor, an area that was later overrun by the Islamic State extremist group.

The International Atomic Energy Agency (IAEA) has said it was "very likely" that the site "was a nuclear reactor that should have been declared."

Syria, a signatory of the 1970 Nuclear Nonproliferation Treaty (NPT), has always denied that the site was a reactor or that Damascus engaged in nuclear cooperation with North Korea, which is believed to have supplied the reactor.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

# EXPLOSIVE NEWS

# Protecting soldiers from blast-induced brain injury

Source: http://www.homelandsecuritynewswire.com/dr20180228-protecting-soldiers-from-blastinduced-brain-injury

Feb 28 – Researchers from the University of Maryland School of Medicine (UMSOM) and the University of Maryland A. James Clark School of Engineering have developed **a new military vehicle shock absorbing device that may protect warfighters against traumatic brain injury (TBI) due to exposure to blasts caused by land mines**. **During Operations Iraqi Freedom and Enduring Freedom, more than 250,000 warfighters were victims of such injuries.**

Prior to this study, most research on blast-induced TBI has focused on the effects of rapid changes in barometric pressure, also known as **overpressure**, on unmounted warfighters. "This is the only research to date to model the effects of under-vehicle blasts on the occupants," explains Gary Fiskum**,** M. Jane Matjasko Professor for Research and Vice-Chair, Anesthesiology at UMSOM. "We have produced new and detailed insights into the causes of TBI experienced by vehicle occupants, even in the absence of significant ambient pressure changes." The research has also resulted in the development of materials and vehicle frame design that greatly reduce injury caused by under-vehicle explosions.

UMaryland notes that Fiskum and William Fourney, Associate Dean of the Clark School, Keystone Professor of Aerospace and Mechanical Engineering and Director of the Dynamic Effects Laboratory were the first to demonstrate how the enormous acceleration (G-force) that occupants of vehicles experience during under-vehicle blasts can cause mild to moderate traumatic brain injury (TBI) even under conditions where other vital organs remained unscathed.

**"Intense acceleration can destroy synapses, damage nerve fibers, stimulate neuroinflammation, and damage the brain's blood vessels,"** explains Fiskum. Researchers also elucidated the molecular mechanisms responsible for this specific form of TBI.

Those findings are described in articles published in the *Journal of Trauma and Acute Care Surgery*, with **Julie Proctor,** UMSOM Lab Manager, as primary author and in *Experimental Neurology*, with Flaubert Tchantchou, UMSOM Research Associate as primary author, and in the *Journal of Neurotrauma*, with Rao Gullapalli, Professor of Diagnostic Radiology, UMSOM, as senior author.

**Mitigating G-force experienced by vehicle occupants**

Fourney, Ulrich Leiste,**,** Assistant Research Engineer in the Clark School's Department of Aerospace Engineering, and doctoral researcher Jarrod Bonsmann, developed highly advanced shock absorber designs that incorporate polyurea-coated tubes and other structures to reduce the blast acceleration experienced by vehicle occupants by up to 80 percent.

"Essentially, it spreads out the application of force," Fourney explains. "Polyurea is compressible and rebounds following compression, resulting in an excellent ability to decrease the acceleration," he says.

**Reducing blast-induced TBI**

These results were combined with those of Dr. Tchantchou, who demonstrated that mitigation of g-force by the elastic frame designs virtually eliminates the behavioral alterations in lab rats and loss of neuronal connections observed using small scale vehicles with fixed frames, as published in the *Journal of Neurotrauma*.

Peter Rock, Martin Helrich Chair of the Department of Anesthesiology, noted that "the research team has addressed an important clinical problem by identifying a novel mechanism to explain TBI, engineered a solution to the problem, and convincingly demonstrated improvements in morphology and behavior. This work has important implications for improving outcomes in military blast-induced TBI and might be applicable to causes of civilian TBI, such as car crashes."

**Looking forward**

UMaryland says that Continued collaboration between the labs of Fiskum and Fourney will hopefully lead to the next generation of armor-protected military vehicles that will further protect warfighters from both injury and death. An important next step will be testing a larger scale model. "If the data holds up for those, it will hold true for full scale," Fourney says.

# Attacks target French embassy, military HQ in Burkina capital

Source: https://www.afp.com/en/news/23/attacks-target-french-embassy-military-hq-burkina-capital-doc-11n6xh1


AFP / Ahmed OUOBA Thick smoke rose from the centre of Ouagadougou as the attacks took place

Mar 02 – The capital of Burkina Faso came under multiple attacks on Friday which targeted the French embassy, the French cultural centre and the country's military headquarters, an AFP reporter and witnesses said.


Witnesses said five armed men got out of a car and opened fire on passersby before heading towards the embassy in the centre of the city.

AFP / Map of Burkina Faso locating Ouagadougou, and a map of the city centre

An AFP reporter heard heavy exchanges of gunfire and saw a blazing vehicle, which witnesses said was the car used by the assailants. Police and army units were deployed in the area.

Other witnesses said there was an explosion near the headquarters of the Burkinabe armed forces and the French cultural centre, which are located about a kilometre (half a mile) from the site of the first attack. There was no early information about any casualties.

The French embassy confirmed that French interests were under attack.

"Attack under way at the French embassy and French Institute. Stay indoors," it said in a terse message posted on Facebook.

**Deadly jihadist insurgency**

Burkina Faso is one of a string of fragile countries on the southern rim of the Sahara that are battling jihadist groups.

**The insurgency has caused thousands of deaths, prompted tens of thousands to flee their homes and dealt crippling blows to economies that are already among the poorest in the world.**

On August 13 last year, two assailants opened fire on a restaurant on Ouagadougou's main avenue, killing 19 people and wounded 21. The attack remains unclaimed.

On January 15 2016, 30 people, including six Canadians and five Europeans, were killed in a jihadist attack on a hotel and restaurant in the city centre.

Responsiblity was claimed by a group called Al-Qaeda in the Islamic Maghreb (AQIM).

France, the former colonial power in the Sahel region, has deployed 4,000 troops and is supporting a five-country joint force gathering Burkina Faso, Chad, Mali, Mauritania and Niger.

The United Nations also has a 12,000-strong peacekeeping force in Mali called MINUSMA, which has taken heavy casualties. Four UN peacekeepers were killed by a mine blast on Wednesday in the centre of the country.

In a separate development on Friday, the specialist US website SITE, which monitors jihadist activity, said kidnappers had released a video of a 75-year-old French hostage, Sophie Petronin, who had been abducted in northern Mali in late 2016.

Petronin, who had been running an association helping Malian orphans, appears in poor health in the brief video.

Her kidnapping, hitherto unclaimed, was carried out by the "Support Group for Islam and Muslims." In the background, the voice of French President Emmanuel Macron is heard on a loop, saying "I will protect you."

# Airborne Counter-IED

**By David Oliver**

Source: https://www.cbrneportal.com/airborne-counter-ied/

Mar 06 – In an age where improvised explosive devices (IED) are being used with devastating effect in a variety of geographic regions, an ability to counter this threat quickly and at no risk to service personnel has become an important strategic imperative worldwide.

The London-based company SteelRock Techonolgies (SRT) provides unmanned aerial vehicle (UAV) and counter-UAV products as well as solutions designed for government and military clients.

Developed in conjunction with technology partner, Richmond Defence Systems (RDS), the SteelRock SRW03 Protector is a UAV-borne IED disrupter that is able to neutralise a wide range of IED threats either from the air or on the ground. Combining SRT's leading-edge UAV technology with RDS's highly effective, laser-guided disrupter technology, the Protector offers a highly effective counter-IED solution.

The SRWO3 Protector UAV is a state-of-the-art rotary-wing UAV that has been designed and configured for IED threat identification and mitigation. Using an interchangeable payload system comprising a sophisticated thermal electro-optical (EO) camera and a 40mm recoilless IED disrupter with an encrypted fire control, the system has been developed as a "seek and destroy" solution to this increasing threat.

The platform is built around an X8 KDE Direct brushless motor/rotor drive system with two counter-rotating propellers and motors at each corner. The platform has been designed with heavy lift payloads and stability in flight for a wide range of operating conditions. The platform integrates a Selex Hawk thermal camera and the RDS recoilless disruptor with a laser targeting system, all configured for use on the WO3 platform.

With a maximum speed of 100 km/h, the SRW03 UAV has a maximum telemetry range of 150 km from base station and can carry a 50 kg payload for up to 2 hours. A series of trials at SteelRock's test facility in South Wales the Protector system has successfully disrupted and neutralised IED threats both at ground level and while airborne.


The ST Engineering Stinger UAV armed with an Ultramax U100 Mk.8 5.56mm machine gun. (David Oliver)

A similar C-IED system has been adopted by the Singapore company, ST Engineering with its Stinger Intelligent Network Gun Equipped Robotics system. The system is under development as part of ST Engineering's Future Soldier Solution and includes a quad-rotor UAV armed with the world's lightest 5.56 mm machine gun, the 6.8 kg Ultramax U100 Mk.8 with a constant recoil system with low-felt recoil which enables it to be fired accurately in full automotive mode from a UAV. It is able to carry 100 rounds and the systems can also include a laser-range finder with an accuracy of up to 300 m.

**▶▶ Read the rest of this article at source's URL.**

***David Oliver*** *is a defence photo-journalist for more than 30 years, and member of the Independent Defence Media Association (IDMA) and the European Security and Defence Press Association (ESDPA). David is the author of 18 defence-related books, and is former IHS Jane's consultant editor and a regular correspondent for defence publications in the UK, USA, France, Poland, Brazil and Thailand.*

# Islamic Jihad terrorist accidentally blows himself up in Gaza

Source: http://www.jpost.com/Arab-Israeli-Conflict/Islamic-Jihadi-dies-in-accidental-explosion-while-manufacturing-weapons-544773

Mar 11 – **A member of Saraya al-Quds, Islamic Jihad's armed wing, died in an "accidental explosion" in the northern Gaza Strip,** said Ashraf al-Qidra, a spokesman for the Hamas-run Health Ministry in the coastal enclave, on Saturday night, according to the Hamas-linked Palestinian Information Center.


Qidra identified the deceased member of Saraya al-Quds as **27-year-old Ibrahim Frahat.**

Saraya al-Quds said in a statement that Frahat died "while preparing for battle," making no mention of an "accidental explosion."

Maj.-Gen. Yoav Mordechai, the Defense Ministry official responsible for liaising with Palestinians, said that Frahat died while "manufacturing weapons and ammunitions for Islamic Jihad in a house in the Sheikh Zayed neighborhood in Beit Lahiya."

"It is no surprise that a person who plays with fire ultimately harms himself," Mordechai said in a Facebook post.

# Teen dies in third package bombing in Austin, Texas

Source: https://news.sky.com/story/police-investigate-third-explosion-in-austin-texas-after-bomb-kills-teenager-11287624

Mar 12 – **Three package bombings which have killed two people in 10 days are believed to be linked,** say police in Texas.

Officers in Austin spoke about the attacks following two explosions on Monday.


Just hours after a package bomb killed a teenager and wounded a woman, police were called to deal with another blast elsewhere in the city.

Detectives are linking the incidents to a similar bombing in the city earlier in March, in which a 39-year-old man was killed.

**They are investigating whether the bombings were racially motivated as all the victims are black.**

Mr Manley told reporters after the latest blast on Monday: "Based on evidence that we have at this scene, as well as at the other two scenes where we've had these explosions, this evidence makes us believe that these incidents are related."

Mr Manley had earlier tweeted: "My heart goes out to the family of the individual who died and was injured from the explosion in Old Fort Hill. This type of crime will not be tolerated in ATX."

It comes as hundreds of thousands of visitors descend on the city for the South By Southwest music, film and technology festival.

Officials have urged the public to call police if they receive any packages they are not expecting.

**The three explosions occurred in different areas in the east of the city.**

The first explosion on Monday happened at a home near the Windsor Park district, and about 12 miles from the home where the first explosion, on 2 March, killed 39-year-old Anthony Stephan House.

The first blast was first thought to have been a suspicious death but is now being treated as murder.

# UAE Armed Forces clear 20,000 landmines across Yemen

Source: https://www.thenational.ae/uae/uae-armed-forces-clear-20-000-landmines-across-yemen-1.713066

Mar 18 – UAE Armed Forces have cleared more than 20,000 landmines across Yemen, according to state news agency Wam.

**The illegal mines were removed from areas stretching across the Red Sea Coast over an eight-month period.**

It is suspected the mines first began to be planted by rebel Houthi militias after the Saudi-led Arab Coalition moved forces into the country to restore Yemen's legitimate government.

Specialists within the UAE Armed Force have trained 65 Yemeni volunteers to safely excavate the suspected areas, a de-mining expert told Wam.

He said **90 per cent of the explosives dug up are Iranian-made and patterned after the Russian TM-57 mine** – that can blast armoured fighting vehicles.

"The mines are being detonated in safe areas as per the latest international standards," he said, adding that most of the mines were found in areas adjacent to heavily populated districts.
The mines planted in mountainous areas are disguised as rocks but are also concealed in sandy dunes, he said.
Health professionals and local activists estimate that thousands of civilians have been injured or killed by the explosives.
Emirates Red Crescent, the UAE's main humanitarian arm, is covering treatment costs for those injured in the blasts, according to Juma Al Mazroui, head of the ERC team in Aden.

“Up to 4,000 wounded Yemenis have been treated in the UAE, Jordan, Sudan and India, some of whom have already recovered and returned home, while the rest are still being treated," he said.
**"The military field hospital staged by the UAE received up to 2,500 persons injured by mines in four months, some of whom are critically wounded,"** said Mohammed Abdullah, the head of the hospital's medical team.
Dr Ishraq Al Sibai, the undersecretary of Yemen’s Ministry of Health, described the landmines as a “stab in the back” by Houthi militias.
She said the illegal mines have triggered a humanitarian crisis in the country and left thousands of people in Yemen’s Red Sea Coast with disabilities.
Saleh Abdu, a father to six children, lost both his legs in a landmine explosion.
"The Houthis planted booby-traps in front of our houses in a way that was impossible for the families to take any precaution of pre-emptive measures,” Mr Abdu said.
He said the mines killed some of the villagers and left others disabled.
The mines planted in mountainous areas are disguised as rocks but are also concealed in sandy dunes, Wam reported. Wam
"I lost consciousness after the explosive went off. And later I came to know that people around me carried me to Mocha Hospital and later to the military field hospital run by the UAE Armed Forces."
Samira Mahmoud, a mother of two, had her right hand amputated after a landmine explosion destroyed her home. "We were expelled from our homes by Houthis," she said.
The mines have also taken their toll on the elderly, leaving some without families to support them.
"I was sitting in front of my house waiting for my grandchildren to come and take me for lunch, then I heard a massive explosion inside the house," said 78-year-old Saleh.
He said his son ran out to rescue the rest of the family only to trigger another explosion which left all of Saleh’s sons, their wives and children dead.
Khalil Ahmed, a 10-year-old Yemeni, was another victim of the explosives.
He was playing with his friends from in Al Ruweis Village in Mocha when he heard a blast. Debris sprayed across the area and tore through his body. Khalil was rushed to the military

field hospital where he underwent a two-hour surgery to remove the shrapnel. He was airlifted to UAE to continue his recovery.

## Letter Bomb and IED Detector for mail & parcel inspection

Source: http://www.ceia.net/security/product.aspx?a=EMIS-MAIL

The EMIS-MAIL is designed to detect a wide variety of metal threat items including detonators, batteries, trigger circuits and other metal components of parcel bombs without false alarms for non-threat items such as metal staples, paper clips and metal binding spirals. The EMIS-MAIL is very easy to use and provides a fast and automatic alarm/no alarm signal confirmation per each inspected package. Its compact, ergonomic design along with the electric and built-in NiMH rechargeable battery power supply allows for independent operation in a variety of locations. An optional embedded radioactive detector is also available for radioactive material threat detection.



The EMIS-MAIL is uniquely qualified to operate in a prison or correctional facility environment with specific settings available for prison parcel inspection. Along with meeting the strictest safety and security standards, EMIS-MAIL is also compliant with the EU Regulation 185/2010 for the inspection of letters and parcels.

**Key features of the CEIA EMIS-MAIL include:**

- Ease of Installation and Setup
- Ease and Speed of System Use with Limited Screener Training Required
- Automatic Inspection of Parcels and Letters up to 450 mm x 75 mm
- No Calibration or Periodic Maintenance Required
- Independent Operation with Mains Power Supply or Built-in NiMH Rechargeable Batteries

## EMA series Liquid Explosive Detector

Source: http://www.ceia.net/security/product.aspx?a=EMA%20series

The EMA is a compact device designed for the analysis of liquid containers and their contents with the goal of detecting the possible presence of explosive precursors and explosive liquids.
The content of the bottles is analyzed without the need to open the container as the detection is effected using simultaneous multiple sensing technologies.
The housing of the analyser, which is extremely robust, durable and easy to clean, is made of AISI 304 Stainless Steel and anti-friction plastic.
The Analyser consists of a main body, a control panel and an analysis compartment. In case of open containers such as cups and thermos flasks, it is possible to carry out the analysis by means of the type A integrated analyser (optional), using small disposable plastic sample cups to be inserted into an external probe.

**Inspection of bottles or containers**

- Independently of their shape
- Made of different materials
- In a wide range of capacity

**CEIA EMA and LEDS Requirements**

Type B Liquid Explosive Detection Systems are intended for the inspection of individual liquid containers with the purpose of detecting explosives and their precursors, according to the current Regulation Authority requirements (EU Reg. No 185/2010).


As containers can be made of different materials and can have different geometry and volume, the use of multiple simultaneous physical principles is necessary for a reliable and secure screening.

The CEIA EMA analyser family design started in 2003; since then the number of sensors installed on-board have been growing in order to comply with the increasing requirements on the liquid threats to be detected and on the kind of containers to be inspected. The comprehensive set of sensors installed on the equipment makes the EMA liquid analyser a unique machine on the market providing very high security and set for future detection requirements.

The CEIA EMA includes an EU Standard 3 Certified type A analyser (optional) to screen loose liquids, open containers or following to an alarm on the type B section. A disposable cup allows sampling and measurement of a minimum quantity of liquid to be analysed.

**Operating principle**

When the operator places the bottle in the inspection cavity, its presence is automatically detected and the analysis is performed in ~ 5 seconds.

The fields generated in the inspection cavity are weak in intensity and non-ionizing, therefore completely safe for the liquids and for the operator.

The fields interact with containers and with their content. The entire volume is analyzed in order to verify its conformity with allowed liquids.

After a few seconds, the unit provides an OK or ALARM message without requiring any data interpretation by the operator.

Calibration is carried out automatically by the unit.

## How Many Bombs Does a Non-Muslim Need to Set Off Before Being Called a Terrorist?

**By Dean Obeidallah**

Source: https://www.mediaite.com/tv/how-many-bombs-does-a-non-muslim-need-to-set-off-before-being-called-a-terrorist/

Mar 22 – What if a 23-year-old Muslim man set off six bombs in a two-week period that killed two Americans and injured several others? Add to that, what if that same Muslim man ended his life as a suicide bomber, blowing himself up as the authorities moved in to arrest him, killing himself and wounding a police officer?

Any doubt the headlines would include the word "terrorist"? Of course not. The "T word" would be everywhere and we would see wall to wall terrorism-focused coverage on cable news, complete with a cadre of former FBI agents and terrorism experts exploring how this man was radicalized.

And of course, Donald Trump would use the incident to further his own political agenda just as he did after last year's deadly terror attack in New York City where he called for an end to the decades old Diversity Visa Program.

But when that exact fact pattern played out with the suspected Austin serial bomber, Mark Conditt, including Conditt in essence ending his life as a suicide bomber and injuring a police officer, the response was starkly different. First off, you don't see the word terrorism used in connection with this incident, except for the media reporting that the White House stated that there's **"no apparent nexus to terrorism."**

Instead of calling Conditt a terrorist, the media has described him with terms like "intense loner," who had


been "homeschooled." Even the Austin police chief told us that the 25-minute confession Conditt recorded before he blew himself up was "the outcry of a very challenged young man talking about challenges in his personal life that led him to this point."

Do you recall these types of words used to describe the ISIS-inspired terrorist who waged a deadly truck attack in New York City last year? Of course not. In fact, shortly after the attack, Trump called that man an "animal" adding that we should "send him to Gitmo."

While the Austin bombing was the top story on cable news on Tuesday morning, that quickly faded. If the bomber had been Muslim, it's unlikely that would have been the case since history tells us that there would've been in depth discussions on how he had been radicalized, how to prevent future attacks, etc.

And Trump just about ignored the story because the incident couldn't help him politically. His sole, simple tweet about the Austin bomber on Tuesday morning was this: "AUSTIN BOMBING SUSPECT IS DEAD. Great job by law enforcement and all concerned!"

We know his tweets would've been far different if Conditt had been an immigrant or a Muslim.

This raises the question: **How many bombs does a non-Muslim need to set off before the media and Trump will call the person a terrorist?** That's easy to answer with Trump. In his case, if it's a white Christian bomber — as with the Austin attacker — we can forget him ever using the word "terrorist." After all this is the same Trump whose response after the white supremacist terror attack last August in Charlottesville that left Heather Heyer dead was to call the white supremacists there "very fine people." Trump understands his base better than any of us, thus, he knows he needs the support of white supremacists.

With respect to the media, it's challenging to get many — though not all — to use the term "terrorism" when it comes to a white person. After Charlottesville, few in the media used the term terrorist to describe the white supremacist who killed Heyer. Same goes for Dylann Roof, who executed nine African Americans in 2015 in the hopes of starting a race war. Instead we saw Roof often described, as the *New York Times* did back in 2015, as being "troubled" and coming from a "broken home." It seems for many in the media, except for Timothy McVeigh, the word terrorism doesn't apply to white people.

**But what Conditt did was in fact terrorism.** As listeners to my SiriusXM radio show who live in Austin, Texas made clear: They had been terrorized by Conditt for nearly two weeks. One listener, an African American woman, explained how after the first two Conditt killed

were black, she and others in her community felt like they were being specifically targeted, adding to the fear.

Others from Austin shared with me how they stayed home at night and changed their daily routines because they were afraid of being the bomber's next target. That's not only the common sense understanding of terrorism but I'd argue fulfills the definition of terrorism under the federal law since Conditt clearly used his bombings to "intimidate or coerce a civilian population."

**The Austin bomber should be called a terrorist.** That is what he was. And same for any person — regardless of religion or race — who engages in a campaign of terror like Conditt did that spanned nearly two weeks and was intended to terrorize Americans. The only thing preventing that appears to be that he isn't Muslim.

And that not only shows a double standard, it makes us less safe as a nation. As the Anti-Defamation League has documented, of the 34 extremist related deaths last year in the United States, 18 were committed by right wing actors compared to nine by Islamic related terrorists.

Words matter and it's time to use the word terrorism in a common sense way and not just apply it people from one religion. That is the only way to keep our nation safe.

***Dean Obeidallah,*** *a lawyer, hosts SiriusXM radio's The Dean Obeidallah show and is a columnist for the Daily Beast and a CNN.com Opinion Contributor.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

# CYBER NEWS

# Hacker-resistant power plant software in a successful Hawaii tryout

Source: http://www.homelandsecuritynewswire.com/dr20180227-hackerresistant-power-plant-software-in-a-successful-hawaii-tryout

Feb 27 – **Johns Hopkins computer security experts recently traveled to Hawaii to see how well their hacker-resistant software would operate within a working but currently offline Honolulu power plant.** The successful resilience testing, funded by the U.S. Department of Defense, was triggered in part by growing concerns about the vulnerability of electric power grids after two high-profile cyber-attacks by Russian government hackers turned out the lights in parts of Ukraine during the past two years. Neither outage in Kiev was long or extensive enough to cause serious harm or panic. Yet the attacks served as a wake-up call, putting a spotlight on power grid security in the United States and elsewhere.

"Today, our power system is not designed to withstand the kind of attacks that happened in Ukraine," said Yair Amir, professor and chair of the Department of Computer Science in the university's Whiting School of Engineering. "If even part of a power grid's control system is compromised, the game is over. We need to make our grid more secure, resilient and intrusion-tolerant."

Amir and his team of researchers hope to help boost resilience with their **new open-source control system for power grids called Spire.** The intrusion-tolerant system is designed to keep power flowing even if part of the system is compromised.

JHU says that in an experiment last April, a Sandia National Laboratories hacker team was able to remotely obliterate a commercial grid control system within a couple of hours, but the team could not penetrate the Spire system for three days. On the third day, the Sandia **attack team was given remote access to part of Spire, but its test hackers still could not disrupt the system's correct operation**.

More recently, the Spire developers from Johns Hopkins were invited to get their feet wet in Hawaii. At the end of January, Amir and his team went to an offline Hawaiian Electric Company plant in Honolulu and spent two weeks testing the Spire system on the power plant's equipment with the help of HECO engineers Keith Webster and John Tica. After a few days of setup and integration, Spire ran continuously without interruption for almost a full week.

The goal of the Hawaii deployment was to verify that Spire can operate without degrading the control system's performance and without adverse effects on other power plant systems.

A power grid needs to respond to adverse events—say, a circuit breaker tripping or a generator shutting down—within hundreds of milliseconds, Amir said. "If a generator goes out, the system needs to quickly detect it and compensate by increasing power in other generators or by cutting power to parts of the grid."

On the last day of the Hawaii test, Webster deployed a device to measure end-to-end reaction time of the commercial control system in the plant and of Spire. The measurements showed that the commercial system reflected a change in the grid's power state within 900 milliseconds to one second. Spire showed the same change within 400–500 milliseconds, meeting the timeliness requirement.

Part of how the system works is with the help of replicas. The researchers built it to contain six copies of the main control server that work together to agree on updates in the system. That's the smallest number of replicas needed to get good protection, Amir says. "Each replica votes on every data and decision," he added. "If one of the replicas is compromised and another is going through maintenance, then the other good replicas will enable the system to continue working properly and in a timely manner."

Why was the test conducted in Hawaii? First, the research project was funded by the Department of Defense, which is one of HECO's largest customers. In addition, Amir said, the unique access to a "mothballed" power plant with fully functional control systems but without active power generation was perfect for grid-level control system tests. "If something goes slightly wrong," he said, "at least you don't have a quarter million people losing power."

**Amir and his colleagues plan to release Spire 1.1, the version that was deployed in this test-deployment, in the coming weeks.** Version 1.0, tested in April, is already available for download.

Making Spire open-source was kind of a "no-brainer," Amir said. He has spent over a decade of his research career working on intrusion-tolerant systems and networks. He said that releasing the source code openly increases awareness and the chance for real-life impact.

The U.S. power grid is a logical target for major cyberattacks, he said. Disabling or tampering

with the grid on a large scale, Amir said, could seriously harm the country by disrupting lives and causing immense economic loss.
"We decided that we won't just publish our results," he added, "but we will release open-source solutions that will show people how to make control systems for the power grid secure, resilient, and intrusion-tolerant," Amir said. "We want to create a community of people who are really interested in that. We need to protect our critical infrastructure."

## Startup offering a solution to deter dangerous railway hacking

Source: http://www.homelandsecuritynewswire.com/dr20180309-startup-offering-a-solution-to-deter-dangerous-railway-hacking

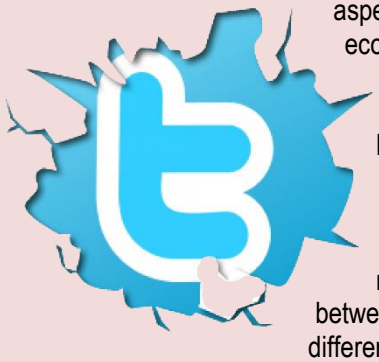
Mar 09 – Rail transport is undergoing a huge transformation thanks to automated, wireless and connected technologies that whoosh passengers down the tracks faster and more efficiently than ever before possible. However, these same technologies have opened a door to new types of cyber-attacks that can threaten passenger safety, disrupt service and cause serious economic damage. A new startup has raised $4.7 million in seed money to develop its proactive solution to protect railways and metros.

## Study: On Twitter, false news travels faster than true stories

**By Peter Dizikes**

Source: http://www.homelandsecuritynewswire.com/dr20180312-study-on-twitter-false-news-travels-faster-than-true-stories

Mar 12 – A new study by three MIT scholars has found that false news spreads more rapidly on the social network Twitter than real news does — and by a substantial margin.
"We found that falsehood diffuses significantly farther, faster, deeper, and more broadly than the truth, in all categories of information, and in many cases by an order of magnitude," says Sinan Aral, a professor at the MIT Sloan School of Management and co-author of a new paper detailing the findings.
"These findings shed new light on fundamental aspects of our online communication ecosystem," says Deb Roy, an associate professor of media arts and sciences at the MIT Media Lab and director of the Media Lab's Laboratory for Social Machines (LSM), who is also a co-author of the study. Roy adds that the researchers were "somewhere between surprised and stunned" at the different trajectories of true and false news on Twitter.



**Moreover, the scholars found, the spread of false information is essentially not due to bots that are programmed to disseminate inaccurate stories. Instead, false news speeds faster around Twitter due to people retweeting inaccurate news items.**
"When we removed all of the bots in our dataset, [the] differences between the spread of false and true news stood,"says Soroush Vosoughi, a co-author of the new paper and a postdoc at LSM whose PhD research helped give rise to the current study.
The study provides a variety of ways of quantifying this phenomenon: For instance, false news stories are 70 percent more likely to be retweeted than true stories are. It also takes true stories about six times as long to reach 1,500 people as it does for false stories to reach the same number of people. When it comes to Twitter's "cascades," or unbroken retweet chains, falsehoods reach a cascade depth of 10 about 20 times faster than facts. And falsehoods are retweeted by unique users more broadly than true statements at every depth of cascade.
The paper, "The Spread of True and False News Online," is published today in *Science*.

**Why novelty may drive the spread of falsity**

The genesis of the study involves the 2013 Boston Marathon bombings and subsequent casualties, which received massive attention on Twitter.
"Twitter became our main source of news," Vosoughi says. But in the aftermath of the tragic events, he adds, "I realized that … a good chunk of what I was reading on social media was rumors; it was false news." Subsequently, Vosoughi and Roy — Vosoughi's

graduate advisor at the time — decided to pivot Vosoughi's PhD focus to develop a model that could predict the veracity of rumors on Twitter.

Subsequently, after consultation with Aral — another of Vosoughi's graduate advisors, who has studied social networks extensively — the three researchers decided to try the approach used in the new study: objectively identifying news stories as true or false, and charting their Twitter trajectories. Twitter provided support for the research and granted the MIT team full access to its historical archives. Roy served as Twitter's chief media scientist from 2013 to 2017.

To conduct the study, the researchers tracked roughly 126,000 cascades of news stories spreading on Twitter, which were cumulatively tweeted over 4.5 million times by about 3 million people, from the years 2006 to 2017.

To determine whether stories were true or false, the team used the assessments of six fact-checking organizations (factcheck.org, hoax-slayer.com, politifact.com, snopes.org, truthorfiction.com, and urbanlegends.about.com), and found that their judgments overlapped more than 95 percent of the time.

Of the 126,000 cascades, politics comprised the biggest news category, with about 45,000, followed by urban legends, business, terrorism, science, entertainment, and natural disasters. The spread of false stories was more pronounced for political news than for news in the other categories.

The researchers also settled on the term "false news" as their object of study, as distinct from the now-ubiquitous term "fake news," which involves multiple broad meanings.

The bottom-line findings produce a basic question: Why do falsehoods spread more quickly than the truth, on Twitter? Aral, Roy, and Vosoughi suggest the answer may reside in human psychology: We like new things.

**"False news is more novel, and people are more likely to share novel information,"** says Aral, who is the David Austin Professor of Management. And on social networks, people can gain attention by being the first to share previously unknown (but possibly false) information. Thus, as Aral puts it, "people who share novel information are seen as being in the know."

The MIT scholars examined this "novelty hypothesis" in their research by taking a random subsample of Twitter users who propagated false stories, and analyzing the content of the reactions to those stories.

The result? "We saw a different emotional profile for false news and true news," Vosoughi says. "People respond to false news more with surprise and disgust," he notes, whereas true stories produced replies more generally characterized by sadness, anticipation, and trust.

So while the researchers "cannot claim that novelty causes retweets" by itself, as they state in the paper, the surprise people register when they see false news fits with the idea that the novelty of falsehoods may be an important part of their propagation.

**Directions for further research**

While the three researchers all think the magnitude of the effect they found is highly significant, their views on its civic implications vary slightly. Aral says the result is "very scary" in civic terms, while Roy is a bit more sanguine. But the scholars agree it is important to think about ways to limit the spread of misinformation, and they hope their result will encourage more research on the subject.

On the first count, Aral notes, the recognition that humans, not bots, spread false news more quickly suggests a general approach to the problem.

"Now behavioral interventions become even more important in our fight to stop the spread of false news," Aral says. "Whereas if it were just bots, we would need a technological solution."

Vosoughi, for his part, suggests that if some people are deliberately spreading false news while others are doing so unwittingly, then the phenomenon is a two-part problem that may require multiple tactics in response. And Roy says the findings may help create "measurements or indicators that could become benchmarks" for social networks, advertisers, and other parties.

The MIT scholars say it is possible that the same phenomenon occurs on other social media platforms, including Facebook, but they emphasize that careful studies are needed on that and other related questions.

In that vein, Aral says, "science needs to have more support, both from industry and government, in order to do more studies."

For now, Roy says, even well-meaning Twitter users might reflect

on a simple idea: "Think before you retweet."

*— Read more in Soroush Vosoughi, Deb Roy, and Sinan Aral, "The spread of true and false news online," Science 359, no. 6380 (9 March 2018) (DOI: 10.1126/science.aap9559).*

# Russia planted sabotage-enabling malware in U.S. energy grid, other critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20180316-russia-planted-sabotageenabling-malware-in-u-s-energy-grid-other-critical-infrastructure

Mar 16 – Russia has not only attacked the infrastructure of American democracy: The U.S. government now says that Russia has engaged in a pervasive, wide-ranging cyber-assault on U.S. energy grid and other key components of the U.S. critical infrastructure.

These sustained attacks on U.S. critical infrastructure – along with the Russian interference in the 2016 election and the Russian-launched NoPetya malware — were the reasons the administration on Thursday imposed a new round of sanctions on Russia.

The sanctions the administration imposed on Thursday, though, still fall short of the sanctions enacted into law by Congress last August, and which were supposed to be imposed by 31 January. Trump reluctantly signed the sanction bill, but refused to order the implementation of the sanctions.

Most of the sanctions announced on Thursday were prepared by the Obama administration in December 2016, and were left for the incoming Trump administration to implement.

The *New York Times* reports that U.S. officials said that malware written by Russian government hackers had been found in the operating systems of several organizations and companies in the U.S. energy, nuclear power and processing, water ,and "critical manufacturing" sectors. The officials said that with the help of sophisticated digital forensic methods, the malware as well as other form of cyberattacks had been traced back to Moscow.

"Russia's behavior continues to trouble us and we are continuing to push back in meaningful ways," a senior national security official said.

The FBI and the DHS jointly issued an alert, calling on firms in the affected critical infrastructure sectors thoroughly to review and upgrade their cybersecurity. The alert said the concerted Russian cyberattack on U.S. infrastructure began in March 2016.

"It is the judgment of the DHS that Russian government cyberhackers were behind the hacking of organizations in the energy sector," a senior official said, adding that it was clear that the cyberattack was coordinated at the highest levels of the Russian government and that the attacks "deliberately targeted" critical infrastructure assets.

U.S. senior intelligence and security officials told the *Times* that the initial motive for the Russian cyberattack was surveillance, aiming to allow Russian intelligence to gather information on computer management systems throughout the U.S. energy sector.

The Russian hackers never went so far as to sabotage or shut down the computer systems of the various companies and organizations they infiltrated – systems which guide the operations of the plants.

Still, new computer screenshots released by DHS on Thursday show that Russian government hackers had gained foothold they would have needed to manipulate, sabotage, or shut down power plants.

In a report made public in October, Symantec noted that a Russian hacking unit "appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so."

"We now have evidence they're sitting on the machines, connected to industrial control infrastructure, that allow them to effectively turn the power off or effect sabotage," Eric Chien, a security technology director at Symantec, a digital security firm, told the *Times*.

"From what we can see, they were there. They have the ability to shut the power off. All that's missing is some political motivation," Chien said.

The U.S. intelligence community has been aware since last June of the scope and reach of Russia's attacks on U.S. infrastructure – but

yesterday joint FBI-DHS alert is the first time the administration names Russia as the perpetrator of the attacks.

The cybersecurity alert issued by the FBI and DHS said: "DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing and gained remote access into energy sector networks."

"After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to industrial control systems," the alert added.

In addition to the Russian cyberattacks on U.S. critical infrastructure assets, the U.S. Treasury Department cited Russian interference in the 2016 election as another reason for the new round of sanctions. Sanctions were imposed on the three main Russian actors – Russia's two main intelligence services, the FSB and the GRU, and the GRU-operated IRA troll farm — which orchestrated the Kremlin's campaign of interference in the 2016 election.

As a result of Russia's election interference, U.S. officials said that thousands of Russian-planted stories reached "millions of people online" during the U.S. presidential campaign.

The *Times* notes that the new sanctions are the broadest set of U.S. punitive measures against Russia since the Trump administration came to power, and that many of the targets of the new sanctions are the same as those indicted by Robert Mueller.

The sanctions were also imposed for the role of Russian intelligence hackers played in writing and in distributing the NotPetya malware and ransomware. Officials said the NoPetya attack was initially aimed to damage Ukraine, but was allowed to "propagate recklessly without bounds" and caused an estimated $10 billion in damage around the world, making it the most damaging and costliest cyberattack in history.

"The administration is confronting and countering malign Russian cyber-activity, including their attempted interference in US elections, destructive cyber-attacks, and intrusions targeting critical infrastructure," Steven Mnuchin, the treasury secretary, said in a statement.

"These targeted sanctions are a part of a broader effort to address the nefarious attacks emanating from Russia. Treasury intends to impose additional … sanctions, informed by our intelligence community, to hold Russian government officials and oligarchs accountable for their destabilizing activities by severing their access to the U.S. financial system."

Cybersecurity experts note that the Russian government hackers who conducted the energy attacks belong to a different group from the two groups of hackers which were involved in the 2016 election interference.

This would suggest that there were at least three separate Russian cyberoperations which were being conducted simultaneously. Two of the operations were geared to help Trump win the election: One focused on stealing documents from the Democratic National Committee, the Clinton campaign, and other political groups. The second, conducted by the St. Petersburg-based IRA troll farm, used social media to reach 126 million Americans with false postings, fake news, and misleading assertions aiming sow discord and division along racial, ethnic, and religious lines. The third effort sought to infiltrate U.S.(and European) critical infrastructure nodes.

The *Times* notes that private security firms have tracked the Russian government assaults on Western power and energy operators — conducted alternately by groups under the names DragonFly, Energetic Bear, and Berserk Bear — since 2011, when the Russian government first started targeting defense and aviation companies in the United States and Canada.

By 2013, researchers had linked the Russian government hackers to hundreds of attacks on energy grid and oil and gas pipeline operators in the United States and Europe. The cyberattacks initially appeared to be motivated by industrial espionage — researchers say that at the time is was a natural conclusion to draw, given the importance of Russia's oil and gas industry.

But by December 2015, the Russian hacks had taken an aggressive turn. The attacks were no longer aimed at intelligence gathering, but at potentially sabotaging or shutting down the operation of infrastructure facilities.

Security experts do not regard the sanctions announced on Thursday as tough enough to cause the Kremlin to rethink its campaign of political interference and infrastructure infiltration.

Lt. Gen. Paul Nakasone, who has been nominated as director of the National Security Agency and

commander of United States Cyber Command, said during his Senate confirmation last week that countries attacking the United States so far have little to worry about.

"I would say right now they do not think much will happen to them," General Nakasone said. He later added, "They don't fear us."


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

# Train Safety Raised as Issue in Hospital Debate

Source: http://www.govtech.com/em/disaster/Train-Safety-Raised-as-Issue-in-Hospital-Debate.html

Feb 22 – The train tracks pass within a half mile of the site proposed by the Mohawk Valley Health System. The group #NoHospitalDowntown has been sounding the alarm over whether it makes sense to build a hospital in an area likely to be evacuated in case of a train wreck that results in a fireball.
Many train safety advocates refer to the area within half a mile of tracks as the red zone.
Brett Truett, a co-founder of the group that opposes the downtown hospital site, warned about the proximity between the site and the tracks in an April 10, 2016, Facebook post.
"It was further explained that in the event of a train derailment, especially one carrying toxic materials, a certain radius around the crash site would need to be evacuated," he wrote. "If this were to include the new hospital, a compound problem would exist; the hospital might need to be evacuated, yet potential accident victims would be seeking care at the hospital."
**But Kevin Revere, director of the Oneida County Department of Emergency Services, dismissed the need to weigh that concern in siting a new hospital. "To me, it's a nonissue. It's so small (a risk), it really shouldn't be under consideration," he said.**

**EDITOR'S COMMENT:** "Small risks sometimes lead to enormous disasters" Mr. Revere! Because the unexpected always happens. It is obvious that he does not live in that area…

**'Safer than ... roads'**
Dangerous liquids are transported by trains because that's the safest method, Revere said. "It's safer than putting it on roads across the country," he said.
That's not to say that the trains don't concern Revere as they pass by many houses and businesses in the county. But the hospital would, first of all, be noncombustible construction, he said.
And the odds of a train derailment affecting the hospital are tiny, he said.
"Something would have to happen literally right there, a little ways from there," he said.
Life is full of scary scenarios with a much higher likelihood of occurring, he said.
Scott Perra, health system president/CEO, said the health system and the county have done extensive research on the issue. Transportation officials do not use the term "red zone," he said.
And CSX, a transportation company that runs freight trains through Utica, says it works with many communities on safety concerns.
"CSX operates an extensive network, encompassing 21,000-plus miles of track through 23 states and thousands of communities, making public safety a top priority," CSX said in a statement sent to the O-D. "CSX works closely with local and state economic development groups, planning departments and commercial real estate professionals in support of growth for communities. Typically, CSX is actively involved in commercial projects involving businesses that use freight rail in their operations. CSX's goal is to balance the needs of growing communities with that of our freight rail customers."

**Lax regulations?**
Fred Millar, an independent rail safety consultant in Washington, D.C., with a background in both emergency management and environmental advocacy, said that guidelines don't prevent construction near tracks.
But he doesn't think that's because building near a rail line is safe. He said he thinks rail safety rules are far too lax with even common-sense precautions fought off by the industry.
"There's not rules in the country, that I know about, in terms of land use in terms of planning and zoning that say you can't do this near a rail line," he said.
He particularly fears the potential outcome of either the derailment of or a terrorist assault on chlorine tankers, which could release a huge cloud of toxic gas.
If the health system really looked at the risks, it would likely choose to go elsewhere, Millar speculated.
"We shouldn't even build railroads through major developed areas," he said.
**The Trump administration recently rolled back one new regulation from the Obama era requiring trains carrying crude oil and hazardous chemicals to update to safer braking systems.**

That regulation came in the wake of several train accidents that spilled crude oil and caused fires, some of which burned for days. The worst was in 2013 in Lac-Megantic, Quebec, when a runaway train car spilled oil that burned downtown, killing 47 and destroying 30 buildings.

# The Interconnectivity Needed to Keep Kids Safe in School

Source: http://www.govtech.com/em/disaster/The-Interconnectivity-Needed-to-Keep-Kids-Safe-in-School.html


Student survivors from Marjory Stoneman Douglas High School are greeted as they arrive at a rally for gun control reform on the steps of the state capitol, in Tallahassee, Fla., Wednesday, Feb. 21, 2018. AP/Gerald Herbert

Feb 22 – Lots of people saw warnings signs that Nikolas Cruz could be a danger to others. It may have been worse than anyone could imagine — 14 students and three teachers killed at Stoneman Douglas High School in Parkland, Fla. — but the signs of trouble were there.

Several students noted after the shooting the antisocial tendencies exhibited by Cruz and that police had been to his house on numerous occasions. Obviously there was no system in which that information could get processed and help, in the form of counseling, restraining order or whatever appropriate, could be dispensed.

This is typical, say experts on school safety, and needs to change. There are other viable ways of protecting students as well, including centralized entry, where the students are greeted and perhaps even move through a metal detector.

"There's certainly value in security measures like access control and securing areas in the school and so on," said Amy Klinger, director of programs and co-founder of Educator's School Safety Network. "The problem is we've spent a lot of time and energy on stuff — access control systems, and metal detectors, and visitor sign-ins and all this — but have not spent equal time and money on training people, and education is a people business."

Klinger said the teachers and administrators on campus are the first responders and are being asked to deal with situations that they are not equipped or trained to deal with. What's needed, along with training, is a system or "coordinated, collaborative" response to the signs that were so evident in the Cruz case and other cases.

The school does one thing, mental health does another and law enforcement does another. They are silos and not connected in terms of communication and cooperation and should be.

"Clearly there is a role for law enforcement but one of my

concerns and ongoing frustrations is that law enforcement is the only entity you hear from," Klinger said. "You don't hear [the media talking] about the educators, the mental health people. We still have this notion that it's a law enforcement problem, and it's not."

Klinger said every school needs an active, well-trained, interdisciplinary threat assessment team and many don't have one. The team should have the ability to identify individuals who may be at risk and be able do something about it.

"You can come at it from many different angles, trying to get counseling, mental health intervention, pressing charges, restraining order or support and intervention in the school," Klinger said. "Not just, 'We tossed the kid and got afraid of what might happen,' not that that happened in [with Cruz] but it's typical."

Most of the training educators get, if any, is Run, Hide, Fight, which is a program for reacting to an active shooter scenario.

Klinger said that's fine but it's not preventive, and it's putting all the eggs in one basket. "Now you have people who are trained in Run, Hide, Fight, but don't know what to do in a medical emergency, a bus accident or an intruder with a knife."

She said school resource officers (SRO) are great too, but you can't deploy enough of them to be everywhere, and she noted that there was an SRO on the Stoneman Douglas campus as well as one on the Columbine and the Arapahoe High School campuses during those Colorado shootings.

President Trump seems to have advocated training and arming six or eight teachers on campus to thwart the threat. Experts say even well-trained police officers have difficulty in the moment identifying what a target is and isn't, and having that many guns on campus is inviting an accident.

Klinger said that just in February, two schools with campus police officers had an accidental discharge of a police firearm. "And that's a trained officer," she said.

"Here's the issue with arming teachers. I can put together a list of probably 100 things that can make your school safer and when you're done and at No. 101, we can talk about arming teachers," Klinger said.

Dan Pascale, vice president at Margolis Healy (a school security provider), said that centralizing entry is a good security practice for schools or businesses. "The battle is fought and won at the point of entry; the other 5 percent is already in the building."

The idea is having an entry place or a few entrances where students are greeted by faculty, and only those who should be in the school are allowed in the school.

There are difficulties, such as a school with 3,000 students and a single point of entry, so flexibility is needed, but all entries need to be treated the same.

"That means if we have access control systems in place or we are using people to vet visitors or using cameras, whatever we're using at the main entrance has to be used at all other entrances," Pascale said.

He said SROs are a great asset but echoed what Klinger said about not being in all places at the same time. "Many of our schools are a five-minute run from one place to another. They could be in an office, talking with a student and might be two, three, four, five minutes away from a suspect."

Pascale said having faculty at the point of entry to greet students when they enter is important.

These are the folks who can recognize patterns in advance or very early identify a problem and take appropriate action. Some institutions do this well and some don't, but it's an invaluable part of the school experience but you're also gaining intelligence at the same time."

Pascale said students also need a place to get help, someone to call and that the "interconnectivity" of school administrators, mental health professionals and counselors is critical.

"It's really that interconnectivity," Pascale said. "Everyone needs to play a role."

## New challenge for first responders: Fake News

Source: http://www.homelandsecuritynewswire.com/dr20180227-new-challenge-for-first-responders-fake-news

Feb 27 – First responders must find ways to address a new challenge: Not only do they have to deal with floods, storms, fires, earthquakes, active shooter events, and other natural and manmade crises – now they also have to find ways to deal with fake news.

Social media may disseminate valuable and helpful information during disasters and extreme events – but it may also be used to spread fake news: disinformation and misinformation about the scope, nature, and sources, and location of a disaster or extreme incident. Such misinformation may not only confuse victims and potential victims, but also confuse and mislead first responders who rush to their rescue.
On 22 February, the Homeland Security Science and Technology Advisory Committee (HSSTAC) issued a pre-decisional draft, titled Countering Misinformation, Rumors, and False Information on Social Media Before, During, and After Disasters and Emergencies, which discusses the fake news problem as it affects first responders, and offers a set of recommendations on how this problem should be addressed in order to reduce its harmful impact.

**From the report's draft:**

**Motivation**

Social media technologies have allowed individuals and organizations to share information with their peers and specific audiences for over fifteen years.[1] Information typically is shared with good intent; however, some share information as a means to further an ulterior agenda. This includes rumors, false information, and misinformation (e.g., deception, propaganda, and malicious spamming).
Researchers have identified different characteristics of information that lead to alternative, fake reality, and suspicious behavior.[2,4] Characteristics of false information include uncertainty in the facts, emotional exploitation to a situation, trending topic discussions for hijacking conversations, as well as attractive financial offer scams, among others.[3,4,5]
An example of false information with these characteristics is deceptive content with a malicious agenda, diverting a user towards a goal of advertising or phishing by coordinated social campaigns.[6] Such campaigns are also used to lead a user to believe in a fake negative opinion to damage an object's reputation; for example, fake reviews on online e-commerce websites, such as Amazon or Yelp.[7] Likewise, deceptive false information has been plotted in large-scale disasters for financial gains by lucrative scam information.[8] False information with a malicious agenda has long existed in the form of propaganda, which has been used by terror organizations as a tactic to recruit.[9]
When discussing the online context of false information in today's information age, the concept of false information driven by a motive of a deceptive agenda has existed for many decades in military warfare.[10,11] Therefore, the strategies for countering false information with a malicious agenda in the online environment by either coordinated efforts of humans or bots could be informed by the offline environment as well.[12]

**Problem**

One of the biggest challenges public safety agencies and organizations face is how to reduce or eliminate the spread of false information especially as public demands for a response from these authorities increases. Social media can distribute news faster and to a wider audience than traditional news sources. However, that also means the potential for misinformation, false information, and rumors o spread and go viral is high.[13] A factor that may impede first responders' ability to mitigate and minimize the spread of misinformation, rumors, and false information is the decreasing public trust in government, media, and nongovernmental organizations (NGOs). While 2017 was a low point in terms of credibility of the media, the 2018 Edelman's Trust Barometer showed trust in journalism jumped five points while trust in social media platforms dipped two points. In addition, the credibility of "a person like yourself" — often a source of news and information on social media — dipped to an all-time low in the study's history. While this paper is focused on social media, responder agencies should be aware that many people still get their news primarily from television, which serves as an additional resource to counter false information.[14,15]
Solving the problem of how to reduce or eliminate the spread of false information requires understanding of the following questions:

- What are the causes of misinformation, rumors, or false information, and what are its characteristics?
- How does false information spread?
- What are best practices to counter the spread of false information?

This paper builds on real-world case studies of several incidents to explain and investigate answers to the aforementioned questions.

After discussing various aspects of the problem; offering case studies on events in which fake news played a part; listing recommendations for action; and highlighting the challenges the implementation of these recommendations face, the draft report concludes:

**Conclusion**

While rumors, misinformation, and false information continue, they cannot be entirely eliminated. Agencies can leverage the above proactive and preemptive measures to lessen the risks during disasters and emergencies as a result of misinformation, rumors, and false information. Some of the measures detailed in this report include mutual aid and partnerships with credentialed digital volunteers, pre-scripting messages, verification tactics, setting up a centralized web page, and more.Agencies should consider testing and exercising with rumors, misinformation, and false information to help them determine which best practices will work best for their audience. The SMWGESDM's [S&T's Social Media Working Group for Emergency Services and Disaster. Management ] previous report on incorporating social media into exercises offers how-to guidance.

Social media is a continually changing topic, and while the tactics discussed in this paper are relevant now, the landscape keeps evolving and will continue to do so. In the future, the authors of this paper may add to this paper or create an external living document of references and resources that may be relevant for first responder agencies.

**References**

[1] An early example of social media being used to share information is the website Friendster.com, which was launched in 2002. https://en.wikipedia.org/wiki/Friendster

[2] Susan Coppess Pendleton. 1998. Rumor research revisited and expanded. Language & Communication, 18,1: 6986;. [4] Jiang, M., Cui, P., & Faloutsos, C. (2016). Suspicious behavior detection: Current trends and future directions. IEEE Intelligent Systems, 31(1), 31-39.

[3] Starbird, K., Spiro, E., Edwards, I., Zhou, K., Maddock, J., & Narasimhan, S. (2016, May). Could This Be True?: I Think So! Expressed Uncertainty in Online Rumoring. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 360-371). ACM.

[4] Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. First Monday, 21(11).

[5] Huang, Y. L., Starbird, K., Orand, M., Stanek, S. A., & Pedersen, H. T.(2015, February). Connected through crisis: Emotional proximity and the spread of misinformation online. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (pp. 969-980). ACM.

[6] Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y.(2010, November). Detecting and characterizing social spam campaigns. In Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (pp. 35-47). ACM.

[7] Mukherjee, A., Liu, B., & Glance, N. (2012, April). Spotting fake reviewer groups in consumer reviews. In Proceedings of the 21st international conference on World Wide Web (pp. 191-200). ACM.

[8] Gupta, A., Lamba, H., & Kumaraguru, P. (2013, September). $1.00 per rt# bostonmarathon# prayforboston: Analyzing fake content on twitter. In eCrime Researchers Summit (eCRS), 2013 (pp. 1-12). IEEE.

[9] Allendorfer, W. H., & Herring, S. C.(2015). ISIS vs. the US government: A war of online video propaganda. First Monday, 20(12).

[10] Whaley, B. (1982). Toward a general theory of deception. The Journal of Strategic Studies, 5(1), 178-192.

[11] Holt, T. (2010). The deceivers: Allied military deception in the Second World War. Simon and Schuster.

[12] A computer program that performs automatic repetitive tasks. https://www.merriamwebster.com/dictionary/bot

[13] Madhusree Mukerjee. "How Fake News Goes Viral – Here's the Math." *Scientific American*, July 14, 2017. https://www.scientificamerican.com/article/how-fake-news-goes-viral-mdash-heres-the-math/

[14] Pew Research Center. "Pathways to News." July 7, 2016. http://www.journalism.org/2016/07/07/pathways-tonews/

[15] Catherine Graham. "The Viral Nature of Social Media Messages in Disaster." January 31, 2018. https://www.slideshare.net/CatGraham/the-viral-nature-of-social-media-messages-in-disaster 18 Humanity Road Rumor Management Team Training June 20, 2016.

*— Read more in Countering Misinformation, Rumors, and False Information on Social Media Before, During, and After Disasters and Emergencies, Pre-Decisional Draft (HSSTAC, 22 February 2018).*

# Why Trump's idea to arm teachers may miss the mark

**By Aimee Huff and Michelle Barnhart**

Source: http://www.homelandsecuritynewswire.com/dr20180227-why-trump-s-idea-to-arm-teachers-may-miss-the-mark

Feb 27 – President Donald Trump's proposal to arm teachers has sparked substantial public debate. As researchers of consumer culture and lead authors of a recent study of how Americans use and view firearms for self-defense, we argue that while carrying a gun may reduce the risk of being powerless during an attack, it also introduces substantial and overlooked risks to the carrier and others.

**Where bullets land**

One of the biggest risks involved with arming teachers would be missing the target – literally. Despite the fact that police must undergo extensive professional training, particularly for high-pressure situations, one study notes that **police involved in gunfights shoot with an accuracy rate of just 18 percent.**

Assuming teachers can achieve the same level of accuracy as police, and that an armed teacher were able to get into position to fire, **just one in five or six bullets would hit the shooter. The other four or five bullets would hit something or someone else.** While an armed and trained teacher may be able to stop a shooter, the teacher may also shoot an innocent person.

**Why might they miss the target?**

Our recent study about people who keep and use handguns for self-defense can help to explain why someone using a gun against an attacker has difficulty hitting their target.

Over 24 months, the research team monitored 6,879 threads in four online discussion forums focused on armed self-defense. One author completed concealed handgun license training. Two contributing authors attended the annual NRA convention. The lead authors attended two gun shows, and interviewed two police officers and nine civilians who keep and/or carry handguns for self-defense.

Individuals in our study expressed concern about effectively using their training during an actual event. They spoke of the **possibility of "freezing up" or clumsily drawing their weapons**. Many, including police and military personnel, acknowledge that the fear and chaos caused by a threatening situation produce involuntary physical responses, such as a **racing heart and loss of fine motor skills**. They believe these responses could impede their ability to accurately fire and could expose themselves and bystanders to the risk of being shot. They engaged in regular rehearsals in an attempt to address these concerns.

Individuals in our study note other risks of using a gun for self-defense, such as **mistaking an innocent** person for an assailant or being **targeted by an assailant** who sees that you are armed. Indeed, if arming teachers becomes commonplace, shooters may target teachers first, further decreasing teachers' firing ability and accuracy.

We contend that other factors could inhibit teachers from effectively using their firearms training. The majority of shooters at high school and middle school incidents are current students. Recognizing the **shooter as a student could emotionally inhibit** a well-intentioned teacher from rapidly and accurately firing at him. Individuals in our study describe their reluctance to respond with firepower because they worry about being **mistaken for assailants by law enforcement** who respond to the scene. In the case of teachers, this fear could further inhibit them from engaging in a firefight.

**The day-to-day risks of arming teachers**

Our findings show that handgun owners perceive a host of other physical, legal, psychological and moral risks associated with day-to-day preparedness for armed self-defense. These risks include unnecessarily drawing or firing in a moment of fear or someone taking their gun to injure others. However, handgun owners express a willingness to accept these risks as a trade-off for decreasing their risk of being victimized.

Teachers who carry firearms would assume a variety of similar day-to-day risks. For instance, **armed teachers could unintentionally discharge their firearm or have their guns taken by an angry student while trying to break-up a fight.** The potential for having

their gun taken is very real. Research on **shootings that took place in hospital emergency departments shows that 23 percent involve a gun that is taken from an armed security guard.**
Reducing these day-to-day risks is taxing on individuals. Our data show that carrying a firearm responsibly involves continuous awareness of the weapon and the situation, understanding complex laws around self-defense, and mental preparedness to end a human life if necessary. More than half of the concealed carry license holders we interviewed and dozens of online discussants stated that they sometimes leave their firearms at home to avoid the burden of having to maintain this mindset.
Based on this finding, we assert that carrying a firearm would be equally taxing on teachers, if not more since they also must engage in the duties of their profession.

**Do the benefits outweigh the risks?**
Despite the widespread news coverage of mass shootings at schools, the reality is that school shootings are still a rare occurrence. In an FBI study of 160 active shooter incidents that FBI identified between 2000 and 2013, 27 – or about 17 percent – occurred at elementary, middle and high schools. Given that rarity, the challenges of effectively using a gun to neutralize a shooter without taking additional lives, and added day-to-day risks, we argue that Trump's proposal would not be effective in making schools safer overall for teachers or students.
It is difficult to address the question of whether, in the moment of a school shooting, the presence of an armed teacher is preferable to an unarmed one.
At least eight states currently permit teachers and school staff to carry firearms. However, the small percentage of schools with armed personnel combined with the small percentage of schools experiencing mass shootings limits the opportunity for a quantitative study of the risks and benefits of arming teachers. A recent review of the available data on the effectiveness of armed security and school resource officers in deterring or responding to a school shooting was inconclusive.
One of the most compelling findings comes from the same FBI report that found **between 2000 and 2013, it was unarmed civilians that stopped more active shooter events than armed civilians – 13.1 percent versus 3.1 percent, respectively.** "Of note, 11 of the incidents involved unarmed principals, teachers, other school staff and students who confronted shooters to end the threat (9 of those shooters were students)," the report states.
**This shows arming teachers isn't the only way to stop active shooters at schools. Often active school shooters are stopped by unarmed educators with the will to act.**

***Aimee Huff** is Assistant Professor, Marketing , Oregon State University.*
***Michelle Barnhart** is Associate Professor of Marketing, Oregon State University.*

# Mediglove pre printed Nitrile Medical Gloves

Source: http://www.mediglove.co.uk/ *Mediglove* is a pre printed Nitrile Medical Glove used for recording


Medigloves are ambidextrous and printed on both ides. Mediglove can be used in dry and wet conditions. 1005 Latex FREE. 50 Gloves per pack.

# U.S. Hospitals Can't Handle Catastrophic Attacks or Disasters, Report Finds

**By Bridget Johnson**

Mar 03 – A new report found that U.S. hospitals would struggle to respond adequately to large-scale catastrophic events such as disasters and attacks, raising concerns about the nation's capacity to handle bioterrorism or other mass-casualty events.

The two-year study from Johns Hopkins University Bloomberg School of Public Health's Center for Health Security states that although the healthcare system is better prepared post-9/11, it's still not par in terms of handling a catastrophic disaster — and "other segments of society that support or interact with the healthcare system and that are needed for creating disaster-resilient communities are not sufficiently prepared for disasters."


**Researchers put disaster prep into four categories: relatively small-scale mass injury/illness events like a tornado, shooting spree or small outbreaks; large-scale natural disasters such as significant hurricanes or earthquakes; complex mass casualty events such as the Las Vegas and Orlando mass shootings, the Boston Marathon bombing, the 2003 Station nightclub fire in Rhode Island, limited radiological and chemical events, and limited spread of deadly pathogens such as bioterrorism agents or Ebola; and catastrophic health events such as a major earthquake in a concentrated population center, a nuclear blast, or a large-scale pandemic or bioterror attack.**

"We conducted a gap analysis for each type of disaster and concluded that the United States is fairly well prepared for relatively small-scale mass injury/illness events that happen more frequently, less well prepared for large-scale and complex disasters, and poorly prepared for catastrophic health events," stated the authors, led by Eric Toner, MD.

One of the challenges is that preparing for one type of disaster "only partially prepares us for other types, and focusing solely on the common elements leaves gaps for specific actions or capabilities required for each type of event."

"Different events require different mixes of skill sets, resources, and response capabilities when the principal goal is to reduce injury and illness and to save lives," the report says. "…Non-English speakers and disabled people are at greater risk for all events, and individuals in inadequate housing may be more vulnerable to severe weather events and epidemics."

In the catastrophic category, the study notes that "infrastructure may be damaged, the normal healthcare system may be degraded and therefore would be enhanced risk, many complex casualties can be anticipated, and the geographic extent of casualties would likely cover a large area."

They cited a 2005 Department of Homeland Security report that laid out 15 catastrophic scenarios, including the detonation of a 10-kiloton nuclear device in Washington that would kill 9,000 people instantly and 36,000 more within 24 hours from trauma or radiation sickness, a wide-scale anthrax attack that would expose 328,000 people to the bacteria and potentially kill 13,000, and a magnitude 7.5 quake in a major city that could kill 1,400 people.

Researchers weighed the characteristics of each disaster category, the burden placed on the healthcare system, and the scope of the response.

Complex mass casualty events "can be expected to create a heavy but transient burden of trauma, critical care, and specialty care patients. Surge capacity at individual facilities may be temporarily overwhelmed, but overall local/regional healthcare system capacity is typically sufficient to meet the increased demand."

"In a catastrophic health event, a markedly increased burden on local and regional health sectors can be expected that may overwhelm surge capacity, even if the infrastructure is fully intact (which it may not be, depending on the scenario). Many parts of the system may be damaged or degraded for prolonged periods. This includes hospitals and healthcare facilities, but also services like home care," the report states. "Patients would include victims of the event as well as patients with chronic conditions who are displaced from their normal sources of care. The magnitude of the healthcare system burden may be affected by policy decisions or actions taken (or not), such as effective public messaging about sheltering."

The study calls for fostering a "**culture of resilience**" that incorporates the grassroots and community leaders.

"Much of civil society and many parts of the health sector are not resilient and are not participating in preparedness activities, as was demonstrated in Hurricanes Katrina and Sandy. When disaster strikes and these entities fail, people suffer and the hospitals become overwhelmed, leading to cascading hardship and suffering. To address this, many more components of the health sector and civil society need to be more resilient and connected to formal preparedness and resilience activities in their communities."

Researchers also called for creating a network of disaster resource hospitals as complex disasters "require expertise and resources that are not found in most hospitals," yet major medical centers with the resources may "lack a dedicated focus on disaster preparedness and response." Additionally, a national coordinator for catastrophic events would be responsible for keeping "sustained focus on catastrophic health events and integrating the work of the various initiatives without the distraction of needing to prepare for and respond to other types of common events."

"The role of the office should be to create a strategy and concept of operations for how all national assets would work together to most effectively respond to a catastrophic health event and then to coordinate efforts to implement them," the report recommended. "This office should also be charged with the implementation of a well-developed strategy for crisis standards of care."

***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 and Washington Bureau Chief for PJ Media. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, New York Observer, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera and SiriusXM.*

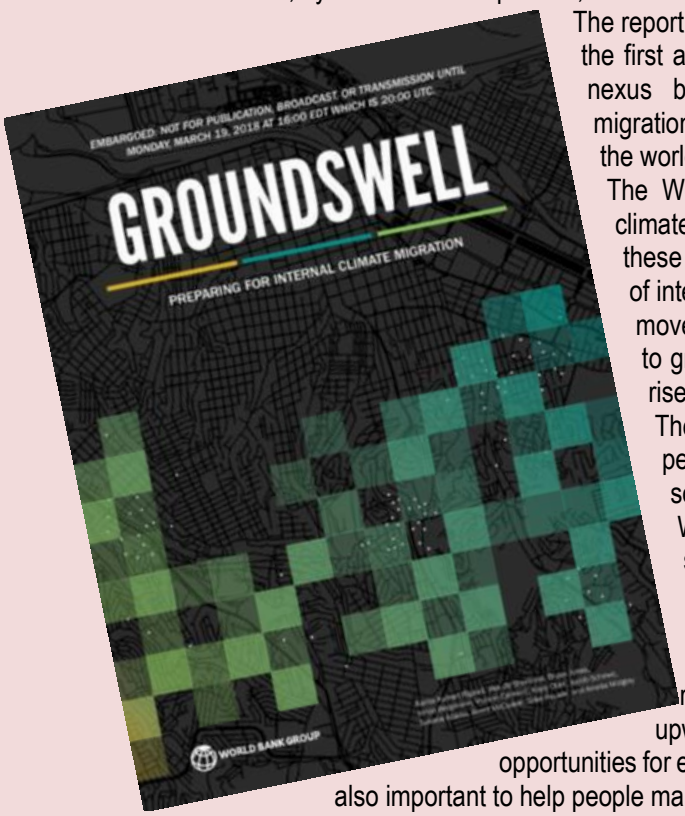

IOI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
ASYMMETRIC
THREATS

# Climate change could force over 140 million to migrate within countries by 2050

Source: http://www.homelandsecuritynewswire.com/dr20180321-climate-change-could-force-over-140-million-to-migrate-within-countries-by-2050

Mar 21 – The worsening impacts of climate change in three densely populated regions of the world could see over 140 million people move within their countries' borders by 2050, creating a looming human crisis and threatening the development process, a new World Bank Group report finds.

But with concerted action - including global efforts to cut greenhouse gas emissions and robust development planning at the country level – this worst-case scenario of over 140m could be dramatically reduced, by as much as 80 percent, or more than 100 million people.




The report, Groundswell – Preparing for Internal Climate Migration, is the first and most comprehensive study of its kind to focus on the nexus between slow-onset climate change impacts, internal migration patterns and, development in three developing regions of the world: Sub-Saharan Africa, South Asia, and Latin America.

The Word Bank notes that the reportfinds that unless urgent climate and development action is taken globally and nationally, these three regions together could be dealing with tens of millions of internal climate migrants by 2050. These are people forced to move from increasingly non-viable areas of their countries due to growing problems like water scarcity, crop failure, sea-level rise and storm surges.

These "climate migrants" would be additional to the millions of people already moving within their countries for economic, social, political or other reasons, the report warns.

World Bank Chief Executive Officer Kristalina Georgieva said the new research provides a wake-up call to countries and development institutions.

"We have a small window now, before the effects of climate change deepen, to prepare the ground for this new reality," Georgieva said. "Steps cities take to cope with the upward trend of arrivals from rural areas and to improve opportunities for education, training and jobs will pay long-term dividends. It's also important to help people make good decisions about whether to stay where they are or move to new locations where they are less vulnerable."

The research team, led by World Bank Lead Environmental Specialist Kanta Kumari Rigaud and including researchers and modelers from CIESIN Columbia University, CUNY Institute of Demographic Research, and the Potsdam Institute for Climate Impact Research - applied a multi-dimensional modeling approach to estimate the potential scale of internal climate migration across the three regions.

They looked at three potential climate change and development scenarios, comparing the most "pessimistic" (high greenhouse gas emissions and unequal development paths), to "climate friendly" and "more inclusive development" scenarios in which climate and national development action increases in line with the challenge. Across each scenario, they applied demographic, socioeconomic and climate impact data at a 14-square kilometer grid-cell level to model likely shifts in population within countries.

This approach identified major "hotspots" of climate in- and out-migration - areas from which people are expected to move and urban, peri-urban and rural areas to which people will try to move to build new lives and livelihoods.

"Without the right planning and support, people migrating from rural areas into cities could be facing new and even more dangerous risks," said the report's team lead Kanta Kumari Rigaud. "We could see increased tensions and conflict as a result of pressure on scarce resources. But that doesn't have to be the future. While internal climate migration is becoming a reality, it won't be a crisis if we plan for it now."

**The report recommends key actions nationally and globally, including:**

- Cutting global greenhouse gas emissions to reduce climate pressure on people and livelihoods, and to reduce the overall scale of climate migration
- Transforming development planning to factor in the entire cycle of climate migration (before, during and after migration)
- Investing in data and analysis to improve understanding of internal climate migration trends and trajectories at the country level.


*Transboundary River Basins and Political Tensions," Sustainable Security (13 July 2017).*